TABLE OF CONTENTS

SECTION **PAGE**

SECTION 5 – UNIFIED CAPABILITIES PRODUCT REQUIREMENTS 113
5.1 Requirements Categories and Language.....113
5.1.1 Minimum Requirements 113
5.1.2 Conditional Requirements 113
5.1.3 Operational Control over Features and Capabilities.....113
5.1.4 General Requirement Language 114
5.1.5 AS-SIP Requirement Adheres to IETF Specification Language.....114
5.2 Circuit-Switched Capabilities and Features.....115
5.2.1 Capabilities and Features 120
5.2.1.0 Introduction.....120
5.2.1.1 Features Common to Single Users and Business Customers 120
5.2.1.1.1 Individual Line.....120
5.2.1.1.2 CLASS^{SM} Feature: Selective Call Rejection 120
5.2.1.1.3 Denied Originating Service.....121
5.2.1.1.4 Code Restriction and Diversion.....121
5.2.1.1.5 Call Waiting Features 121
5.2.1.1.6 Three-Way Calling.....122
5.2.1.1.7 Add-On Transfer and Conference Calling Features 122
5.2.1.1.8 Call Forwarding Features and Call Forwarding Subfeatures.....125
5.2.1.1.9 Call Pick-Up Features 127
5.2.1.2 Attendant Features 128
5.2.1.2.1 Precedence and Preemption 128
5.2.1.2.2 Call Display 128
5.2.1.2.3 Class of Service Override 128
5.2.1.2.4 Busy Override and Busy Verification.....128
5.2.1.2.5 Night Service 129
5.2.1.2.6 Automatic Recall of Attendant 129
5.2.1.2.7 Calls in Queue to the Attendant.....129
5.2.1.2.8 Release to Pivot for Operator Services 129
5.2.1.3 Customer Access Interfaces.....130
5.2.1.3.1 PBX Line 130
5.2.1.3.2 Direct Inward Dialing 131
5.2.1.3.3 National ISDN 1/2 Basic Access 131

5.2.1.3.4 ISDN Primary Access 132
5.2.1.3.5 Analog Line 133
5.2.1.4 Public Safety Features 133
5.2.1.4.1 911 Service.....133
5.2.1.4.2 Tracing of Terminating Calls.....135
5.2.1.4.3 Outgoing Call Tracing 136
5.2.1.4.4 Tandem Call Trace.....136
5.2.1.4.5 Trace a Call in Progress 136
5.2.1.5 Trunk, Line, and Special Service Circuit Service Test Features.....136
5.2.1.5.1 Local Office Test Lines 137
5.2.1.5.2 Outside Plant Test Lines 138
5.2.1.5.3 Test Incoming Trunks in Tandem or Local State.....138
5.2.1.5.4 Manual Testing 139
5.2.1.5.5 Trunk Group – Remove from Service (Make Busy) 139
5.2.1.5.6 Trunk Group – Restore to Service (Make Idle) 139
5.2.1.5.7 Carrier Group Alarm.....140
5.2.1.6 Conferencing.....140
5.2.1.6.1 Preset Conferencing.....140
5.2.1.6.2 Meet-Me Conferencing.....144
5.2.1.6.3 Progressive Conferencing 144
5.2.1.7 Address Translation 145
5.2.1.8 Nailed-Up Connections.....145
5.2.1.9 Assured Dial Tone 146
5.2.1.10 DSN Remote Switching Unit Requirements 146
5.2.1.11 Control of Precedence Calls 147
5.2.1.11.1 Precedence Access Threshold.....147
5.2.1.12 DSN Hotline Service 152
5.2.1.12.1 Protected Hotline Calling.....152
5.2.1.12.2 Hotline Service Protection 153
5.2.1.12.3 Non-Pair Protected Hotline Calling 155
5.2.1.12.4 Pair Protected Hotline Calling 155
5.2.2 Multilevel Precedence and Preemption 155
5.2.2.0 Introduction.....155
5.2.2.1 MLPP Overview 155
5.2.2.1.1 Description.....155
5.2.2.1.2 Precedence Levels.....156
5.2.2.1.3 Announcements.....156

5.2.2.1.4 Invocation and Operation.....157
5.2.2.2 Preemption in the Network.....159
5.2.2.2.1 Network Facilities Active with Lower Precedence Calls.....159
5.2.2.2.2 Network Facilities Active with Equal or Higher Precedence Call.....160
5.2.2.2.3 MLPP Trunk Selection (Hunting).....160
5.2.2.2.4 MLPP Interworking with Other Networks 163
5.2.2.3 Precedence Call Diversion.....164
5.2.2.4 Preempt Signaling.....165
5.2.2.4.1 Channel Associated Signaling 165
5.2.2.4.2 Primary Rate Interface 167
5.2.2.4.3 Common Channel Signaling Number 7.....167
5.2.2.5 Analog Line MLPP.....168
5.2.2.5.1 Busy at the Called Party's Interface.....168
5.2.2.6 ISDN MLPP BRI.....168
5.2.2.6.1 General Description 168
5.2.2.6.2 Single B Channel, Single Appearance, Single Directory Number 169
5.2.2.6.3 Single B Channel, Multiple Appearances, Single Directory Number 169
5.2.2.6.4 Two B Channels, Multiple Appearances, Single Directory Number 170
5.2.2.6.5 Two B Channels, Two Directory Numbers (Data Mode Only).....171
5.2.2.7 ISDN MLPP PRI 171
5.2.2.7.1 Definitions.....171
5.2.2.7.2 Precedence Level Information Elements 171
5.2.2.7.3 Disconnect Message Information Cause Values 173
5.2.2.7.4 Signal Information Element.....173
5.2.2.7.5 ANSI T1.619a Setup Message Called Party Number Format.....174
5.2.2.7.6 ANSI T1.619a and Non-ANSI T1.619a Interaction 175
5.2.2.8 MLPP Interactions with Common Optional Station Features and Services.....176
5.2.2.8.1 Precedence Call Waiting.....176
5.2.2.8.2 Call Forwarding 177
5.2.2.8.3 Call Transfer 178
5.2.2.8.4 Call Hold.....179

5.2.2.8.5 Three-Way Calling....181
5.2.2.8.6 Call Pick-up 181
5.2.2.8.7 Conferencing....182
5.2.2.8.8 Multiline Hunt Service....182
5.2.2.8.9 Community of Interest 183
5.2.2.9 MLPP CCS7 189
5.2.2.9.1 General Description 189
5.2.2.9.2 Definitions....189
5.2.2.9.3 Look-Ahead for Busy 189
5.2.2.9.4 Precedence Parameters....190
5.2.2.9.5 RELEASE Message Cause Values 192
5.2.2.9.6 DSN MLPP CCS7 IAM Called Party Number Format 193
5.2.2.10 MLPP Interactions with Electronic Key Telephone Systems Features....197
5.2.2.10.1 Electronic Key Telephone Systems 197
5.2.2.11 Backward Compatibility....199
5.2.2.11.1 Precedence Parameter 199
5.2.2.11.2 Cause Values and Location Codes....199
5.2.2.12 Network Management Manual Controls....199
5.2.2.13 Data Collection 199
5.2.3 Call Processing 200
5.2.3.0 Introduction....200
5.2.3.1 Call Treatments....200
5.2.3.1.1 Origination Treatment....200
5.2.3.1.2 Termination Treatment 201
5.2.3.1.3 Release Treatment....201
5.2.3.1.4 Interruption Treatment 202
5.2.3.1.5 Connections....202
5.2.3.1.6 Class of Service....202
5.2.3.2 Primary and Alternate Routing 202
5.2.3.3 User Access Line Call Processing (Non-CCS/ISDN Type)203
5.2.3.3.1 E&M Lead Signaling States....203
5.2.3.3.2 4-Wire Analog User Access Lines....204
5.2.3.3.3 2-Wire User Access Lines 206
5.2.3.3.4 Termination to Analog Lines 209
5.2.3.4 DSN Interswitch Trunk Call Processing (Non-CCS/ISDN Type)....209
5.2.3.4.1 Originating Call Processing 209
5.2.3.4.2 Terminating Call Processing....212
5.2.3.5 Code Interpretation 217

5.2.3.5.1 DSN Worldwide Numbering and Dialing Plan 217
5.2.3.5.2 DSN Switch Outpulsing Digit Formats 221
5.2.3.5.3 Standard Directory Numbers 233
5.2.3.5.4 Standard Test Numbers 234
5.2.3.5.5 Base Services – Abbreviated Numbers 234
5.2.3.5.6 Digit Reception Requirements 234
5.2.3.5.7 Digit Registration Capacity 234
5.2.3.5.8 Screening 235
5.2.4 Signaling 236
5.2.4.0 Introduction 236
5.2.4.1 Network Power Systems for External Interfaces 236
5.2.4.2 Line Signaling 236
5.2.4.2.1 Loop Start Line 236
5.2.4.2.2 Ground Start Line 236
5.2.4.3 Trunk Supervisory Signaling 237
5.2.4.3.1 Reverse Battery 237
5.2.4.3.2 Immediate Start 237
5.2.4.3.3 Normal and Abnormal Wink Start Operation 238
5.2.4.3.4 Delay Dial 239
5.2.4.3.5 Call for Service Timing 239
5.2.4.3.6 Guard Timing 239
5.2.4.3.7 Satellite Interface 239
5.2.4.3.8 Disconnect Control 239
5.2.4.3.9 Reselect or Retrial 240
5.2.4.3.10 Off-Hook Supervision Transitions (Unexpected Stop) 240
5.2.4.4 Control Signaling 240
5.2.4.4.1 Dial-Pulse Signals 241
5.2.4.4.2 DTMF Signaling 241
5.2.4.4.3 Multifrequency (MF(R1) 2/6) Signaling 241
5.2.4.5 Alerting Signals and Tones 242
5.2.4.5.1 Ringing 242
5.2.4.5.2 DSN Information Signals 242
5.2.4.6 Common Channel Signaling Number 7 243
5.2.4.6.1 CCS7 Network Structure 244
5.2.4.6.2 Functional Description of the Signaling System Message Transfer Part 244
5.2.4.6.3 Signaling Network Functions and Messages .245
5.2.4.6.4 Non-Circuit-Related Information Exchange – Signaling Connection Control Part 246

5.2.4.6.5 Additional Procedures for Switch-to-Switch/SCP TCAP Messages 246
5.2.4.6.6 Message Transfer Part Restart 247
5.2.4.6.7 Signaling Link Management.....247
5.2.4.6.8 Signaling Route Management.....247
5.2.4.6.9 Common Characteristics of Message Signal Unit Formats 247
5.2.4.6.10 Formats and Codes of Signaling Network Management Messages 248
5.2.4.6.11 Numbering of Signaling Point Codes 248
5.2.4.6.12 Functional Descriptions of ISDN User Part...249
5.2.4.6.13 Formats and Codes – ISDN User Part Parameters.....249
5.2.4.7 ISDN Digital Subscriber Signaling System No. 1 Signaling 250
5.2.4.7.1 DSN ISDN User-to-Network Signaling.....250
5.2.5 Transmission.....256
5.2.5.0 DSN Transmission Interface.....256
5.2.5.1 Input Impedance 256
5.2.5.2 Inserted Connection Loss 257
5.2.5.2.1 Average Loss at 1004 Hz And Loss Control .257
5.2.5.2.2 Loss Variability at 1004 Hz 258
5.2.5.2.3 Attenuation Distortion 258
5.2.5.2.4 Tracking Error.....259
5.2.5.3 Frequency Response 259
5.2.5.4 Overload Level 260
5.2.5.5 Return Loss.....260
5.2.5.5.1 2-Wire Line Return Loss 260
5.2.5.5.2 4-Wire Trunk Return Loss (Impedance).....260
5.2.5.6 Longitudinal Balance.....261
5.2.5.7 60 Hertz Longitudinal Current.....261
5.2.5.8 Idle Channel Noise.....261
5.2.5.8.1 C-Message Weighting.....261
5.2.5.8.2 Flat-Weighting Noise.....262
5.2.5.9 Power Line Interference.....262
5.2.5.10 Impulse Noise 262
5.2.5.11 Crosstalk Coupling 262
5.2.5.12 Intermodulation Distortion 262
5.2.5.13 Signal to Distortion Ratio (C-Notched Noise).....263
5.2.5.14 Absolute Delay 263
5.2.5.15 Envelope Delay Distortion.....263

5.2.5.15.1 Echo Path Delay....264
5.2.5.16 Bit Integrity....264
5.2.5.17 Switched Digital Bit Error Rate....264
5.2.5.18 Encoding and Decoding Levels....265
5.2.5.18.1 DSN Fixed Loss Plan....265
5.2.6 System Interfaces....266
5.2.6.1 PCM-24 Digital Trunk Interface....266
5.2.6.1.1 Interface Characteristics....266
5.2.6.1.2 Supervisory Channel Associated Signaling...268
5.2.6.1.3 Clear Channel Capability....269
5.2.6.1.4 Alarm and Restoral Requirements....269
5.2.6.2 PCM-30 Digital Trunk Interface....269
5.2.6.2.1 Supervisory Channel Associated Signaling...272
5.2.6.2.2 Alarm and Restoral Requirements....272
5.2.6.3 Interoperation of PCM-24 and PCM-30 Systems....273
5.2.6.4 Analog Trunk Interface....273
5.2.6.4.1 E&M Trunk Circuits....273
5.2.6.4.2 Single Frequency Trunk Circuits....274
5.2.6.4.3 Dual Frequency Trunk Circuits....274
5.2.6.5 Integrated Digital Loop Carrier....274
5.2.6.5.1 E-Telemetry Scan Point System Operation...275
5.2.7 Tandem Switching....276
5.2.7.1 Network Plan....276
5.2.7.2 System Design....276
5.2.7.3 Tandem Capabilities....276
5.2.7.4 Call Processing....276
5.2.7.5 Signaling....278
5.2.7.6 Transmission....278
5.2.7.7 Measurements and Administration....278
5.2.7.8 Service Standards....278
5.2.7.9 Network Management....279
5.2.8 Network Management....279
5.2.8.1 DISA/DSN Network Management....279
5.2.8.2 Measurements and Data Generation....280
5.2.8.2.1 Common Data Requirements....280
5.2.8.2.2 Circuit-Switched Network Measurements....280
5.2.8.2.3 Common Channel Signaling Network Measurements....282
5.2.8.2.4 ISDN Measurements....283
5.2.8.2.5 Traffic Capacity....283
5.2.8.3 Fault Management....283

5.2.8.4 Configuration Management 283
5.2.8.5 Automated Message Accounting 283
5.2.8.5.1 DSN Call Detail Recording Fields 283
5.2.8.5.2 Call Detail Recording Data Retention 284
5.2.8.6 Performance Management 284
5.2.8.7 Network Management Controls 287
5.2.8.7.1 Automatic Controls 287
5.2.8.7.2 Overload Controls 289
5.2.8.7.3 Manual Controls 289
5.2.8.7.4 Treatment Options of Calls Terminated 294
5.2.8.8 Remote Access to Switch 294
5.2.9 Integrated Services Digital Network 294
5.2.9.1 ISDN Overview 294
5.2.9.2 DSN Generic ISDN Features and Interface Descriptions 295
5.2.10 Synchronization 300
5.2.10.1 Timing Modes 300
5.2.10.1.1 External Timing Mode 300
5.2.10.1.2 Internal Clock Requirements 301
5.2.10.2 Synchronization Performance Monitoring Criteria 301
5.2.10.3 DS1 Traffic Interfaces 301
5.2.10.4 DS0 Traffic Interconnects 301
5.2.11 Reliability 301
5.2.11.1 Reliability Requirements 301
5.2.11.2 System Availability 302
5.2.11.2.1 Vendor Reliability Model 302
5.2.11.2.2 Hardware Failure Detection 302
5.2.11.2.3 Individual Termination Downtime 302
5.2.11.2.4 Predicted Multi-Termination Downtime 302
5.2.11.2.5 Predicted Total Capability Downtime 303
5.2.11.2.6 Hardware Cutoff Call Rate 303
5.2.11.2.7 Operations System Interface Downtime 303
5.2.11.2.8 Capability Downtime 303
5.2.11.3 Backup Power 304
5.2.11.3.1 Power Components 304
5.2.11.3.2 UPS Requirements 304
5.2.11.3.3 Backup Power (Environmental) 305
5.2.11.3.4 Alarms 305
5.2.12 Specific Circuit-Switched Peripherals 305
5.2.12.1 Echo Canceller Requirements 305
5.2.12.1.1 Background 305
5.2.12.1.2 Purpose 306

5.2.12.1.3 Applicability 306
5.2.12.1.4 Definitions.....307
5.2.12.1.5 Requirements 307
5.2.12.1.6 Echo Canceller Application Guidelines.....310
5.2.12.2 DSN Switch SONET Digital Trunk Interface 312
5.2.12.2.1 Background.....312
5.2.12.2.2 Purpose.....313
5.2.12.2.3 Applicability 313
5.2.12.2.4 Definitions.....314
5.2.12.2.5 Requirements 314
5.2.12.3 Customer Premises Equipment Requirements.....317
5.2.12.3.1 Background.....317
5.2.12.3.2 Purpose.....317
5.2.12.3.3 Applicability 317
5.2.12.3.4 Definitions.....318
5.2.12.3.5 Requirements 320
5.2.12.4 Video Teleconferencing Requirements 325
5.2.12.4.1 Background.....325
5.2.12.4.2 Purpose.....325
5.2.12.4.3 Applicability 325
5.2.12.4.4 General.....326
5.2.12.4.5 Video Teleconferencing Requirements.....327
5.2.12.4.6 Definitions.....328
5.2.12.5 DSN Strategic Network Element Generic Requirements...329
5.2.12.5.1 Background.....329
5.2.12.5.2 Purpose.....330
5.2.12.5.3 Applicability 330
5.2.12.5.4 Definitions.....330
5.2.12.5.5 Requirements 330
5.2.12.6 DoD Secure Communications Devices.....335
5.2.12.6.1 Background.....335
5.2.12.6.2 Definitions.....335
5.2.12.6.3 Scope.....335
5.2.12.6.4 Purpose.....335
5.2.12.6.5 Applicability 336
5.2.12.6.6 Requirements 336
5.2.12.7 Integrated Access Switch/System Requirements.....337
5.2.12.7.1 Background.....337
5.2.12.7.2 Purpose.....337
5.2.12.7.3 Applicability 337
5.2.12.7.4 Integrated Access Switch Requirements.....338

5.2.12.8 DSN Line Side Voice over Internet Protocol Requirement....345
5.2.12.8.1 Background....345
5.2.12.8.2 VoIP System Requirements....347
5.2.12.8.3 Softphones....349
5.2.12.8.4 V.150.1 Gateway Capability....349

SECTION 5
UNIFIED CAPABILITIES PRODUCT REQUIREMENTS

5.1 REQUIREMENTS CATEGORIES AND LANGUAGE

Section 5 of UCR 2008 identifies the minimum functional and performance requirements for products to be placed on the UC APL. Requirements are specified in terms of two categories: Minimum requirements and Conditional requirements.

5.1.1 Minimum Requirements

Minimum requirements are features and capabilities considered necessary for a particular switch type to support warfighter missions in the DoD. These features and capabilities will require certification prior to introduction into the DISN.

5.1.2 Conditional Requirements

Conditional requirements are features and capabilities that are not considered critical for DoD mission support based on DoD policies. Nevertheless, it is recognized that such features do have utility for some users or for specific operations. To ensure interoperability and consistency of the Assured Services (AS) across all platforms, these features and capabilities are specified with set parameters. If these features and capabilities are provided, the UC product shall perform and meet the requirements as identified in UCR 2008.

5.1.3 Operational Control over Features and Capabilities

Some features and capabilities are dependent on permission for implementation control.

Vendors shall provide features and functions in accordance with Telcordia, Internet Engineering Task Force (IETF), and/or other commercial standards unless specifically altered (i.e., added, modified, or deleted) by UCR 2008. Additionally, those features and functions that are not specified in Telcordia, IETF, and/or other commercial standards shall optionally be either parameter(s) and/or software controlled whenever practical, especially if the UCR requirement used is conditional, to either permit or not use.

Examples of some features and capabilities are call forwarding off the DSN, routing a call from the DSN to terminate on the Public Switch Telephone Network (PSTN), providing a “leaving command and control (C2) environment” message, and changing the dial plan from NYX-NNX

to KXX-NXX. The permission to use these features and capabilities may come from DoD policy and/or base commander decision and shall not be limited by the vendor.

5.1.4 General Requirement Language

The word "REQUIRED" or the term "MUST" or "SHALL" means the definition is an absolute requirement of the product.

The word "CONDITIONAL" or the term "MAY" means an item is optional.

The phrase "MUST NOT" or "SHALL NOT" means the definition is an absolute prohibition of the item.

The word "RECOMMENDED" means the reference is given as guidance and is not a testable requirement.

The phrase "THE NETWORK", as referenced in the LATA Switching Systems Generic Requirements (LSSGR), shall mean the DSN network.

5.1.5 AS-SIP Requirement Adheres to IETF Specification Language

The AS-SIP requirement of UCR 2008 is built on IETF Request for Comments (RFC). The AS-SIP requirement therefore adheres to the IETF terminology which use terms or key words including: "MUST," "MUST NOT," "REQUIRED," "SHALL," "SHALL NOT," "SHOULD," "SHOULD NOT," "RECOMMENDED," "NOT RECOMMENDED," "MAY," and "OPTIONAL." These terms indicate requirement levels for compliant SIP implementations and are to be interpreted as described in IETF BCP 14, RFC 2119.

5.2 CIRCUIT-SWITCHED CAPABILITIES AND FEATURES

This section defines UCR 2008 circuit-switched system capabilities and features. The requirements for this section of the DoD UCR are written as a military requirements for a telephone switching facility, and it is written as a hardware requirement (a telecommunications switch) and uses the commercial standards Local Access and Transport Area (LATA) Switching Systems Generic Requirements (LSSGR) as the base structure. The requirements have been expanded to include limited, best-effort IP, wireless, and softphone interface requirements. This section continues using the LSSGR with references to the Generic Requirements document for circuit-switched networks. Except for Military Unique Features (MUFs), such as Multilevel Precedence and Preemption (MLPP), there should be no differences in the technical requirements between the LSSGR and UCR 2008 circuit-switched requirements.

The DSN circuit-switched design is a two-level network hierarchy consisting of DSN backbone switches and military or agency installation switches. The DSN also consists of the Deployable Voice Exchange (DVX) that is a tactical switch with MUF capabilities to support the DoD assured service requirements used for rapid deployment situations and contingencies in the tactical environment. The DVXs can be either DVX COTS (DVX-C), or DVX legacy (DVX-L) tactical (TRI-TAC) systems. Normally, a DVX is connected to the DSN using gateway trunks routed through a standard tactical entry point (STEP)/Teleport location. It can be connected directly to the DSN (TS/MFS/EO/SMEO), if it is to be used as a temporary solution for either of the following:

1. An initial capability that will be replaced by a more permanent solution for sustainment of strategic operations.

2. A solution for augmenting a strategic communications facility to meet rapid growth or restoration requirements.

Detailed requirements for the DVX are contained in individual paragraphs in this section. A strategic DSN PBX1 is connected to a DSN EO or SMEO switch; however, a deployable DSN PBX1 may need to connect through a STEP/Teleport to a DSN switch. This configuration includes some limitations, as follows:

1. The PBX1 functionality shall be limited only to those that were tested and certified by the JITC and as posted on the APL. The user assumes all limitations identified in the JITC test report.

2. The PBX1 was designed for connecting to only one supporting DSN switch. If connections to more than one switch are required, testing must verify this capability.

3. The PBX1 must not tandem and shall not have any subordinate switches or lateral connectivity.

4. Fewer variants may be available for PSTN/PTT connections.

5. The PBX1 requirements do not include the use of an attendant and this capability is not tested.

6. PBX1s are not approved to support special C2 (FLASH and FLASH OVERRIDE) users as their only means of communication. Special C2 users shall be supported by other means such as a long local.

The switches are connected by several types of trunks, as shown in the following tables.

Joint Staff policy and subscriber mission requirements determine which location requires the full set of MUFs and capabilities offered by the DSN circuit-switched network. The DSN design therefore consists of several categories of switches. They may be used as outlined in this document.

The interfaces of the DSN circuit-switched design are shown in the following tables.

Table 5.2-1 lists the trunk types and signaling used in the DSN, including legacy interfaces.

Table 5.2-1. Trunk Types and Signaling Used in the DSN (Includes Legacy Interfaces)

TRUNK TYPE	PURPOSE/USE	SWITCH-TO-SWITCH SIGNALING	ELECTRICAL INTERFACE
Interswitch Trunk (IST)	Backbone transport TS-to-TS	SS7 (ANSI T1.619a & ITU Q.735.3), CAS MF(R1) 2/6	T1:(B8ZS/ESF, AMI/D4) E1:(HDB3) OC3
Community of Interest Trunk (COI)	EO/SMEO to EO/SMEO direct traffic		T1:(B8ZS/ESF, AMI/D4) E1:(HDB3) OC3, Analog
EO Access Trunk	EO/SMEO to Tandem Switch	SS7/PRI (ANSI T1.619a, and ITU Q.955.3 & Q.735.3), CAS (MF(R1) 2/6, DP, DTMF), Analog (E&M)	T1:(B8ZS/ESF, AMI/D4) E1:(HDB3) OC3, Analog
Gateway Trunk	DSN to other networks	SS7/PRI (ANSI T1.619a, and ITU Q.955.3 & Q.735.3), CAS (MF(R1) 2/6, DP, DTMF), Various host nation -Analog Commercial Interfaces	T1:(B8ZS/ESF, AMI/D4) E1:(HDB3) OC3

TRUNK TYPE	PURPOSE/USE	SWITCH-TO-SWITCH SIGNALING	ELECTRICAL INTERFACE
Host Remote (H-R) Link	Remote Unit to Host umbilical only	Proprietary	T1:(B8ZS/ESF, AMI/D4) E1:(HDB3), OC3
PBX1 Access Trunk (MLPP Capable)	PBX to EO/SMEO Access	SS7/PRI (ANSI T1.619a, and ITU Q.955.3 & Q.735.3), CAS (MF(R1) 2/6, DP, DTMF), Analog (E&M)	T1:(B8ZS/ESF, AMI/D4) E1:(HDB3) OC3, Analog
PBX2 Access (Non-MLPP) Trunk	PBX to EO/SMEO Access	One of the following is required as a minimum: Non-MLPP Commercial ISDN PRI, CAS (MF(R1), MF(R2) 2/6, DP, DTMF), Analog (E&M)	T1:(B8ZS/ESF, AMI/D4) E1:(HDB3) OC3, Analog
Tactical Trunk	Legacy Tactical Communications Teleport, STEP, SMU and various Tactical Switches	TRI-TAC Unique DTG T1/E1 CAS (DTMF), T1 PRI (T1.619a)	CVSD-conditioned Diphase T1CEPT: B8ZS/ESF, AMI/D4 E1:(HDB3)

LEGEND

AMI	Alternate Mark Inversion	DTMF	Dual-Tone Multifrequency	OC3	Optical Carrier Level 3
ANSI	American National Standards Institute	E&M	Ear and Mouth	PBX	Private Branch Exchange
B8ZS	Bipolar with Eight-Zero Substitution	EO	End Office	PBX1	Private Branch Exchange Type 1
CAS	Channel Associated Signaling	ESF	Extended Superframe	PBX2	Private Branch Exchange Type 2
CEPT	Commission of European Post and Telecommunication	HDB3	High Density Bipolar 3 Code	PRI	Primary Rate Interface
COI	Community of Interest	H-R	Host Remote	SMEO	Small End Office
CVSD	Continuously Variable Slope Delta	ISDN	Integrated Services Digital Network	SMU	Switch Multiplexing Unit
D4	Fourth Generation Channel Bank	IST	Interswitch Trunk	SS7	Signaling System No. 7
DP	Dial Pulse	ITU	International Telecommunications Union	STEP	Standardized Tactical Entry Point
DSN	Defense Switched Network	MF	Multifrequency	TRI-TAC	Tri-Service Tactical Communications
DTG	Date-Time-Group	MLPP	Multilevel Precedence and Preemption	TS	Tandem Switch

Table 5.2-2, Subscriber Access Lines Used in the DSN, describes the types of subscriber access lines used in the DSN.

Table 5.2-2. Subscriber Access Lines Used in the DSN

TYPE SUBSCRIBER LINE	SIGNALING	ELECTRICAL INTERFACE
2-Wire Analog Subscriber Line	IAW GR-506-CORE For precedence, see UCR 2008, Table 5.2.2-2 and Figure 5.2.2-3.	2-Wire Analog Loop
Digital/Analog Proprietary Subscriber Line	Proprietary	Proprietary
ISDN BRI Subscriber Line	ISDN BRI ANSI T1.619a, NI-1, NI-2, 5ESS Custom, NTI MSL-100, ETSI ITU-T,	ST, U
4-Wire Analog Subscriber Line	DP, DTMF, E&M	4-Wire E&M Type I, Type II Type V
ISDN PRI	ISDN PRI, (Commercial, NI-2, 619a, 5ESS Custom)	T1, E1

LEGEND

ANSI	American National Standards Institute	GR	Generic Requirement	NI-1	National ISDN 1
BRI	Basic Rate Interface	IAW	In Accordance With	NI-2	National ISDN 2
DP	Dial Pulse	ISDN	Integrated Services Digital Network	NTI	Northern Telecom, Inc.
DTMF	Dual-Tone Multifrequency	ITU-T	International Telecommunications Union – Telecommunication Standardization Sector	PRI	Primary Rate Interface
E&M	Ear and Mouth			ST	Signaling Terminal
ETSI	European Telecommunications Standards Institute			U	Unit of Measurement
				UCR	Unified Capabilities Requirements

Table 5.2-3, Trunk and Line Types Required by Switch Type, summarizes the trunk types required for each DSN switch type.

Table 5.2-3. Trunk and Line Types Required by Switch Type

TRUNK/LINE TYPE	TS	MFS	EO	SMEO	PBX1	PBX2	DVX[1]
T1 SS7 (T1 619a)	R	R	R	C	C	C	C
E1 SS7 (ITU-T Q.735.3 (R=EUROPE ONLY)	R[2]	R[2]	R[2]	C	C	C	C
T1 CAS MFR1	R	R	R	C	C	C[3]	C
T1 CAS DTMF	R	R	R	R	C	C[3]	R
T1 CAS DP	R	R	R	R	C	C[3]	R
E1 CAS MFR1 (R=EUROPE ONLY)	R	R	R	R	C	C	R
E1 CAS DTMF (R=EUROPE ONLY)	R	R	R	R	C	C	R
E1 CAS DP (R=EUROPE ONLY)	R	R	R	R	C	C	R
T1 ISDN PRI (ANSI T1.619a)	R	R	R	R	R	C	R
ISDN PRI NI-1/2 Network and User)	R	R	R	R	R	C[3]	R
E1 ISDN PRI (ITU-T Q.955.3) (R=EUROPE ONLY) (Network and User)	R[2]	R[2]	R[2]	C	C	C	C
2-Wire Analog Lines		R	R	R	R	C[4]	R
ISDN BRI Subscriber NI-1/2		R	R	R	C	C[4]	C
ISDN-BRI ANSI T1-619a		R	R	R	C	C	C

NOTES:
1. DVX-C only. See UCR 2008, Section 4.2.1.7, Deployable Voice Exchange, for DVX-L requirements.
2. Required if switch is to be installed in OCONUS-ETSI-compliant countries.
3. One of the trunk types is required.
4. One of the line types is required.

LEGEND

ANSI	American National Standards Insitute	EO	End Office	OCONUS	Outside the Continental United States
BRI	Basic Rate Interface	ETSI	European Telecommunications Standards Institute	PBX1	Private Branch Exchange Type 1 (MLPP Capable)
C	Conditional	ISDN	Integrated Services Digital Network	PBX2	Private Branch Exchange Type 2 (Non-MLPP Capable)
CAS	Channel Associated Signaling	ITU-T	International Telecommunications Union – Telecommunication Standardization Sector	PRI	Primary Rate Interface
COTS	Commerical Off-the-Shelf	MF	Multifrequency	R	ROUTINE
DP	Dial Pulse	MFS	Multifunction Switch	SMEO	Small End Office
DTMF	Dual-Tone Multifrequency	NI-1/2	National ISDN 1/2	SS7	Signaling System No. 7
DVX	Deployable Voice Exchange			TS	Tandem Switch
DVX-C	Deployable Voice Exchange – COTS				
DVX-L	Deployable Voice Exchange – Legacy				

5.2.1 Capabilities and Features

5.2.1.0 Introduction

This section defines UCR 2008 circuit-switched system capabilities and features. Not all features and capabilities listed in this section are required for all DSN switching systems. The applicability of a particular capability or feature to a type of switch is shown in brackets at the start of each feature description.

5.2.1.1 Features Common to Single Users and Business Customers

Features common to residence and business customers are based on features found in Telcordia Technologies GR-520-CORE, *Features Common to Residence and Business*, Issue 1, June 2000.

5.2.1.1.1 Individual Line

[Required: EOS, MFS, SMEO, DVX-C, DVX-L, PBX1, PBX2] An individual line is a line arranged to serve only one main station, although additional stations may be connected to the line as extensions of the main station. The system shall be capable of automatically identifying the directory number (DN) assigned to a line based on the originating appearance to the system. Service-related features such as manual originating, dial-pulse (DP) dialing, or dual-tone multifrequency (DTMF) dialing assigned to individual lines may vary from line to line in a switch.

5.2.1.1.2 CLASS^{SM} Feature: Selective Call Rejection

[Conditional: EOS, DVX-C, DVX-L, MFS] The CLASS^{SM} Feature: Selective Call Rejection (SCR) is conditional because it interacts with MLPP. A DSN call above the ROUTINE precedence shall not be rejected if this feature is activated. Procuring agencies specifying this feature shall supply the rejection announcement for their local customers. This feature allows customers to block subsequent calls from a calling directory number after receiving a harassing call. After receiving an undesired call, the customer dials a code that places the last calling party's directory number on a list for rejection. Subsequent calls from the rejected party are intercepted and routed to an announcement. In addition, this feature enables customers to enter additional directory numbers onto the list.

If this feature is provided, it shall be in accordance with Telcordia Technologies GR-218-CORE, *CLASS^{SM} Feature: Selective Call Rejection*, Issue 1, June 2000.

5.2.1.1.3 Denied Originating Service

[Conditional: EOS, MFS, SMEO, DVX-C, DVX-L, PBX1] The Denied Originating Service feature is conditional because C2 users could be denied originating service. The feature does not directly interact with MLPP, but operational controls must ensure that C2 users are not denied originating service.

Denied originating is a system feature that provides the capability to deny call originations selectively to individual lines.

If this feature is provided, it shall be in accordance with Telcordia Technologies GR-562-CORE, *Manual Line Features*, Issue 1, June 2000.

5.2.1.1.4 Code Restriction and Diversion

[Required: EOS, MFS, SMEO, DVX-C – Conditional: DVX-L, PBX1] Code restriction and diversion destination limitations on calls provide originated at designated lines to specified codes (i.e., to include Numbering Plan Area).

5.2.1.1.5 Call Waiting Features

5.2.1.1.5.1 Call Waiting

[Required: EOS, SMEO, DVX-C, MFS, PBX1 – Conditional: DVX-L] The Call Waiting (CW) feature interacts with MLPP. The MLPP interaction requirements are found in Section 5.2.2, Multilevel Precedence and Preemption. The switch must provide the DSN precedence call waiting tone.

Call Waiting is a feature whereby a line in the talking state is alerted by a call waiting tone when another call is attempting to complete to that line. The call waiting tone is only audible to the line with the Call Waiting feature activated. Audible ringing is returned to the originating line. The service also provides a hold feature that is activated by a switchhook flash. Consecutive flashes allow the customer (with the service activated) to alternately talk to the original and the new calling party. If the customer with the service activated hangs up while one party is on hold, the customer with the service activated is automatically rung back, and upon answer is connected to the held party.

If this feature is provided, it shall be in accordance with Telcordia Technologies GR-571-CORE, *Call Waiting*, Issue 1, June 2000.

5.2.1.1.5.2 Cancel Call Waiting

[Required: EOS, MFS, SMEO, DVX-C, PBX1 – CONDITIONAL: DVX-L] The Cancel Call Waiting feature is required when call waiting is active. The user must be able to cancel the call waiting service. Cancel call waiting is a feature that allows the customer with the Call Waiting service to inhibit the operation of call waiting for one call. The customer dials the cancel call waiting code, obtains recall dial tone, and places a call normally. During this call, the Call Waiting service shall be inactive so that anyone calling the call waiting customer shall receive the normal busy treatment, and no call waiting tones shall interrupt the customer's call.

If this feature is provided, it shall be in accordance with Telcordia Technologies GR-572-CORE, *Call Waiting,* Issue 1, June 2000.

5.2.1.1.6 Three-Way Calling

[Required: EOS, MFS, SMEO, DVX-C, PBX1 – Conditional: DVX-L] The Three-Way Calling (TWC) feature interacts with MLPP. See Section 5.2.2.8.5, Three-Way Calling, for specific MLPP interaction requirements.

Three-Way Calling is a feature that allows a station in the talking state to add a third party to the call without operator assistance. To add a third party to the call, the TWC customer flashes the switchhook once to place the other party on hold, receives recall dial tone, dials the third party's telephone number, and then flashes the switchhook again to establish the TWC connection. The second switchhook flash may occur any time after the completion of dialing. After the TWC connection has been established, the customer with the service activated may disconnect the last party added by a single switchhook flash or by depressing a feature key. The customer with the service activated may terminate the TWC call by disconnecting. If either of the other two parties hangs up while the service-activating customer remains off-hook, the TWC is returned to a two-party connection between the remaining parties.

If this feature is provided, it shall be in accordance with Telcordia Technologies GR-577-CORE, *Three-Way Calling,* Issue 1, June 2000.

5.2.1.1.7 Add-On Transfer and Conference Calling Features

[Conditional: EOS, MFS, SMEO, PBX1 DVX-C, DVX-L] The Add-On Transfer and Conference Calling features are conditional because they interact with MLPP.

The feature set provides the user with the capabilities to handle more than one call at a time on a given line. The capability to hold a call and originate an additional call (Call Hold); the capability to form a three-way conference ((add-on) TWC); the capability to redirect a call to

another line (Call Transfer); and the capability to create a larger conference (Conference Calling Six Way Station Controlled) shall be included in this feature.

If this feature is provided, it shall be in accordance with Telcordia Technologies GR-579-CORE, *Add-on Transfer and Conference Calling Features*, Issue 1, June 2000. References to the Public Switched Telephone Network (PSTN) in GR-579-CORE are interpreted as the DSN.

5.2.1.1.7.1 Call Transfer Individual – All Calls

[Required: EOS, MFS, SMEO, DVX-C, PBX1 – CONDITIONAL: DVX-L] The Call Transfer Individual – All Calls feature interacts with MLPP. See Section 5.2.2.8.3, Call Transfer, for specific MLPP interaction requirements.

If this feature is provided, it shall be in accordance with Telcordia Technologies GR-579-CORE, *Add-on Transfer and Conference Calling Features,* Issue 1, June 2000.

5.2.1.1.7.2 Call Transfer – Internal Only

[Required: EOS, MFS, SMEO, DVX-C, PBX1 – CONDITIONAL: DVX-L] The Call Transfer – Internal Only feature interacts with MLPP. See Section 5.2.2.8.3, Call Transfer, for specific MLPP interaction requirements. This service is a restricted form of the Call Transfer Individual – All Calls feature but does not allow transfer to lines reached via the network.

If this feature is provided, it shall be in accordance with Telcordia Technologies GR-579-CORE, *Add-on Transfer and Conference Calling Features,* Issue 1, June 2000.

5.2.1.1.7.3 Call Transfer – Individual – Incoming Only/Add-On Consultation Hold – Incoming Only

[Required: EOS, MFS, SMEO, DVX-C, PBX1 – CONDITIONAL: DVX-L] The Call Transfer – Individual – Incoming Only/Add-On Consultation Hold – Incoming Only feature interacts with MLPP. See Section 5.2.2.8.3, Call Transfer, for specific MLPP interaction requirements. This feature is a version of the Call Transfer Individual – All Calls feature that may be applied only to calls incoming to the business group from the network.

If this feature is provided, it shall be in accordance with Telcordia Technologies GR-579-CORE, *Add-on Transfer and Conference Calling Features,* Issue 1, June 2000.

5.2.1.1.7.4 Call Transfer – Outside

[Required: EOS, MFS, SMEO, DVX-C, PBX1 – CONDITIONAL: DVX-L] The Call Transfer – Outside feature interacts with MLPP. See Section 5.2.2.8.3, Call Transfer, for specific MLPP interaction requirements. This feature is a version of the Call Transfer Individual – All Calls feature to transfer a call to lines reached via the network.

If this feature is provided, it shall be in accordance with Telcordia Technologies GR-579-CORE, *Add-on Transfer and Conference Calling Features,* Issue 1, June 2000.

5.2.1.1.7.5 Call Transfer – Add-On to Fully Restricted Station

[Conditional: EOS, MFS, SMEO, DVX-C, DVX-L, PBX1] The Call Transfer – Add-On to Fully Restricted Station feature is conditional because it interacts with MLPP. See Section 5.2.2.8.3, Call Transfer, for specific MLPP interaction requirements. This feature allows consultation with a fully restricted station on a call incoming or outgoing from the business group, but it restricts conference and transfer capabilities to situations in which the original call would have been allowed for a fully restricted line.

If this feature is provided, it shall be in accordance with Telcordia Technologies GR-579-CORE, *Add-on Transfer and Conference Calling Features,* Issue 1, June 2000.

5.2.1.1.7.6 Call Transfer Attendant

[Conditional: EOS, MFS, SMEO, DVX-C, DVX-L, PBX1] The Call Transfer Attendant feature is conditional because it interacts with MLPP. See Section 5.2.2.8.3, Call Transfer, for specific MLPP interaction requirements. This feature provides a restricted transfer capability. Only calls incoming to the business group from the network may be transferred, and only to the business group attendant. Users can reach the attendant to request the transfer by either flashing, or by flashing and dialing 0.

If this feature is provided, it shall be in accordance with Telcordia Technologies GR-579-CORE, *Add-on Transfer and Conference Calling Features,* Issue 1, June 2000.

5.2.1.1.7.7 Call Hold

[Required: EOS, MFS, SMEO, PBX1 – CONDITIONAL: DVX-C, DVX-L] The Call Hold feature interacts with MLPP. See Section 5.2.2.8.4, Call Hold, for specific MLPP interaction requirements. This feature provides the capability for the user to hold a call for an extended period, and then return to the call, with or without making another call.

If this feature is provided, it shall be in accordance with Telcordia Technologies GR-579-CORE, *Add-on Transfer and Conference Calling Features,* Issue 1, June 2000.

5.2.1.1.7.8 Conference Calling – Six-Way Station Controlled

[Conditional: EOS, MFS, SMEO, DVX-C, DVX-L, PBX1] The Conference Calling – Six-Way Station Controlled feature is conditional because it interacts with MLPP. See Section 5.2.2.8.5, Three-Way Calling, for specific MLPP interaction requirements. This feature allows the user to establish a conference call involving up to six conferees (including the user). This feature is requested via an access code.

If this feature is provided, it shall be in accordance with Telcordia Technologies GR-579-CORE, *Add-on Transfer and Conference Calling Features,* Issue 1, June 2000.

5.2.1.1.8 Call Forwarding Features and Call Forwarding Subfeatures

5.2.1.1.8.1 Call Forwarding Variable

[Required: EOS, MFS, SMEO, DVX-C, PBX1 – CONDITIONAL: DVX-L] The Call Forwarding Variable feature interacts with MLPP. See Section 5.2.2.8.2.1, Call Forwarding at a Busy Station, for specific MLPP interaction requirements.

With this feature, ROUTINE precedence calls attempting to terminate to a line are redirected to another customer-specified line served by the same office or by another office for DSN and/or commercial. The customer activates and deactivates the forwarding function and specifies the desired terminating address (DSN and/or commercial) during each activation procedure. When activated, calls forwarded while the line is idle cause a short (about 0.5 second) ring on the forwarding line as a reminder that the service is active. The user cannot answer the call while this feature is active, but can originate calls.

If this feature is provided, it shall be in accordance with Telcordia Technologies GR-580-CORE, *Call Forwarding Variable,* Issue 1, June 2000.

5.2.1.1.8.2 Call Forwarding Busy Line

[Required: EOS, MFS, SMEO, DVX-C, PBX1 – CONDITIONAL: DVX-L] The Call Forwarding Busy Line (CFBL) feature interacts with MLPP. See Section 5.2.2.8.2.1, Call Forwarding at a Busy Station, for specific MLPP interaction requirements.

The CFBL feature provides the capability to associate with a given line another line to which calls shall be forwarded when the given line is busy. This capability applies to lines within the same business group, within the same switch, or within the network.

If this feature is provided, it shall be in accordance with Telcordia Technologies GR-586-CORE, *Call Forwarding Subfeatures*, Issue 1, June 2000.

5.2.1.1.8.3 Call Forwarding – Don't Answer – All Calls

[Required: EOS, MFS, SMEO, DVX-C, PBX1 – CONDITIONAL: DVX-L] The Call Forwarding – Don't Answer – All Calls feature interacts with MLPP. See Section 5.2.2.8.2.1, Call Forwarding at a Busy Station, and Section 5.2.2.8.2.2, Call Forwarding – No Reply at Called Station, for specific MLPP interaction requirements.

This feature allows calls terminating to an idle station to ring that station a customer-specified number of ringing cycles, and if the call is not answered, then route to another station within the same switching system. If the station to which the call is to be routed is busy, the original station continues to ring until the originator of the call abandons it or the call is answered.

If this feature is provided, it shall be in accordance with Telcordia Technologies GR-586-CORE, *Call Forwarding Subfeatures*, Issue 1, June 2000.

5.2.1.1.8.4 CLASS^{SM} Feature: Selective Call Forwarding

[Conditional: EOS, MFS, SMEO, DVX-C, DVX-L, PBX1] The CLASS^{SM} Feature: Selective Call Forwarding (SCF) feature is conditional because it interacts with MLPP. See Section 5.2.2.8.2.1, Call Forwarding at a Busy Station, and Section 5.2.2.8.2.2, Call Forwarding – No Reply at Called Station, for specific MLPP interaction requirements.

This feature allows customers to have only calls from selected calling parties forwarded. The SCF customer specifies the callers who are to receive special treatment by including their directory numbers on a screening list. If a call is placed from a directory number on the customer's SCF screening list, the call shall be forwarded to the remote station.

If this feature is provided, it shall be in accordance with Telcordia Technologies GR-217-CORE, *CLASS^{SM} Feature: Selective Call Forwarding*, Issue 1, June 2000.

5.2.1.1.9 Call Pick-Up Features

5.2.1.1.9.1 Call Pick-Up

[Conditional: EOS, MFS, SMEO, DVX-C, DVX-L, PBX1] The Call Pick-Up feature is conditional because it interacts with MLPP. See Section 5.2.2.8.6, Call Pick-Up, for specific MLPP interaction requirements.

A station may answer a call that has been terminated to another station in its common call pick-up group in a business group. This is accomplished by dialing a pick-up access code while the called station is being rung. If more than one station in the group is being rung, the station that has been ringing longer shall be picked up first.

If this feature is provided, it shall be in accordance with Telcordia Technologies GR-590-CORE, *LSSGR: Call Pickup Features*, Issue 1, June 2000.

5.2.1.1.9.2 Directed Call Pick-Up

[Conditional: EOS, MFS, SMEO, DVX-C, DVX-L, PBX1] The Directed Call Pick-Up feature is conditional because it interacts with MLPP. See Section 5.2.2.8.6, Call Pick-Up, for specific MLPP interaction requirements.

Directed call pick-up permits a user to dial a code and station number and pick up a call that has been answered or is ringing at another telephone, provided the rung telephone permits dial pick-up. If the other station has answered, a TWC is established.

If this feature is provided, it shall be in accordance with Telcordia Technologies GR-590-CORE, *LSSGR: Call Pickup Features,* Issue 1, June 2000.

5.2.1.1.9.3 Directed Call Pick-Up without Barge-In

[Conditional: EOS, MFS, SMEO, DVX-C, DVX-L, PBX1] The Directed Call Pick-Up without Barge-In feature is conditional because it interacts with MLPP. See Section 5.2.2.8.6, Call Pick-Up, for specific MLPP interaction requirements.

This feature is identical to the Directed Call Pick-Up feature, except that if the line being picked up has already answered, the party dialing the pick-up code shall be routed to reorder rather than be permitted to barge in on the established connection to create a TWC.

If this feature is provided, it shall be in accordance with Telcordia Technologies GR-590-CORE, *LSSGR: Call Pickup Features*, Issue 1, June 2000.

5.2.1.2 Attendant Features

Attendant features in this section apply to attendant consoles that are provided with the local switch and/or centralized attendant services.

5.2.1.2.1 Precedence and Preemption

[Required: MFS, EOS – Conditional: SMEO, DVX-C, DVX-L, PBX1] The attendant console shall interoperate with MLPP as described in Section 5.2.2, Multilevel Precedence and Preemption. The console shall be able to initiate all levels of precedence calls (i.e., ROUTINE through FLASH-OVERRIDE).

5.2.1.2.2 Call Display

[Required: MFS, EOS – Conditional: SMEO, DVX-C, DVX-L, PBX1] The attendant console shall provide a visual display of each precedence level, the calling number, and class of service for incoming direct dialed calls and diverted calls to the attendant.

5.2.1.2.3 Class of Service Override

[Required: MFS, EOS – Conditional: SMEO, DVX-C, DVX-L, PBX1] The attendant shall provide the capability to override any class of service (calling area or precedence) of the calling party on a call-by-call basis.

5.2.1.2.4 Busy Override and Busy Verification

[Required: MFS, EOS – Conditional: SMEO, DVX-C, DVX-L, PBX1] The attendant shall have the capability to override a busy line condition. If the called line being verified is busy, off-hook supervision shall be given to the attendant performing the busy verification. When a verification code is used, all digits of the code must be dialed before cut-through to the line can be accomplished. Connections to commercial Central Office access lines shall be restricted from busy verification access. The attendant shall have the capability to enter an existing busy line to inform the user of an incoming call. An override tone shall be provided to the busy line prior to the attendant entering the conversation, and the tone shall be repeated periodically as long as the attendant is connected. Selected stations may be classmarked to deny attendant break-in. In particular, it shall be possible to classmark the lines of selected stations (e.g., all data and secure voice) to preclude the busy verification or busy override being applied to the selected station lines.

5.2.1.2.5 Night Service

[Required: MFS, EOS – Conditional: SMEO, DVX-C, DVX-L, PBX1] The attendant console shall have the ability to route all calls normally directed to the console to a night service deflection. The night service deflection shall be a fixed or manually selected directory number.

5.2.1.2.6 Automatic Recall of Attendant

[Required: MFS, EOS – Conditional: SMEO, DVX-C, DVX-L, PBX1] When an attendant extends a call to a station that is busy or does not answer within a preset time, the extended party shall be recalled automatically to the console. Recalls shall be transferred to the console that originally processed the call. If that console is busy, the recall shall be placed into the console queue; but if the console is out of service, the recall shall be routed to another console.

5.2.1.2.7 Calls in Queue to the Attendant

[Required: MFS, EOS – Conditional: SMEO, DVX-C, DVX-L, PBX1] The attendant console shall have the capability to place calls in a waiting queue. Calls placed in queue to the attendant console shall be retrieved by the attendant in order of precedence level (i.e., FLASH-OVERRIDE first, ROUTINE last) and longest holding time. Calls in queue shall not be lost when a console is placed out of service or forwarded to night service deflection. When the console is placed out of service or forwarded to night service while calls are in queue, the console shall be capable of one of the following solutions:

1. All calls in queue shall be forwarded first to the centralized attendant, and then night service, or

2. All subsequent calls placed to the attendant console shall be forwarded first to the centralized attendant, and then night service. The attendant console shall be able to answer all remaining calls in queue preventing any calls from being lost.

5.2.1.2.8 Release to Pivot for Operator Services

[Required: MFS, EOS – Conditional: SMEO, PBX1] The Release to Pivot (RTP) for Operator Services capability shall conform to Telcordia Technologies SR-2275, Section 6, Signaling; and Feature Service Description (FSD) 30-33-0000. The RTP network capability is a network routing capability that consists of a collection of call setup procedures that provides flexibility to a TS/MFS/EO-type switch to determine conditions for either forwarding a call or releasing it back to a previous switch in the call path. The RTP is a network capability that is invoked in support of service or business needs, and not invoked directly by an end user. The RTP network capability permits an operator services switch, after it has determined a new

destination for the call, to have the connection established from the originating switch. The basic capability allows any switch to indicate to switches farther forward in the call path that it has the ability to pivot the call. Then an application that determines the new destination for the call (in this case, the operator services switch) can release the call with a Redirection Number parameter containing the address of the new destination. The pivot switch (in this case, the originating switch) will not terminate the call on receipt of the release message, but will pass the call forward toward the new destination. The result is that the release switch, which determined the new destination, saves an incoming and an outgoing trunk relative to the case where the call is forwarded to the new destination. Basic RTP uses the Signaling System No. 7 (SS7) to perform the following:

1. Redirect Capability parameter to indicate support for the capability.

2. Redirect Counter parameter to prevent looping of a call among a set of switches invoking the capability.

3. Release Cause value 23 to indicate RTP caused the release. (Other values are also allowed.)

Additional SS7 parameters have been defined to allow future expansion of the use of RTP by operator services, including:

1. Redirect Status parameter to allow the operator system to acknowledge receipt of the offer to perform RTP from the originating switch.

2. Redirect Forward Information parameter to carry additional information in the forward direction.

3. Redirect Backward Information parameter to carry additional information in the backward direction.

5.2.1.3 Customer Access Interfaces

5.2.1.3.1 PBX Line

[Required: MFS, EOS – Conditional: SMEO, DVX-C, DVX-L, PBX1] The PBX Line interface is required but the type of interface is conditional because it is not required for all DSN switches, and recognizes that PBXs may be interfaced with DSN switches using other interfaces. Each MILDEP acquisition agent is responsible for specifying the type of PBX interfaces required at the base, post, camp, station (B/P/C/S), or facility location.

A PBX line is a line appearance at the local switching system that permits connection to a customer premise switching system. The connecting facility may be 1- or 2-way, and it may be loop start or ground start. A PBX line is like an individual line except for ringback, power cross test, and permanent signal treatment.

If this feature is provided, it shall be in accordance with Telcordia Technologies GR-524-CORE, *LSSGR: Attendant and Customer Switching System Features and Customer Interfaces, PBX Line,* Issue 1, FSD 04-01-0000, June 2000.

5.2.1.3.2 Direct Inward Dialing

[Required: MFS, EOS – Conditional: SMEO, DVX-C, DVX-L, PBX1] The Direct Inward Dialing (DID) interface is required for MFS and End Office Switch (EOS) and conditional for all other DSN switches, and, recognizes that PBXs may be interfaced with DSN switches using other interfaces. Each MILDEP acquisition agent is responsible for specifying the type of PBX interfaces required at the B/P/C/S, or facility location.

This feature allows an incoming call to reach a specific PBX station line without attendant assistance. With DID, the switch seizes a DID trunk and outpulses the station line number to the PBX. If the called station's line is idle and not restricted from receiving terminating calls, the PBX alerts the called station and returns audible ringing on the incoming connection. If the called station's line is busy, the PBX returns busy tone. If the called station is restricted from receiving terminating calls, the PBX routes the incoming call to an announcement, reorder tone, or to the attendant.

If this feature is provided, it shall be in accordance with Telcordia Technologies GR-524-CORE, *LSSGR: Attendant and Customer Switching System Features and Customer Interfaces, PBX Line,* Issue 1, FSD 04-02-0000, June 2000.

5.2.1.3.3 National ISDN 1/2 Basic Access

[Required: EOS, MFS, SMEO – Conditional: DVX-C, PBX1, PBX2] The switch shall include both S/T and U interfaces for Integrated Services Digital Network (ISDN) Basic Access. The ISDN Basic Access interface allows the simultaneous transmission of voice, circuit-switched data, and packet data over a single customer line connecting Customer Premises Equipment (CPE) and a digital switch. Specifically, the ISDN Basic Access allows the provisioning of two 64-kilobits per second (kbps) B channels, which may be used to carry voice, circuit-switched data, or packet data, and a 16-kbps D channel, which can carry signaling and packet information.

Requirements for this feature shall be in accordance with Telcordia Technologies references SR-NWT-002120, SR-NWT-002343, and TR-NWT-001268.

The MLPP service capability requirements for this interface shall be in accordance with American National Standards Institute (ANSI) T1.619-1992 (R1999) and ANSI T1.619a-1994 (R1999), "Multi-Level Precedence and Preemption (MLPP) Service, ISDN Supplementary Service Description."

5.2.1.3.4 ISDN Primary Access

5.2.1.3.4.1 National ISDN 1/2 Primary Access

[Required: TS, EOS, MFS, SMEO, DVX-C, PBX1 – Conditional: PBX2] The ISDN Primary Access interface is an ISDN user-network interface in which the interface structure is composed of multiple B channels and one D channel. The bit rate of the D channel in this structure is 64 kbps. When a 1544-kbps Primary Rate Interface (PRI) is provided, the interface structure is 23B+1D.

Requirements for this feature shall be in accordance with Telcordia Technologies SR-NWT-002120, SR-NWT-002343, and TR-NWT-001268. The DSN user-to-network signaling physical layer specification for the PRI operating at 1.544 megabits per second (Mbps) shall be ANSI T1.408.

5.2.1.3.4.1.1 ISDN ANSI MLPP Service Capability

[Required: TS, EOS, MFS, SMEO, DVX-C, PBX1 – Conditional: PBX2] The ISDN ANSI MLPP service capability shall be in accordance with ANSI Standards T1.619-1992 and T1.619a-1994.

5.2.1.3.4.2 ITU-T ISDN Primary Access

[Required: TS, EOS, MFS (OCONUS Locations Using ETSI Standards) – Conditional: SMEO, DVX-C, PBX1, PBX2] Requirements for the Primary Rate User-Network interface shall be in accordance with International Telecommunication Union (ITU) Recommendation I.431, "Primary Rate User-Network Interface – Layer 1 Specification," as required for outside the continental United States (OCONUS) applications. The DSN user-to-network signaling requirement for the PRI operating at 2.048 Mbps shall be ITU Recommendation I.431.

5.2.1.3.4.2.1 ITU-T ISDN Promary Access Digital Subsciber Signaling System Number 1 MLPP

[Required: TS, EOS, MFS (OCONUS Locations Using ETSI Standards) – Conditional: SMEO, DVX-C, PBX1, PBX2] The ITU-T ISDN Primary Access MLPP shall be in accordance with ITU-T Recommendation Q.955.3 (1993), "Description for community of interest supplementary services using DSS1 – Multilevel precedence and preemption (MLPP)."

5.2.1.3.5 Analog Line

[Required: EOS, MFS, SMEO, DVX-C, DVX-L, PBX1 – Conditional: PBX2] The analog line interface is required for all DSN switches.

Requirements for this feature shall be in accordance with Telcordia Technologies GR-510-CORE, *System Interfaces*, Issue 1, June 2000.

5.2.1.4 Public Safety Features

5.2.1.4.1 911 Service

5.2.1.4.1.1 Emergency Service (911) Calls

The 911 Emergency Service feature provides a 3-digit universal telephone number (911) that gives the caller access to help and support from an emergency service bureau.

[Required: EOS, MFS, SMEO, PBX1, PBX2 – CONDITIONAL: DVX-C, DVX-L] If the 911 caller can access multiple networks (e.g., DSN, Federal Technology Service (FTS), PSTN), the calling number delivered to the service bureau shall be only one number, decided upon by the requirements of the service bureau, regardless of which network the call was originated on. The calling number may be delivered by Automatic Number Identification (ANI) (Channel Associated Signaling (CAS)), Calling Number Delivery (non-CAS), or Calling Line Identifier (CLID) for individual lines.

5.2.1.4.1.2 Emergency Service (911) Public Safety Answering Point

The emergency service is a one-way only, terminating service. The service bureau is usually called a Public Safety Answering Point (PSAP) and may be located within a police department, a fire department, or in an independent agency serving as a communications center. Based on security control requirements for a military installation, the PSAP for the 911 service may be operated within the B/P/C/S or shared with the local community's PSAP.

[Conditional: EOS, MFS, SMEO, DVX-C, PBX1, PBX2] When the originating line and the emergency service bureau are served by the same switching system, the bureau shall have the capability of:

- Holding and releasing the calling line connection
- Monitoring the supervisory state of the calling line
- Ringing the originating station back

If the PSAP and the 911 caller are served by different switches, the ability to hold the trunk up, maintain supervision, and provide ringback will be determined by both the switch capability and the trunk type used to tandem the 911 call.

If the PSAP receives calls on older analog trunks, they may be centralized automatic message accounting (CAMA) circuits. These circuits are formatted to pass the calling party number. If the PSAP receives calls on older-style digital trunks, they are specially formatted multifrequency trunks that pass ANI only. If the PSAP receives calls on ISDN User Part (ISUP) trunks controlled by the SS7 protocol, the calling party number is present in the SS7 setup message. The Charge Number parameter contains the ANI.

The PSAP trunking does not pass any other address information along with the call, only the calling party number is passed.

An Automatic Location Identification (ALI) Failure happens when the telephone number is not passed or when the telephone number is not in the ALI database. If this happens, the call is passed to the trunk group's default Extended Sequence Number (ESN), which is a PSAP designated for this function. The PSAP operator must ask the incoming call for its location and redirect it to the correct PSAP.

[Conditional: EOS, MFS, SMEO, DVX-C, PBX1, PBX2] If this feature is provided, it shall be in accordance with Telcordia Technologies GR-529-CORE, *Public Safety*, Issue 1, June 2000.

[Required: MFS, EOS, SMEO, PBX1, PBX2 – CONDITIONAL: DVX-C] The PSAP shall not be able to place callers to 911 on hold while connected to the 911 termination.

5.2.1.4.1.3 Enhanced Emergency Service (E911)

[Conditional: EOS, MFS, SMEO, DVX-C, PBX1, PBX2] If Enhanced Emergency Service (E911) is provided, the following conditions apply:

1. Enhanced 911 or E911 service is a North American telephone network (North American Numbering Plan (NANP)) feature of the 911 emergency calling system that automatically

associates a physical address with the calling party's telephone number. Computer software makes an association between the caller line identification number and an address, which provides emergency responders with the location of the emergency call caller's location without the person calling for help having to provide it.

2. Normally, the 911 caller's provided location information is integrated into an emergency dispatch center's computer-assisted dispatch (CAD) system, to provide the dispatcher with an on-screen street map that highlights the caller's position and the nearest available emergency responders. This is done by a form of reverse telephone directory that is supplied by the service provider as a computerized file.

3. The PSAP uses the calling party number to look up the address in the ALI database. The ALI database is secured and separate from the public telephone network by design. The information is gathered by mapping the calling telephone number to an address. The database is maintained by the service provider under contract with the PSAP. Each service provider has its own standards for the formatting of the database. Most ALI databases have a companion database known as the Master Street Address Guide (MSAG). The MSAG describes the exact spelling of streets, street number ranges, and other address elements.

[Required: MFS, EOS, SMEO, PBX1, PBX2 – CONDITIONAL: DVX-C] The PSAP shall not be able to place callers to 911 on hold while connected to the 911 termination.

[Conditional: EOS, MFS, SMEO, DVX-C, PBX1, PBX2] For Wireline E911, the location is a physical address. For Wireless E911, the location could be an address or a coordinate (i.e., specific latitude and longitude location information, known as ALI). Not all PSAPs have the Wireless and Wireline systems integrated.

If these features are provided, the calling party number shall be processed in accordance with Telcordia Technologies GR-529-CORE, *Public Safety*, Issue 1, June 2000, and Telcordia Technologies Generic FR-E911-1, *Requirements to Support E9-1-1 Service*, Issue 5, January 2007.

5.2.1.4.2 Tracing of Terminating Calls

[Required: EOS, MFS, SMEO, DVX-C – Conditional: PBX1, DVX-L] The Tracing of Terminating Calls feature identifies the calling number on intraoffice calls or the incoming trunk on incoming calls for calls terminating to a specified directory number. When this feature is activated, a printout of the originating directory number or incoming trunk number, terminating directory number, and the time and date is generated for every call to the specified line.

Requirements for this feature shall be in accordance with Telcordia Technologies GR-529-CORE, *Public Safety,* Issue 1, FSD 15-03-0000, June 2000.

5.2.1.4.3 Outgoing Call Tracing

[Required: EOS, MFS, SMEO, DVX-C – Conditional: PBX1, DVX-L] The Outgoing Call Tracing feature allows the tracing of nuisance calls to a specified directory number suspected of originating from a given local office. The tracing is activated when the specified directory number is entered. A printout of the originating directory number, outgoing trunk number, or terminating number, and the time and date is generated for every call to the specified directory number.

Requirements for this feature shall be in accordance with Telcordia Technologies GR-529-CORE, *Public Safety,* Issue 1, FSD 15-03-0000, June 2000.

5.2.1.4.4 Tandem Call Trace

[Required: EOS, MFS, SMEO, DVX-C, TS – Conditional: DVX-L] The Tandem Call Trace feature identifies the incoming trunk of a tandem call to a specified office directory number. The feature is activated by entering the specified distant office directory number for a tandem call trace. A printout of the incoming trunk number and terminating directory number, and the time and date is generated for every call to the specified directory number.

Requirements for this feature shall be in accordance with Telcordia Technologies GR-529-CORE, *Public Safety,* Issue 1, FSD 15-03-0000, June 2000.

5.2.1.4.5 Trace a Call in Progress

[Required: TS, EOS, MFS, SMEO, DVX-C – Conditional: DVX-L] The Trace a Call in Progress feature identifies the originating directory number or incoming trunk for a call in progress. The feature is activated by authorized personnel entering a request that includes the specific terminating directory number or trunk involved in the call.

Requirements for this feature shall be in accordance with Telcordia Technologies GR-529-CORE, *Public Safety,* Issue 1, FSD 15-03-0000, June 2000.

5.2.1.5 Trunk, Line, and Special Service Circuit Service Test Features

The majority of the capabilities listed in this section do not have an FSD in the LSSGR. These capabilities are definitions only in Section 2 of the LSSGR. However, the capabilities may be provided on a local basis to enhance assured services.

5.2.1.5.1 Local Office Test Lines

Test lines shall be provided for testing lines and incoming trunks from connecting offices. The transmission test lines listed in the following paragraphs may be used for tandem applications also.

5.2.1.5.1.1 100-Type Test Line

[Required: TS, EOS, MFS – Conditional: SMEO, DVX-C, DVX-L] A 100-type test line provides a local office with equipment that first applies a precise (1004 Hertz (Hz) at 1 milliwatt (mW)) tone for a timed period, and then a balanced termination for transmission level and noise measurements. Line and trunk access shall be provided to the 100-type test line.

5.2.1.5.1.2 101-Type Test Line

[Required: TS, EOS, MFS – Conditional: SMEO, DVX-C, DVX-L] A 101-type test line provides a communication line to a craftsperson's position.

5.2.1.5.1.3 102-Type Test Line

[Required: TS, EOS, MFS – Conditional: SMEO, DVX-C, DVX-L] A 102-type test line applies a precise (1004 Hz at 1 mW) tone for approximately 9 seconds on and 1 second off, in a repetitive sequence.

5.2.1.5.1.4 105-Type Test Line

[Required: TS, EOS, MFS – Conditional: SMEO, DVX-C, DVX-L] A 105-type test line, with responder, provides for automatic two-way loss and noise measurements, plus gain slope, return loss, and noise in the presence of tone-on trunks requiring transmission testing.

5.2.1.5.1.5 Synchronous Test Line

[Required: TS, EOS, MFS – Conditional: SMEO, DVX-C, DVX-L] A synchronous test line provides diagnostic tests of incoming trunk equipment. Six supervisory pulses are returned.

5.2.1.5.1.6 Non-Synchronous Test Line

[Required: TS, EOS, MFS – Conditional: SMEO, DVX-C, DVX-L] A non-synchronous test line tests incoming trunk equipment. Supervisory pulses are repeated until disconnection takes place.

5.2.1.5.1.7 Permanent Busy Test Line

[Required: TS, EOS, MFS – Conditional: SMEO, DVX-C, DVX-L] A permanent busy test line shall return a permanent busy signal.

5.2.1.5.1.8 108-Type Test Line

[Required: TS, EOS, MFS – Conditional: SMEO, DVX-C, DVX-L] A 108-type test line provides a non-inverting loopback for digital testing between digital exchanges and/or digital PBXs. The test line accepts and loops back received octets that are retransmitted so that the positions of the bits within the octets are preserved. All digital services (e.g., 56 kbps, 64 kbps restricted, and 64 kbps clear) can pass digital test signals over this test line.

5.2.1.5.2 Outside Plant Test Lines

5.2.1.5.2.1 Dialable Cable Pair Locator Tone

[Conditional: EOS, SMEO, DVX-C, DVX-L, MFS] The Dialable Cable Pair Locator Tone feature is designed to give the field technician the capability via a secured dial-up access to apply identification tone to a single subscriber loop. This feature eliminates the involvement of the mainframe personnel in applying the identification tone on working subscriber lines.

If this feature is provided, it shall be in accordance with Telcordia Technologies GR-533-CORE, *Database Services Service Switching Points,* Issue 1, June 2000.

5.2.1.5.2.2 DTMF Station Test Circuit

[Required: EOS, MFS – Conditional: SMEO, DVX-C, DVX-L] The DTMF Station Test Circuit provides the capability for an installer (or a customer assisted by test desk personnel) to test the station ringer and directory number line assignment in the Central Office. In addition, it shall be possible to test DTMF stations including 12-button sets and repertory dialers.

5.2.1.5.3 Test Incoming Trunks in Tandem or Local State

[Conditional: TS, EOS, SMEO, DVX-C, DVX-L, MFS] The system shall provide the ability to place incoming trunks in the local or tandem state on incoming calls to 100-, 102-, and 105-type test lines. The choice of state shall be based on the directory number received from the originating office.

5.2.1.5.4 Manual Testing

5.2.1.5.4.1 Manual Test of Line

5.2.1.5.4.1.1 Basic Line Test Capabilities

[Required: EOS, MFS, SMEO, PBX1 – CONDITIONAL: DVX-C, DVX-L] The Basic Line Test Capabilities feature provides a craftsperson at a Trunk Line Workstation (TLWS), or at another local test position interfacing with the switching system, with basic line maintenance capabilities, such as removing lines from service, restoring lines to service, and verifying the status of lines.

5.2.1.5.4.1.2 Advanced Line Test Capabilities

[Required: EOS, MFS – Conditional: SMEO, DVX-C, DVX-L , PBX1] The Advanced Line Test Capabilities feature includes advanced line capabilities, such as resistance, leakage and current measurements, and ringing.

5.2.1.5.4.2 Manual Test of Trunks

[Required: TS, EOS, SMEO, DVX-C, MFS – CONDITIONAL: DVX-L] The Manual Test of Trunks feature provides a craftsperson at a TLWS, or at another local test position interfacing with the switching system, with trunk maintenance capabilities, such as removing trunks from service, restoring trunks to service, and verifying trunk states.

5.2.1.5.5 Trunk Group – Remove from Service (Make Busy)

[Required: TS, EOS, SMEO, DVX-C, MFS – Conditional: PBX1, DVX-L] On request from the local test position, the system shall place all idle (not traffic busy) trunks in a specified trunk group in the out-of-service locked out manual state or the out-of-service disabled manual state requested. Traffic busy trunks are camped-on, and as they become idle, are placed in the requested state.

5.2.1.5.6 Trunk Group – Restore to Service (Make Idle)

[Required: TS, EOS, SMEO, DVX-C, MFS – Conditional: PBX1, DVX-L] On request from the local test position, the system shall provide the ability to restore to service in the idle state all trunks in a specified trunk group that were removed from service by use of the Remove from Service (Make Busy) feature.

5.2.1.5.7 Carrier Group Alarm

[Required: TS, EOS, SMEO, DVX-C, DVX-L, MFS] The system shall provide the capability of detecting a carrier group alarm (CGA). When this alarm is detected, all associated outgoing trunks shall be made busy automatically to subsequent customer call attempts. Call attempts on associated incoming trunks shall not be processed. When possible, the Reverse Make Busy feature shall be exercised on incoming trunks.

5.2.1.5.7.1 Software Carrier Group Alarm

[Conditional: TS, EOS, SMEO, DVX-C, DVX-L, MFS] The Software Carrier Group Alarm feature is conditional because not all switch manufacturers may provide this feature. This feature allows the local switching system to infer the failure of a carrier group from observed call failures on only a few trunks in the trunk group.

5.2.1.6 Conferencing

5.2.1.6.1 Preset Conferencing

[Requiredl: TS, EOS, MFS, DVX-C, DVX-L – Conditional: SMEO, PBX1] Preset conferencing may be implemented via an internal or external conference bridge. The DSN TS, EOS, and MFS systems shall be able to support conference bridges and the following preset conference requirements:

1. Ten (10) separate bridges with each bridge having the capacity for one (1) originator and twenty (20) conferees.

2. Each bridge shall have the capability to function as the “Primary,” “Secondary,” or “Alternate” bridge that will interconnect to other bridges that support up to a maximum of one hundred ninety-one (191) conferees using all ten (10) bridges off the same switch for the same conference.

3. Preset Conference (abbreviated pool of subscribers/bridges) assignment of abbreviated numbers shall not be greater than twenty (20) switch address numbers per bridge. Such address numbers could be a combination of subscriber lines and other conference bridge access.

4. Preset Conference network(s) that require more than twenty (20) conferees shall use the cascading bridge method of expanding the number of conferees beyond twenty (20) conferees.

5. Each preset conference bridge shall be fully capable of MLPP access and control. If such a bridge is external, then such a bridge must be fully interoperable with the serving switch to permit full MLPP access and control.

Access to preset conference equipment shall be by means of one or more KXX codes assigned solely for this use. A preset conference shall be established as follows:

1. The originating office shall screen the unique KXX office code and precedence level to protect against unauthorized preset conference usage, and, where authorized, attempt the connection, either locally or by way of interswitch trunks (ISTs). The KXX conference codes shall be translated as vacant codes on 10-digit calls.

2. The originator of a preset conference shall key the digits KXX-XXXX. This address may be preceded by:

    a. A route code for choice of data-grade or voice-grade circuits, in the form 1X-KXX-XXXX.

    b. Access digit and precedence digit for precedence level treatment, in the form 9P-KXX-XXXX, where P is any digit 0-4.

    c. Both the route code and precedence level in the form of 9P-1X-KXX-XXXX.

3. Translation of the 7-digit address shall determine routing to the appropriate switching center to obtain conferencing equipment.

4. At the appropriate switching center, the received address shall be translated to determine the conference group and the desired list of conferee addresses.

5. The number assignments shall be made in accordance with the DSN numbering plan, DISA Circular (DISAC) 310-255-1, “DSN Worldwide Numbering and Dialing Plan.”

6. If a called conferee’s telephone is not answered, automatic disconnect is to take place within an adjustable interval of 15 to 60 seconds after a bridge leg is first connected to the conferee line.

7. Originators of preset conferences shall have the capability of adding up to five (5) non-programmed conferees (within the twenty-one (21) conferees capability) to the conference by sequentially keying each add-on address and connecting the conferee to the bridge, by hook flashing, dialing the potential conference, and then hook flashing again when the next conferee answers.

5.2.1.6.1.1 Conference Notification Recorded Announcement

[Required: TS, MFS, EOS, DVX-C, DVX-L – Conditional: SMEO, PBX1] When the conference equipment receives the first off-hook supervisory signal from an answering conferee, a conference notification recording shall be applied, and shall continue as an audible announcement to answering conferees and to the originator until all conferees answer. The conference notification recording shall be removed automatically 2 seconds after the last conferee answers, indicating, by such removal, that the conferees have all answered and that the conference is ready to begin. The originator shall have the ability to remove the conference notification recording and force the conference via line or trunk by depressing the "A" or "#" key on a DTMF instrument or a programmed feature key on ISDN or digital instruments. Prematurely forcing the conference shall not interfere with attempts to complete the connections to unanswered conferees, or to add on new conferees.

Where access to secondary and tertiary bridges are necessary in a conference, arrangements shall be made so that the conference notification recordings applied at each bridge are not superimposed, as follows:

1. Each bridge shall generate a conference notification recording that is audible only to those conferees on that bridge.

2. When all conferees on a bridge have answered, the conference notification recording shall be removed automatically from that bridge 2 seconds after the last conferee answers.

3. When the conference notification recording is removed automatically from a bridge, the notification recording from the adjacent bridge, if still continuing, shall then become audible to the originator and to the conferees on the remaining bridge(s).

4. When a conferee disconnects, a conference disconnect tone, as described in Table 5.2.4-5, DSN Information Signals, shall be sent to the originator and other conferees in the conference.

5.2.1.6.1.2 Automatic Retrial and Alternate Address

[Required: TS, MFS, EOS, DVX-C, DVX-L– Conditional: SMEO, PBX1] Off-hook supervision shall be returned to the originator from each bridge when all conferees have answered or when the originator has forced the conference prior to all conferees answering. If off-hook supervision is not returned from any conferee location, within an adjustable interval of 15 to 60 seconds, one automatic retrial shall be made to the primary conferee address, as follows:

1. Conferees may be provided with alternate addresses that the switch shall try when the call fails to complete to the primary address.

2. If a call to a primary address fails to complete within two trials, the call shall be directed to an alternate address, if provided, and two call attempts shall be made to the alternate address.

5.2.1.6.1.3 Bridge Release

[Required: TS, MFS, EOS, DVX-C, DVX-L – Conditional: SMEO, PBX1] The releasing of primary, secondary, and tertiary bridges shall occur as follows:

1. The primary bridge shall be released when on-hook supervision is received on the originating port of the primary bridge or on all the other conference bridge ports.

2. If on-hook supervision is received on the originating port of secondary or tertiary bridges, all subsequent connections and equipment shall be released.

3. A conference bridge shall be released after all attempts at call completion are made and no answers are received on all ports.

4. Release of conference bridges shall be such that it shall be impossible for the bridges to become locked together.

5.2.1.6.1.4 Lost Connection to Conferee or Originator

[Required: TS, MFS, EOS, DVX-C, DVX-L – Conditional: SMEO, PBX1] If a connection to a conferee is lost, due to disconnection or preemption, a distinctive disconnect signal, defined as a conference disconnect tone, shall be provided to the conference originator and all conferees. If the originator is lost or preempted, the bridge shall be held up long enough for a preempt tone to be given to all conferees. (See Table 5.2.4-5, DSN Information Signals.)

5.2.1.6.1.5 Secondary Conferencing

[Required: TS, MFS, EOS, DVX-C, DVX-L – Conditional: SMEO, PBX1] The switch shall provide the capability of secondary conferencing, which is the ability to interconnect conference bridges located at separate DSN switches, as follows:

1. When a conference is activated and two or more of the addressees require a secondary bridge, the address shall be processed in the normal manner and directed toward the office serving the secondary equipment.

2. The conference equipment shall be designed so that it may be used alternatively for primary or secondary conferences.

3. Identical operational features, such as application and removal of the conference notification recorded announcement, shall be provided for both primary and secondary conferences.

5.2.1.6.2 Meet-Me Conferencing

[Required: TS, EOS, MFS – Conditional: SMEO, DVX-C, DVX-L, PBX1] Meet-me conferencing may be implemented via an internal or external conference bridge.

Each conferee dials into the conference bridge at a scheduled time as directed by a conference attendant. At least two conferees are required to dial the bridge number to establish the bridge. Once the bridge is established, when a conferee is added an audio connect tone, as described in Table 5.2.4-5, DSN Information Signals, will be sent to all remaining conferees. If a conferee hangs up or the conferee is preempted, an audio disconnect tone, as described in Table 5.2.4-5, will be sent to all remaining conferees.

The switching system shall be able to support the following Meet-me conference requirements:

1. Each Meet-me conference bridge shall be fully capable of MLPP access and control, as described in Section 5.2.2.1.4, Invocation and Operation.

2. When a precedence level call above the ROUTINE precedence is placed to a Meet-me conference bridge that is activated with no remaining idle resources, the switch shall conduct a preemptive search to determine the lowest active resource on the bridge, and that resource shall receive a preemption notification tone and be preempted. All remaining conferees on the bridge shall receive a conference disconnect tone.

    a. **[Required: TS, EOS, MFS]** Minimum of two (2) separate bridges with each bridge having the capacity for twenty (20) conferees.

    b. **[Conditional: SMEO, PBX1]** Minimum of two (2) separate bridges with each bridge having the capacity for ten (10) conferees.

5.2.1.6.3 Progressive Conferencing

[Conditional: TS, EOS, MFS, SMEO, DVX-C, DVX-L, PBX1] In progressive conferencing, each segment of the conference call shall be established by the originator and shall be

classmarked at its own precedence level. When a progressive conference call is established, each connection shall maintain its assigned precedence level.

When a higher precedence call is placed to any of the conferees, that conferee receives a preemption notification tone (see Table 5.2.4-5, DSN Information Signals). The other remaining conferees shall receive a conference disconnect tone, as described in Table 5.2.4-5. This tone indicates to the other parties that one of the conference call participants is being preempted.

In a progressive conference call where at least two of the conferees are established by the conference originator at different precedence levels, the switch shall classmark the precedence level of the originator of the conference call at the highest precedence of all the established conferees.

5.2.1.7 Address Translation

[Required: TS, EOS, MFS – Conditional: SMEO, DVX-C, DVX-L, PBX1] Translation of the 7-digit conference address shall be as follows:

1. The switch shall have the capability to translate three digits of the switch code.

2. The first two digits of the 4-digit line number may be utilized to identify the switching center at which conferencing equipment is located.

The 4-digit line number shall be translated to indicate the particular preset conference arrangement.

5.2.1.8 Nailed-Up Connections

[Required: TS, EOS, MFS – Conditional: SMEO, DVX-C, DVX-L, PBX1] Nailed-up connections are intended for special use, providing a permanently established path through a switch for either a network circuit (trunk) or a special service facility. The DSN switching system shall provide the following functionality for nailed-up connections:

1. A switch shall support the establishment of a nailed-up connection between any two like Pulse Code Modulation (PCM) interfaces (i.e., PCM-24, PCM-30). If a switching system supports a nailed-up connection between unlike PCM interfaces, then µ (mu)-to-A-Law conversion shall be accomplished in accordance with ITU-T Recommendation G.711, “Pulse Code Modulation (PCM) of Voice Frequencies – General Aspects of Digital Transmission Systems.”

2. The switch shall be capable of supporting a direct PCM-24 and PCM-30 interface to the DSN at the digital signal level 0 (DS0) level as follows:

    a. The switch shall support CAS at 56 kbps for PCM-24 and 64 kbps for PCM-30.

    b. The switch shall support non-CAS Clear Channel 64 kbps nailed-up connections for both PCM-24 and PCM-30 interfaces.

3. Supervision received at one side of the nailed-up connection shall be repeated at the other end. This requirement includes analog-to-digital and digital-to-digital connections.

4. All nailed-up connections through the switch shall be monitored by the normal maintenance routines to ensure proper operating paths through the switch. In the event that a switch fault affects a nailed-up connection, the system shall reconfigure the connection automatically once the fault is cleared.

5. The DSN switch shall have the capability to nail-up at least 10 percent of the switch's circuits as determined from the engineered design load.

6. Nailed-up connections shall not be preemptable but may be taken out of service to support emergency situations as determined by the commander.

5.2.1.9 Assured Dial Tone

[Required: TS, EOS, MFS, SMEO, DVX-C, DVX-L, PBX1 – Conditional: PBX2] The DoD mandates nonblocking service (P.00 threshold) from user to user for FLASH and FLASH OVERRIDE users. To meet this requirement, FLASH and FLASH OVERRIDE users shall receive dial tone at all times. The switch shall provide assured dial tone on a minimum of 3 percent (3%) of all station lines.

Requirements for this feature shall be in accordance with Telcordia Technologies GR-512-CORE, *Reliability*, Issue 2, January 1998, Section 12.

5.2.1.10 DSN Remote Switching Unit Requirements

The RSU is a switching capability that is connected to a host as a remote via an umbilical, dependent upon the host switch for software control, some or all centralized OA&M, and is integral to the Line Concentrating Module, or Remote Module that depends upon a host switch.

1. The RSU can best be described or envisioned as an installation of the host switch's internal "line and trunk cabinets" at a location within the confines of the Installation, B/P/C/S

authorized boundaries, or at a related adjacent site, normally with in few miles of the host switch." During degraded operating conditions, only partial service may be available from the RSU. The RSUs line and trunk cabinets are of the same basic type and originally certified by the JITC during the "host switch's" MFS, EO, or SMEO certification process.

2. RSUs are cost effective ways to improve "reach" and extension of voice communications capabilities and services to users located in buildings that are some distance from the host switch. An RSU is an extension for the voice switch's previously certified DoD components. For this reason:

   a. RSUs retain legacy status even if the host switch is upgraded.

   b. RSUs can be capacity upgraded, expanded, and moved within the authorized boundaries (within a reasonable distance of the Installation, B/P/C/S).

   c. RSUs used to extend the host switches' capability do not require stand-alone (MUF) capability.

   d. Stand-alone capability is only required if an RSU is utilized in EO/SMEO applications not within a reasonable distance of the host switch.

   e. Line and trunk sizing does not trigger APL requirements.

   f. CAS to PRI transitions do not trigger APL requirements.

5.2.1.11 Control of Precedence Calls

[Conditional: MFS] The Precedence Access Threshold (PAT) mechanism feature is described in the following paragraphs and may be provided to control the number of simultaneously outgoing calls for each precedence level and calling area entering the DSN. All access lines shall be capable of being classmarked for or not for PAT screening.

5.2.1.11.1 Precedence Access Threshold

[Conditional: MFS] The software-controlled PAT mechanism shall limit the number of simultaneous calls originated by selected user stations, interswitch trunk groups, attendant consoles, and other designated switch terminations where traffic input to the DSN requires screening. The PAT mechanisms shall allow termination of each application (e.g., user station, attendant positions, or special switch interfaces to users or networks) where traffic needs to be screened. The switch shall provide a minimum of seven (7) PAT mechanisms. Each PAT mechanism shall accommodate any number of the switch's terminations and any combination of

those terminations. The switch shall be equipped, through classmarks, to assign any PAT mechanism to any switch termination or conversely, any switch termination to any PAT mechanism. It shall be possible to classmark any switch termination as subject to PAT mechanism restrictions or not subject to PAT mechanism restrictions.

5.2.1.11.1.1 Call Screening

[Conditional: MFS] Outgoing calls shall be screened by classmark prior to being presented to the appropriate PAT mechanism. The classmark screening shall determine whether or not the outgoing call shall be presented to the PAT mechanism based on a comparison of the dialed address with the calling user's class of service privileges, including precedence, calling area, route code, zone restriction, and community of interest (COI) classmarks. Outgoing calls that successfully pass all tests shall be presented to the appropriate PAT mechanism. Calls that fail one or more of the tests shall be rejected and given the proper signal and/or announcement.

5.2.1.11.1.2 Functional Structure

[Conditional: MFS] Each PAT mechanism shall functionally consist of a set of Precedence Level/Calling Area (PL/CA) thresholds, a summation-of-thresholds count, and a total-calls-in-progress counter. The total-calls-in-progress counter shall count all calls in progress that were permitted by the PAT mechanism. The summation-of-thresholds count shall register the sum of all threshold levels associated with the PAT mechanism. The PL/CA thresholds place limits on the number of simultaneous calls allowed of a given combination of precedence level and calling area. There shall be five (5) precedence levels (i.e., ROUTINE, PRIORITY, IMMEDIATE, FLASH, and FLASH OVERRIDE) and five (5) progressively wider calling areas (i.e., A1, A2, A3, A4, and A5) established. Each PAT mechanism shall have twenty-five (25) PL/CA thresholds. Associated with each of these PL/CA combinations shall be a threshold setting and a calls-in-progress counter that registers the current count of the calls in progress for that PL/CA combination. Each PAT mechanism shall functionally consist of the following elements:

- A set of twenty-five (25) PL/CA thresholds.
- A set of twenty-five (25) calls-in-progress counters. Each calls-in-progress counter is associated with a PL/CA threshold.
- A summation-of-thresholds count.
- A total-calls-in-progress counter.

The calls-in-progress counter associated with a PL/CA threshold registers the number of calls in progress for that PL/CA combination.

The summation-of-thresholds count shall register the sum of the number of simultaneous calls allowed for each PL/CA combination, which corresponds to summing the PL/CA thresholds.

The total-calls-in-progress counter shall register the total number of calls in progress that were permitted by the PAT mechanism.

5.2.1.11.1.3 Simultaneous Calls Limitation

[Conditional: MFS] Each PAT mechanism shall set the limit on the number of simultaneous calls permitted at each precedence level and calling area combination, subject to permissible overflow conditions specified in Section 5.2.1.11.1.4, Overflow Process. The simultaneous calls limitation process shall be as follows:

1. A call that is presented to the PAT mechanism shall be tested initially against the PL/CA threshold that has the same PL/CA precedence level and calling area of the call. The call will be permitted if the threshold setting for that PL/CA is greater than the calls–in-progress count for that PL/CA. If the call is permitted, the calls-in-progress count for that PL/CA and the total-calls-in-progress counter shall be incremented.

2. If the threshold setting is equal to or less than the calls-in-progress count for that PL/CA, the call will be tested against the overflow process.

5.2.1.11.1.4 Overflow Process

[Conditional: MFS] The functional objective of the overflow process is for calls of lower precedence level and narrower calling area to utilize unused calling capacity of higher precedence level and equal and wider calling area, and equal precedence level and wider calling area call types without blocking calls of higher precedence level and wider calling area. The general rule for the overflow process shall be that if a call has not been permitted by initial simultaneous-calls-limitation testing, as specified in Section 5.2.1.11.1.3, Simultaneous Calls Limitation, the call will be permitted if the three following conditions are met:

1. The sum of the threshold settings of the PL/CAs with equal and higher precedence levels, and equal and wider calling areas than the call, is greater than the sum of the calls-in-progress counts of the PL/CAs with equal and higher precedence levels, and equal and wider calling areas than the call; and

2. The summation-of-thresholds count is greater than the total-calls-in-progress count.

3. The PAT algorithm shall never allow any FLASH or FLASH OVERRIDE call to be blocked, dropped, delayed, discarded, suppressed, or otherwise mutilated and interfered with in favor of calls of lesser precedence.

When a call is permitted due to the overflow procedure, it shall increment the calls-in-progress counter of the PL/CA that has the same precedence level and calling area combination of the call. This entry will be in excess of the quantity permitted by Section 5.2.1.11.1.3, Simultaneous Calls Limitation. In addition, it shall increment the total-calls-in-progress counter.

5.2.1.11.1.5 Decrementing the Calls-In-Progress Count

[Conditional: MFS] The appropriate calls-in-progress counter for the PL/CA assignment of the call and the total-calls-in-progress counter shall be decremented when any of the following occur:

1. A call permitted by the PAT mechanism is unable to find an idle or preemptable outgoing trunk during the routing process.

2. A call permitted by the PAT mechanism is preempted or is discontinued for any reason.

5.2.1.11.1.6 Call Treatment

[Conditional: MFS] Call treatments are as follows:

1. Calls that are permitted DSN access shall search the appropriate DSN trunk groups for idle or preemptable trunks in accordance with normal routing procedures.

2. ROUTINE precedence calls that are denied DSN access by a PAT mechanism shall be provided a 120 impulses per minute (IPM) busy tone.

3. PRIORITY or higher precedence calls that are denied DSN access by a PAT mechanism shall be provided the recorded Precedence Access Limitation Announcement (PALA) (see Table 5.2.2-1, Announcements).

5.2.1.11.1.7 Queuing

[Conditional: MFS] The switch shall be equipped to provide queuing for the PAT mechanism on both an off-hook and on-hook basis as follows:

1. When off-hook queuing is activated, calls shall be held in queue for a minimum of thirty (30) seconds per interval. The holding time shall be programmable and composed of a minimum of five (5) intervals.

2. When on-hook queuing is activated, calls shall be held in queue for a minimum of five (5) minutes per interval. The holding time shall be programmable and composed of a minimum of five (5) intervals. Automatic callback to the caller shall be initiated after both the PAT mechanism outlet and the needed trunk are available.

3. The switch shall be equipped to permit enabling and disabling either off-hook or on-hook queuing for each PAT mechanism on a local or remote basis.

5.2.1.11.1.8 Attendant Calls

[Conditional: MFS] The attendant shall be allowed to upgrade the PL/CA of any call on a per call basis only. After the higher PL/CA has been authorized by the attendant, the call shall be routed through the PAT screening prior to accessing the DSN. The Call Detail Recording (CDR) function shall record the escalated PL/CA granted by the attendant. This requirement will ensure proper charges for service received.

5.2.1.11.1.9 Operational Measurement Registers

[Conditional: MFS] Three operational measurement registers shall be associated with each PL/CA threshold. The first register shall be a peg count of the number of calls offered to the PAT mechanism logic at that PL/CA combination. The second register shall record the number of calls not permitted by the PAT mechanism at that PL/CA threshold combination. The third register shall record the number of calls successfully processed through the PAT mechanism at that PL/CA combination that fails to find an idle or preemptable outgoing trunk.

5.2.1.11.1.10 Maintenance and Administration of Thresholds

[Conditional: MFS] Each switch shall be able to establish and change PL/CA threshold settings and calling area restrictions of each PAT mechanism by administrative commands, and shall not require switch downtime to accomplish. A software log shall be maintained of any changes to the threshold levels for a period of ninety (90) days. An entry shall be made automatically in the log whenever a threshold level or group of threshold levels is changed. Each entry shall record the date and time the threshold levels were changed, the identity of the terminal from which the change was made (with user ID), the threshold levels resulting from the change, and the identification of personnel that made the change. The Government shall be provided access to these software logs upon request.

5.2.1.12 DSN Hotline Service

[Required: MFS, EOS, SMEO DVX-C– Conditional: DVX-L] The DSN Hotline service shall allow an analog subscriber/user to initiate a voice or data call to a predetermined party automatically by going off-hook. The switch shall dial hotline calls automatically when an off-hook condition occurs and outpulses the appropriate routing digit, i.e., "5" for voice and "6" for circuit mode data calls when transported on non-ISDN circuits. In addition, the hotline information can be carried in the Information Elements on DSN ISDN circuits. Refer to Table 5.2.3-8, Route Code Assignments.

[Conditional: MFS, EOS, SMEO, DVX-C, DVX-L] This service may be allowed for digital (ISDN or non-ISDN) users.

[Required: MFS, EOS, SMEO, DVX-C– Conditional: DVX-L] The switching system shall have the ability to classmark a designated hotline user with a hotline indicator of either voice or data. The switching system shall also have the ability to option a hotline user as follows: origination only, termination only, and both origination and termination. Hotline users assigned a hotline indicator of voice shall only be allowed to connect with other hotline users assigned as voice, and hotline users assigned a hotline indicator of data shall only be allowed to connect with other hotline users assigned as data.

5.2.1.12.1 Protected Hotline Calling

[Required: MFS, EOS, SMEO, DVX-C – Conditional: DVX-L] The DSN Hotline Service protection shall be accomplished within the same service switch (intraswitch) and outside the serving switch (interswitch) as follows:

1. Classmarking the Hotline User for Data or Voice. This protection shall allow calls to complete only between hotline users with the same hotline indicator (i.e., data or voice).

    a. Only allowing completion of calls from hotline users found in a specified screening list. (This feature is only required between intraswitch hotline users.)

    b. The MLPP interaction between hotline users shall be allowed only between hotline users classmarked with the same hotline indicator (i.e., voice or data) as described in Section 5.2.2, Multilevel Precedence and Preemption, with the exception that unanswered hotline calls above ROUTINE precedence will not divert as defined in Section 5.2.2.3, Precedence Call Diversion. Hotline user calls regardless of precedence level placed between hotline users with unlike hotline indicators (i.e., voice or data) shall receive a Vacant Code Announcement (VCA).

5.2.1.12.2 Hotline Service Protection

[Required: MFS, EOS, SMEO, DVX-C – Conditional: DVX-L] The DSN Hotline Service Protection interswitch shall be accomplished between DSN hotline users as follows:

1. T1/E1 CAS, T1 SS7 ANSI T1.619a, and E1 SS7 Q.735.3 Interfaces. The DSN Hotline Service Protection via these interfaces shall be accomplished by the use of the Route Digit (i.e., Hotline Voice-5, Hotline Data-6). Hotline users classmarked as voice originating a call over these interfaces shall outpulse a Route Digit of 5, and hotline users classmarked as data shall outpulse a Route Digit of 6. Incoming calls, via these trunk types, with a Route Digit of 5 shall only be allowed to terminate at voice classmarked hotline users. Incoming calls with a Route Digit of 6 shall only be allowed to terminate at data classmarked hotline users. The hotline Route Digit of 5 or 6 shall be included in the DSN Worldwide Numbering and Dialing Plan, as described in Section 5.2.3.5.1, DSN Worldwide Numbering and Dialing Plan.

2. T1 ISDN PRI ANSI T1.619a and E1 ISDN PRI ANSI Q.955.3 Interfaces. The DSN Hotline Service Protection via this interface shall be accomplished by the use of the Optional Off-Hook Indicator parameter in the Setup Message. This indicator shall be assigned in Code Set 5 with an element identifier of 01100101 binary (i.e., 65 hexadecimal). The data value within this identifier shall be one of two values: 00000001 (1) for Hotline Voice or 00000010 (2) for Hotline Data in Octet 3 as shown in Table 5.2.1-1. These parameters will correlate directly to Route Digit 5 (voice) or Route Digit 6 (data), respectively. Interaction between Hotline Voice and Hotline Data indicator parameters via this interface, and voice and data hotline users shall be the same as described in Section 5.2.1.12.1, Protected Hotline Calling.

3. E1 ISDN PRI ANSI Q.955.3. The DSN Hotline Service Protection via this interface shall be accomplished by the use of the Optional Off-Hook Indicator parameter in the Setup Message. This indicator shall be assigned in Code Set 5 with an element identifier of 01100101 binary (i.e., 65 hexadecimal). The data value within this identifier shall be one of two values: 00000001 (1) for hotline voice or 00000010 (2) for hotline data. These parameters will correlate directly to Route Digit 5 (voice) or Route Digit 6 (data), respectively. Interaction between Hotline Voice and Hotline Data indicator parameters via this interface, and voice and data hotline users shall be the same as described in Section 5.2.1.12.1, Protected Hotline Calling.

Table 5.2.1-1. Code Set 5 Optional Off-Hook Parameter

8	7	6	5	4	3	2	1	Octet
Optional Off-hook Information								1
0	1	1	0	0	1	0	1	
Element Identifier								
Format Descriptor								2
0	0	0	0	0	0	0	1	
Value								3
See Note 1 for values								
Note 1. Values for Octet 3								
0	0	0	0	0	0	0	1	voice
0	0	0	0	0	0	1	0	data

Hotline Service Protection interaction between hotline user indicators shall be as depicted in Table 5.2.1-2.

Table 5.2.1-2. DSN Hotline Service Protection Matrix

CALLED FROM	CALLED TO	PROTECTION	TREATMENT
Hotline Data user	Hotline Voice user	Denied	VCA
Hotline Data user	Hotline Data user	Allowed	
Hotline Voice user	Hotline Data user	Denied	VCA
Hotline Voice user	Hotline Voice user	Allowed	
Non-Hotline Data user	Hotline Voice user	Denied	VCA
Non-Hotline Voice user	Hotline Voice user	Denied	VCA
Non-Hotline Data user	Hotline Data user	Denied	VCA
Non-Hotline Voice	Hotline Data user	Denied	VCA

The DSN Hotline service shall not be allowed to interact with the following services (This restriction shall be applied manually in software or by default when a user is classmarked as a hotline user.):

- Hold (line terminator denied to put call on “HOLD”)
- Three-way calling
- Normal call transfer
- Electronic Key Telephone System (EKTS)
- Ad hoc conferencing

5.2.1.12.3 Non-Pair Protected Hotline Calling

[Required: MFS, EOS, SMEO, DVX-C – Conditional: DVX-L] A Non-Pair Protected Hotline user shall be able to receive calls from any other hotline user with the same hotline indicator (i.e., voice or data) as described in Section 5.2.1.12.1, Protected Hotline Calling. The Non-Pair Protected Hotline user shall originate calls to a specified destination only, called the Designated Called Party (DCP).

5.2.1.12.4 Pair Protected Hotline Calling

[Required: MFS, EOS, SMEO, DVX-C – Conditional: DVX-L] Pair Protected Hotline users shall only be able to call each other and shall not be allowed to receive calls from a third party. This protection shall be required for intraswitch hotlines. It may be allowed for interswitch hotlines when end-to-end ISDN is supported between hotline users.

5.2.2 Multilevel Precedence and Preemption

5.2.2.0 Introduction

This section covers the MLPP requirements for DSN switching systems. It discusses precedence levels, cause values, preemption in the network, interface requirements for MLPP with ISDN, and MLPP interactions with other features and services. No feature or function specifically identified in UCR 2008 or in the referenced standards shall prevent the completion or connection of a PRIORITY or higher precedence call in accordance with this section.

5.2.2.1 MLPP Overview

5.2.2.1.1 Description

[Required: TS, EOS, MFS, SMEO, DVX-C, DVX-L, PBX1] The MLPP service applies to the MLPP service domain only. Connections and resources that belong to a call from an MLPP subscriber shall be marked with a precedence level and domain identifier (refer to Section 5.2.2.7, ISDN MLPP PRI, and Section 5.2.2.9, MLPP CCS7, and shall only be preempted by calls of higher precedence from MLPP users in the same MLPP service domain. The maximum precedence level of a subscriber is set at the subscription time by the DSN network administrator based on the subscriber's validated need. The subscriber may select a precedence level up to and including the maximum authorized precedence level on a per call basis.

Precedence provides preferred handling of MLPP service requests. It involves assigning and validating priority levels to calls, and prioritized treatment of MLPP service requests.

Precedence calls (i.e., PRIORITY and above) that are not responded to by the called party (e.g., call unanswered) shall be diverted in accordance with Section 5.2.2.3, Precedence Call Diversion. If precedence call waiting has been invoked, these calls shall be handled in accordance with Section 5.2.2.8.1, Precedence Call Waiting. Unanswered calls placed at a ROUTINE precedence level shall continue to ring.

Preemption may take one of two forms. First, the called party may be busy with a lower precedence call that must be preempted in favor of completing the higher precedence call from the calling party. Second, the network resources may be busy with calls; some of which are of lower precedence than the call requested by the calling party. One or more of these lower precedence calls shall be preempted to complete the higher precedence call. The four characteristics of preemption are as follows:

1. Any party whose connection was terminated, whether that resource is reused or not, shall receive a distinctive preemption notification (see Table 5.2.4-5, DSN Information Signals).

2. Any called party of an active call that is being preempted by a higher precedence call shall be required to acknowledge the preemption by going on-hook, before being connected to the new calling party.

3. When there are no idle resources, preemption of the lowest of these lower level precedence resources shall occur.

4. A call can be preempted any time after the precedence level of the call has been established and before call clearing has begun.

5.2.2.1.2 Precedence Levels

[Required: TS, EOS, MFS, SMEO, DVX-C, DVX-L, PBX1] The switch shall provide five precedence levels. The precedence levels listed from lowest to highest are ROUTINE, PRIORITY, IMMEDIATE, FLASH, and FLASH OVERRIDE.

5.2.2.1.3 Announcements

[Required: TS, EOS, SMEO, DVX-C, DVX-L[R2], MFS, PBX1] With the exception of the PALA and the Attendant Queue announcement (ATQA), the announcements in Table 5.2.2-1, Announcements, are required for all DSN switches and for all announcements that are associated with specific network management trunk group and/or code control implementation. Each

announcement shall contain a location identification number to be provided by the Government. The switching system shall be identified by "Switch Name and Location." Announcements shall be capable of being recorded and changed by Government operations and maintenance (O&M) personnel. Additional local messages may be added and optionally activated, deactivated, or modified via administrative/operational controls

[Required: MFS, EOS] The ATQA is required for an MFS and an EOS.

[Required: TS, EOS, SMEO, MFS, PBX1 - Conditional: DVX-C, DVX-L] The Loss of C2 (LOC2) Features announcement shall be played when the call leaves the MLPP-capable DSN network to a non-MLPP capable location. For example, DSN callers who place calls to locations that permit off-net terminations may be provided with a voice message announcement informing them that they have left the DSN.

5.2.2.1.4 Invocation and Operation

[Required: TS, EOS, MFS, SMEO, DVX-C, DVX-L, PBX1] The precedence level of a call is selected by the subscriber on a per call basis. The subscriber may select any precedence level up to and including his or her maximum authorized precedence level. The network at the subscriber's originating interface ensures that the selected precedence level does not exceed the maximum level assigned to that telephone number. Once set for a call, this precedence level cannot be changed. In addition, a connection between two DSN subscribers shall not have different precedence levels. A call will default automatically to the ROUTINE precedence unless a higher precedence is dialed. The DSN Worldwide Numbering and Dialing Plan is specified in Section 5.2.3.5.1, DSN Worldwide Numbering and Dialing Plan, Section 5.2.3.5.3, Standard Directory Numbers, and Section 5.2.3.5.4, Standard Test Numbers.

During a call setup, if there is a shortage of network resources, the switch shall determine whether resources are held by calls of lower precedence. If there is a shortage, the switch shall release the lowest of these lower precedence call(s) and seize the resources required to set up the higher precedence call. These resources include interoffice circuits, intraoffice circuits, lines, conference bridges, and circuit-switched data circuits.

The preemption operation depends on whether the switch needs to preempt a common network facility, such as an IST that is currently being used by a different subscriber than the intended called subscriber, or whether it needs to preempt a channel on the user access of the called subscriber.

Table 5.2.2-1. Announcements

ANNOUNCEMENT CONDITION	ANNOUNCEMENT
An equal or higher precedence call is in progress	Blocked Precedence Announcement (BPA). "(Switch name and Location). Equal or higher precedence calls have prevented completion of you call. Please hang up and try again. This is a recording. (Switch name, location identification number, and Location)."
Unauthorized precedence level is attempted	Unauthorized Precedence Level Announcement (UPA). "(Switch name and Location). The precedence used is not authorized for your line. Please use an authorized precedence or ask your attendant for assistance. This is a recording. (Switch name, location identification number, and Location)."
No such service or Vacant Code	Vacant Code Announcement (VCA). "Switch name and Location. Your call cannot be completed as dialed. Please consult your directory and call again or ask your operator for assistance. This is a recording. (Switch name, location identification number, and Location)."
Operating or equipment problems encountered	Isolated Code Announcement (ICA). "(Switch name and Location). A service disruption has prevented the completion of your call. Please wait 30 minutes and try again. In case of emergency, call your operator. This is a recording. (Switch name, location identification number, and location)."
Precedence Access Threshold (PAT) limitation	Precedence Access Limitation Announcement (PALA). "(Switch name and Location). Precedence access limitation has prevented the completion of your call. Please hang up and try again. This is a recording. (Switch name, location identification number, and Location)."
Busy station not equipped for preemption	Busy Not Equipped Announcement (BNEA). "(Switch name and Location). The number you have dialed is busy and not equipped for call waiting or preemption. Please hang up and try again. This is a recording. (Switch name, location identification number, and Location)."
Attendant Queue Announcement	Attendant Queue Announcement (ATQA). "This is the <site name> [multifunction, end office] switch. All attendants are busy now. Please remain on the line until an attendant becomes available or try your call later. This is a recording. <site name> [multifunction, end office] switch."
Loss of C2 Features	Loss of C2 Features Announcement (LOC2). "This is the (Switch name, location identification number, and Location). This call is leaving the DSN. This is a recording."

If a called user access line is to be preempted, both the called party and its connected-to parties shall be, at a minimum, audibly notified of the preemption using the preemption tone in Table 5.2.4-5, DSN Information Signals, and the existing MLPP call shall be immediately cleared. The called party must acknowledge the preemption by going on-hook or pressing a feature button, before the higher precedence call is completed. Then the called party is offered the new MLPP call.

After attempting a precedence call, the calling party shall receive an audible ringback precedence call tone when the call is offered successfully to the called party as a precedence call. These alerting tones are provided in Table 5.2.4-5, DSN Information Signals.

The calling party shall receive a BPA, as shown in Table 5.2.2-1, Announcements, for the following reasons:

1. Equal or higher precedence calls have prevented completion.

2. No idle network resources are available to make a connection to the dialed number and the called subscriber belongs to a network that does not support preemption.

The calling party shall receive an UPA, as shown in Table 5.2.2-1, Announcements, if the requested precedence level is not subscribed to.

The calling party shall receive a BNEA, as shown in Table 5.2.2-1, Announcements, if the called party is assigned as nonpreemptable. Precedence calls (i.e., PRIORITY and above) that are not responded to by the called party (e.g., call unanswered) shall be diverted in accordance with Section 5.2.2.3, Precedence Call Diversion. If precedence call waiting has been invoked, these calls shall be handled in accordance with Section 5.2.2.8.1, Precedence Call Waiting. Unanswered calls placed at a ROUTINE precedence level shall continue to ring.

5.2.2.2 Preemption in the Network

[Required: TS, EOS, SMEO, DVX-C, DVX-L, MFS, PBX1] The following sections describe the treatment for precedence calls at the called party's interface and applies to both analog and digital (ISDN and non-ISDN) terminating lines.

5.2.2.2.1 Network Facilities Active with Lower Precedence Calls

[Required: TS, EOS, SMEO, DVX-C, DVX-L, MFS, PBX1] For PRIORITY precedence calls and above, during call setup, if there is a shortage of a network resource, then the network shall determine if resources are held by calls of lower precedence. The network shall release the lowest of these lower precedence call(s) and seize the necessary resources that are required to set up the higher precedence call. These resources include interoffice circuits, channels, conference bridges, and circuit-switched data circuits.

When a common network facility is preempted, all existing parties shall receive a preemption tone (see Table 5.2.4-5, DSN Information Signals) and the existing connection is disconnected. The new higher precedence call is set up using the preempted facility.

5.2.2.2.1.1 CANCEL To / CANCEL From

[Required: TS, EOS, MFS – Conditional: SMEO, DVX-C, DVX-L,] Requirements for the CANCEL to/CANCEL from feature shall be in accordance with Telcordia Technologies GR-477-CORE, *Network Traffic Management*, Section 6, NTM Manual Controls, Issue 4, February 2000.

In addition, FLASH and FLASH OVERRIDE calls shall be exempted from these controls. The application of any trunk group control shall not prevent precedence calls from performing a preemptive search on all trunk groups that were friendly searched previously.

5.2.2.2.2 Network Facilities Active with Equal or Higher Precedence Call

[Required: TS, EOS, SMEO, DVX-C, DVX-L, MFS, PBX1] If all network facilities required to complete a precedence call are busy with equal or higher precedence calls, the calling user shall be sent the BPA (see Table 5.2.2-1, Announcements).

5.2.2.2.3 MLPP Trunk Selection (Hunting)

[Required: TS, EOS, SMEO, DVX-C, DVX-L, MFS] The DSN route selections shall be based on PL/CA classmarks for both voice-grade and data-grade trunk groups. The DSN hunting sequence shall be capable of being varied depending on the route. Hunt sequences shall be capable of scanning data-grade trunk groups for voice-grade calls. The hunting sequence shall be capable of searching all trunks. The hunting sequence shall first examine the route digit so that, for data calls only, data-grade trunks shall be searched. For voice-grade calls, all trunks shall be searched.

5.2.2.2.3.1 Hunt Sequence for Trunks

[Required: TS, EOS, SMEO, DVX-C, MFS – Conditional: DVX-L] The switches shall route DSN calls to trunks that have classmarks to indicate the maximum PL/CA permitted. Calls shall not be originated over trunk groups when the call attempt exceeds the precedence level or calling area.

5.2.2.2.3.1.1 ROUTINE Precedence Calls

[Required: TS, EOS, SMEO, DVX-C, DVX-L, MFS] For ROUTINE precedence calls, the switch shall employ an idle search on all programmed routes to the call destination. Failing to find an idle trunk, the switch shall provide a trunk busy tone to the caller.

5.2.2.2.3.1.2 Precedence Calls Above ROUTINE Precedence

[Required: TS, EOS, SMEO, DVX-C, DVX-L, MFS] The switch shall provide for two methods of trunk route selection for precedence level calls above the ROUTINE precedence. Either method can be assigned to a destination route based on the DSN Area Code (KXX) and/or DSN Switch Code (KXX) of the call. In each method, trunks shall be tested individually for idle or busy conditions. If preemption is required, only a call of the lowest level of precedence, lower than the dialed precedence, shall be preempted.

5.2.2.2.3.1.2.1 Method 1

[Required: TS, EOS, SMEO, DVX-C, DVX-L, MFS] In method 1, the switch shall perform an idle search on the direct route and all alternative routes, as shown in Figure 5.2.2-1, Example Hunt Sequence for Method 1.

Failing to find an idle trunk, the switch shall enter the preemptive search. In the preemptive search, the switch shall search again for an idle trunk in the direct route, and if so, shall select any idle trunk found. If no idle trunk exists in the direct route, the switch shall preempt the call of the lowest precedence in the direct route, provided the precedence of the call selected for preemption is lower than the precedence of the call being processed. Failing to complete the call on the direct route, the switch shall advance the preemptive search to the next alternate route, and repeat the preemptive search process described above. This process will continue through all possible alternate routes. When the switch is unable to preempt, it shall route the caller to the BPA.

5.2.2.2.3.1.2.2 Method 2

[Required: TS, MFS – Conditional: EOS, SMEO, DVX-C, DVX-L,] In method 2, the switch shall directly enter a friendly, then a preemptive, search of the direct route before searching the next alternate route choice, as shown in Figure 5.2.2-2, Example Hunt Sequence for Method 2.

In the preemptive search, the switch shall search for an idle trunk in the direct route, and if so, shall select any idle trunk found. If no idle trunk exists in the direct route, the switch shall preempt the call of the lowest precedence in the direct route, provided the precedence of the call selected for preemption is lower than the precedence of the call being processed. Failing to complete the call on the direct route, the switch shall advance the preemptive search to the next alternate route, and repeat the preemptive search process described above. This process will continue through all possible alternate routes. When the switch is unable to preempt, it shall route the caller to the BPA.

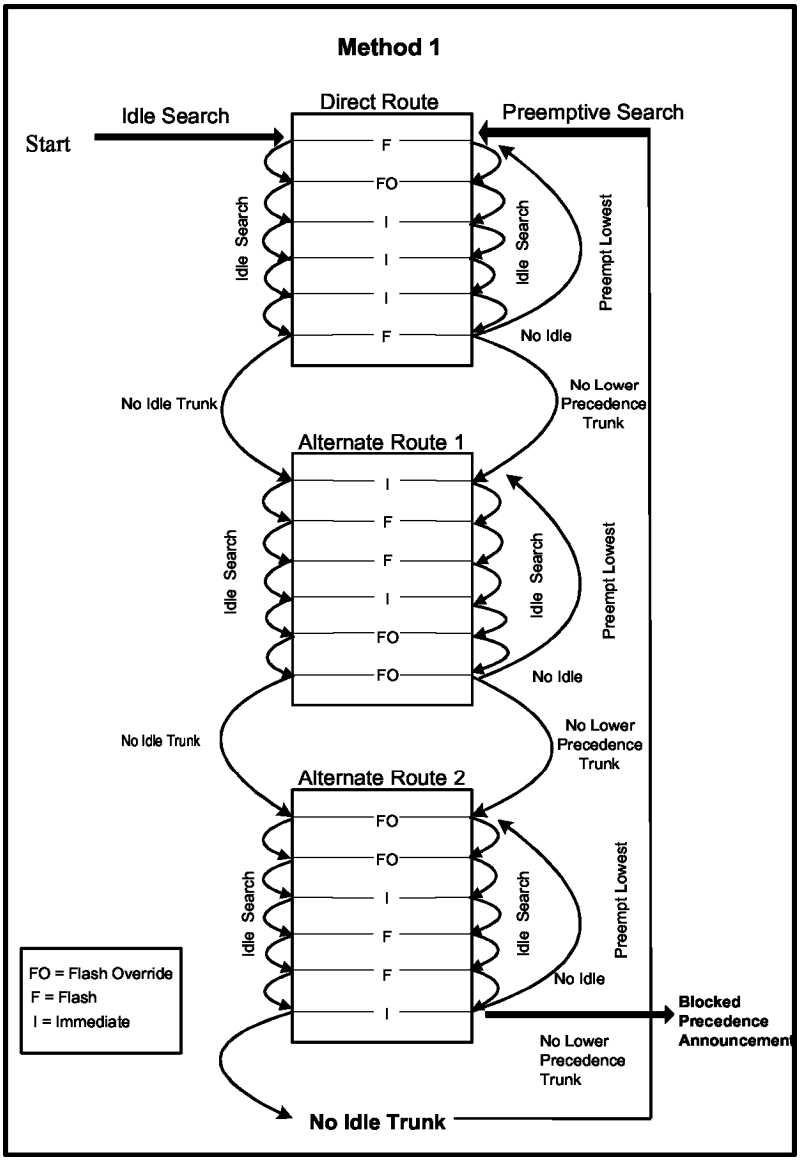


Figure 5.2.2-1. Example Hunt Sequence for Method 1

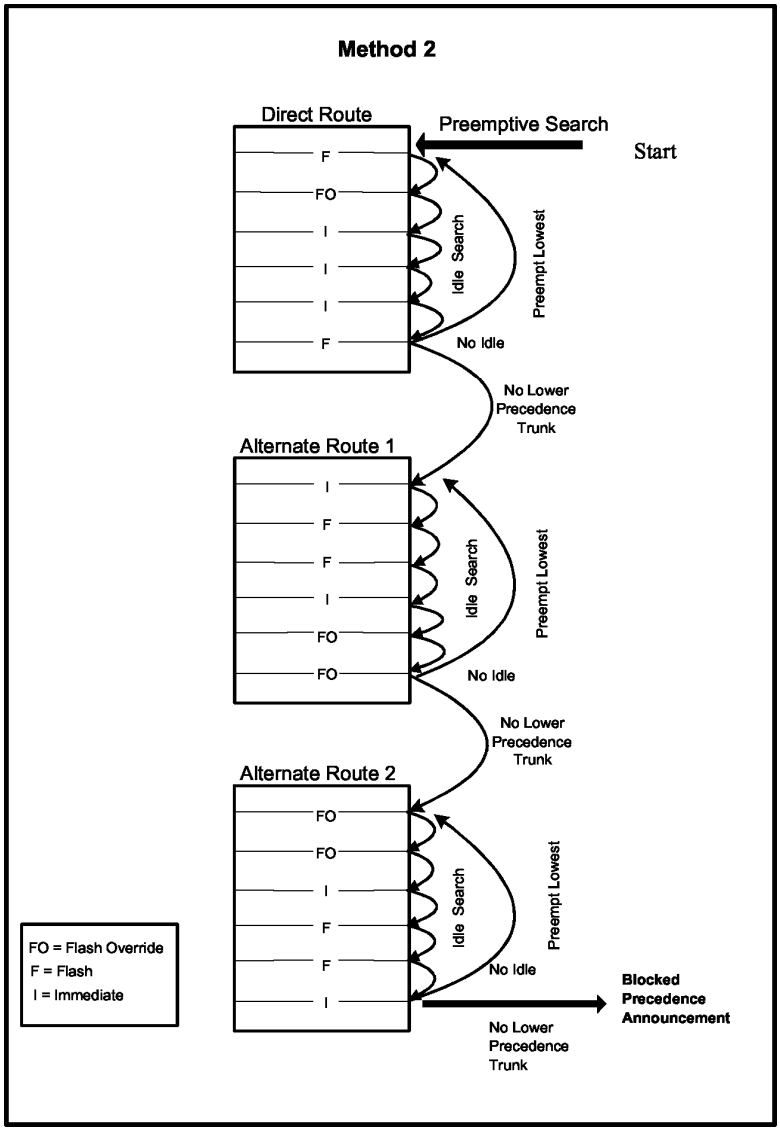


Figure 5.2.2-2. Example Hunt Sequence for Method 2

5.2.2.2.4 MLPP Interworking with Other Networks

5.2.2.2.4.1 Calls from Non-MLPP Networks

[Required: TS, EOS, SMEO, DVX-C, DVX-L, MFS] Calls from non-MLPP networks that enter the DSN shall be assigned the lowest precedence level and the DSN MLPP service domain identification at the network boundary and may be preempted within the DSN.

5.2.2.2.4.2 Precedence Calls to Non-MLPP Networks

[Required: TS, EOS, SMEO, DVX-C, DVX-L, MFS] When a precedence call leaves the DSN (line originated or trunk tandem) and enters a network (i.e., PSTN, North American Treaty Organization (NATO), Enhanced Mobile Satellite Systems (EMSS), etc.) or a non-MLPP device (e.g., ARD) that does not support the MLPP service, the call is treated as a non-MLPP call. The switching system that is directly connected to the non-MLPP network shall send an LOC2 announcement via the bearer speech path to the originator as described in Section 5.2.2.1.3, Announcements.

On a trunk group basis, switches shall be capable of terminating incoming calls above ROUTINE to trunk groups classmarked as non-preemptable (e.g., to a PBX2, PSTN, or other non-DSN network). The switch shall be capable of providing the following capabilities:

1. The switch shall divert the precedence call to an alternate directory number or location capable of handling the precedence level of the call.

2. The switch shall pass the precedence call, including MLPP information element for ISDN/SS7, to the distant switch (e.g., PSTN). That call shall be preemptable and maintain its precedence level within its domain of the DSN network.

   NOTE: Any network that does not support the MLPP service shall convey, if technically possible, the parameters of the MLPP service (e.g., precedence level, domain, etc.) intact. In this case, the network shall pass them on with no action taken.

3. The switch shall extend the precedence call as routine (i.e., no T1.619a information elements) to the PBX2 or a non-MLPP network.

5.2.2.3 Precedence Call Diversion

[Required: MFS, EOS SMEO, DVX-C, DVX-L, PBX1] The switch shall provide a global default diversion of all unanswered calls above the ROUTINE precedence to a designated directory number (e.g., attendant console), after a specified period of time, selectable 15–45 seconds and before the voice mail and Automatic Call Distribution (ACD) system diversion. Calls above ROUTINE precedence destined to directory numbers that are configured with voice mail or ACD systems shall only divert as specified above. ROUTINE precedence calls destined to directory numbers that are configured with voice mail or ACD systems are allowed and shall be configurable to divert after the global default diversion timer interval.

Precedence level calls above the ROUTINE precedence shall not be forwarded to voice mail.

Incoming DSN precedence calls to the attendant's listed directory number and incoming calls diverted to an attendant shall signal the attendant by a distinctive visual signal, indicating the precedence level, and shall be placed in queue. Call distribution shall be accomplished to reduce excessive waiting times. Each attendant position shall operate from common queue(s). Incoming calls shall be queued for attendant service by precedence and time of arrival. The highest precedence with the longest holding time call shall be answered first. A recorded message of explanation (e.g., ATQA) shall be applied automatically to the waiting calls (refer to Table 5.2.2-1, Announcements).

5.2.2.4 Preempt Signaling

5.2.2.4.1 Channel Associated Signaling

[Required: TS, EOS, SMEO, DVX-C, DVX-L, MFS – Conditional: PBX1] Preemption on CAS trunks is accomplished at a DSN switch by sending a measured supervisory signal toward both the calling user and the called user lines of an established or ringing call connection. The supervisory signal is recognized at each DSN switch, causing disconnect of any intermediate trunk circuits. Following intermediate circuit release, a preempt warning tone of 440 + 620 Hz is applied to each end user line or PBX access line circuit. The preempt warning tone is introduced by the terminating DSN switch at a composite level of -16 dBm, measured at the zero transmission level point (TLP). The preempt warning tone is maintained until a disconnect signal is returned to the switch. The trunk or line that was selected for Preemption for Reuse is reused to serve the waiting precedence call. Four preemption signals exist, depending upon the circuit condition and intended disposition. They are Answered Call: Circuit to be Reused, Unanswered Call: Circuit to be Reused, Answered Call: Circuit Not to be Reused, and Unanswered Call: Circuit Not to be Reused, and are illustrated in Figure 5.2.2-3, DSN Preempt Signals.

Table 5.2.2-2 describes the preemption signals.

Preemption for Reuse can be exercised only on classmarked trunks or access lines in a preemptable group. Preemption Not for Reuse may occur on any classmarked trunk or access line when another link in the established connection is preempted for reuse. The DSN switches shall apply a preemption warning tone to DP and DTMF access lines and access trunks that do not use Wink Start signaling for supervision. Trunks that use Wink Start supervision must conform to the preempt signals, as shown in Figure 5.2.2-3, DSN Preempt Signals. Access lines and trunks using common channel supervision (i.e., D channel signaling) shall apply the preemption warning tone to the user that is preempted. Switches that support MF(R1) signaling shall be capable of interpreting and responding to the four preempt signals, as shown in Figure 5.2.2-3.

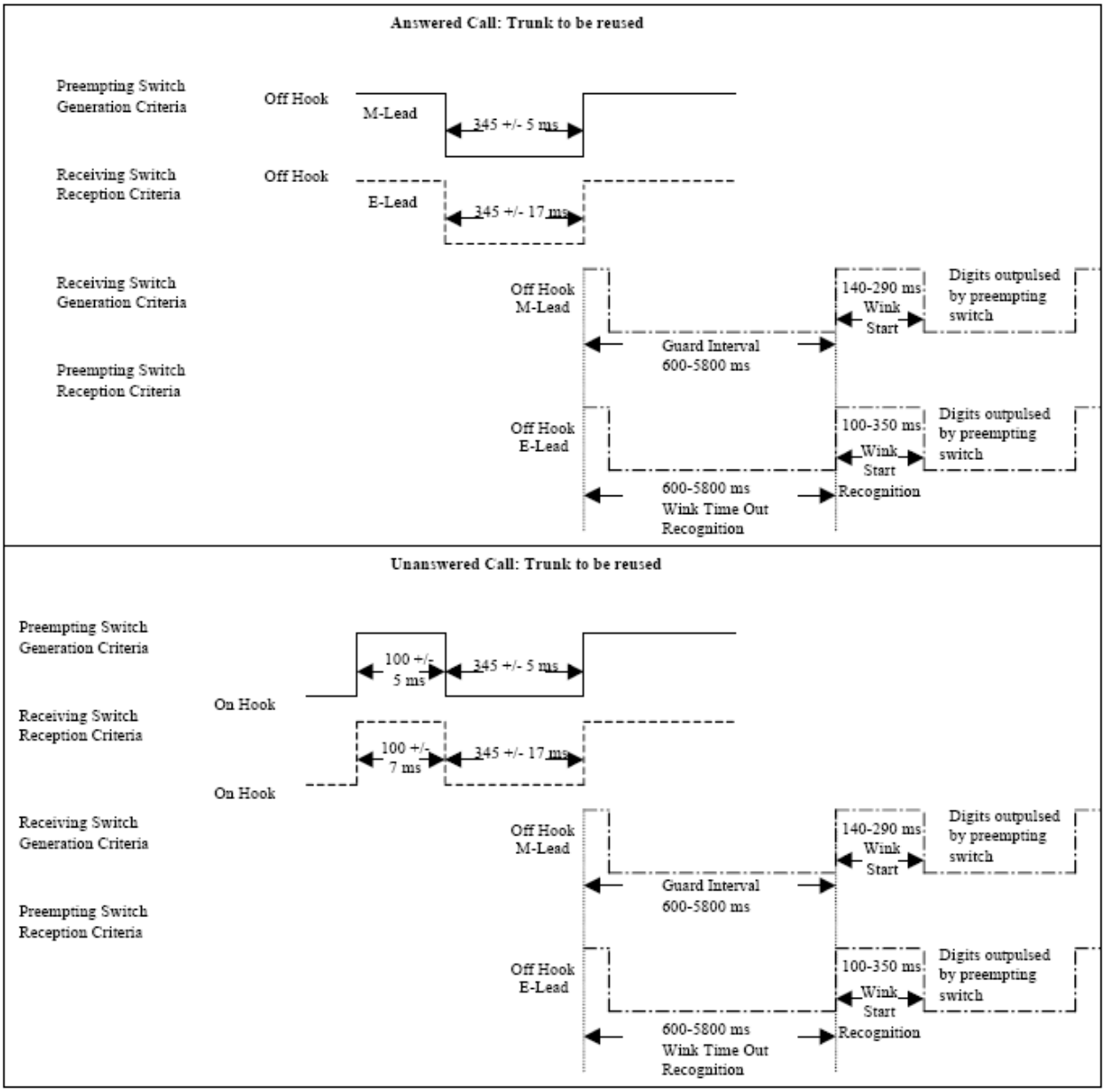


Figure 5.2.2-3. DSN Preempt Signals

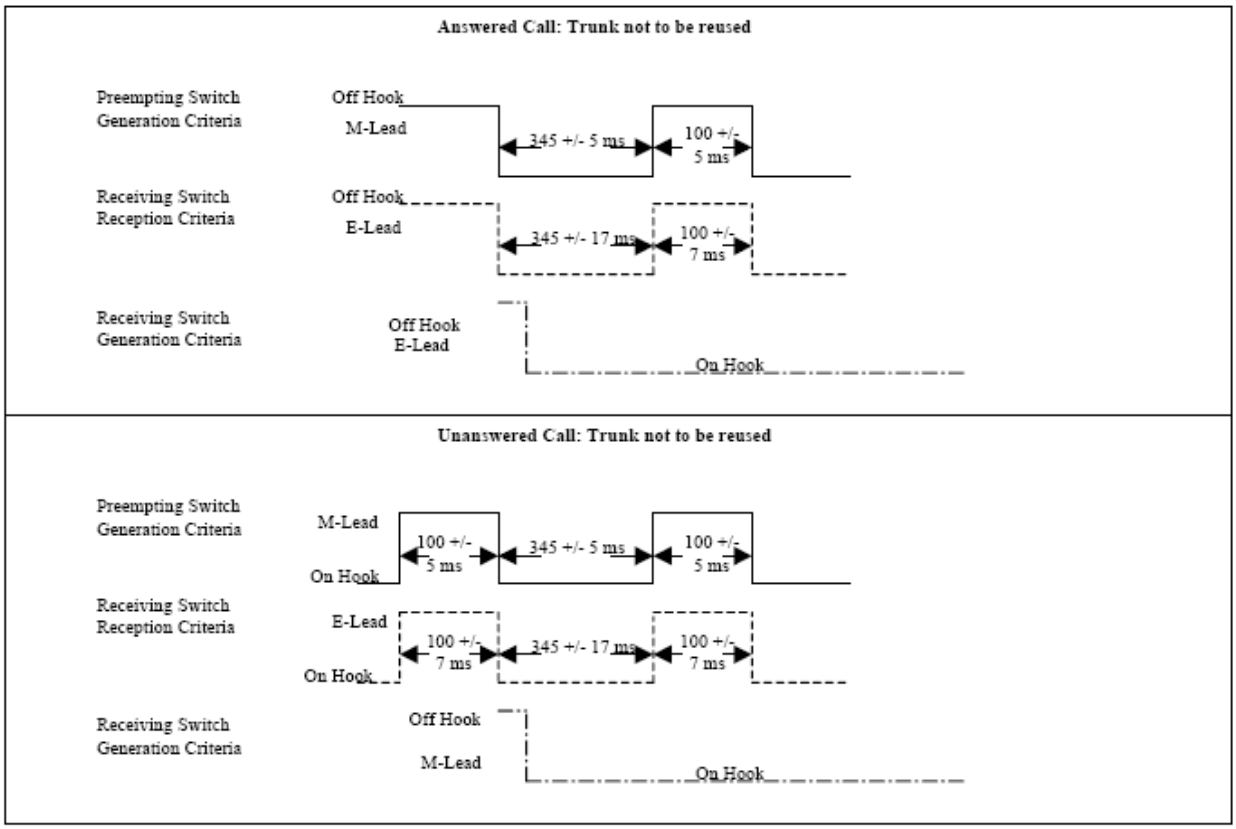


Figure 5.2.2-3. DSN Preempt Signals (continued)

5.2.2.4.2 Primary Rate Interface

[Required: TS, EOS, SMEO, DVX-C, MFS, PBX1] Requirements for MLPP PRI signaling shall be in accordance with ANSI Standards T1.619-1992 and T1.619a-1994, and UCR 2008, Section 5.2.1.3.4, ISDN Primary Access.

5.2.2.4.3 Common Channel Signaling Number 7

[Required: TS, EOS, MFS – Conditional: SMEO, DVX-C] Requirements for MLPP Common Channel Signaling Number 7 (CCS7) signaling shall be in accordance with ANSI Standards T1.619-1992 and T1.619a-1994.

5.2.2.5 Analog Line MLPP

5.2.2.5.1 Busy at the Called Party's Interface

[Required: EOS, SMEO, DVX-C, DVX-L, MFS, PBX1] The following busy line treatment at the called party's interface for precedence calls applies to analog terminating lines. The line treatments apply to interswitch calls or calls between stations on the same switch.

5.2.2.5.1.1 Line Active with a Lower Precedence Call

[Required: EOS, SMEO, DVX-C, DVX-L, MFS, PBX1] Precedence calls arriving at a busy station that is classmarked as preemptable shall preempt the active lower precedence call. The active busy station shall receive a continuous preemption tone until an on-hook signal is received and the other party shall receive a preemption tone for a minimum of 3 seconds (see Table 5.2.4-5, DSN Information Signals). After going on-hook, the station to which the precedence call is directed shall be provided precedence ringing (see Table 5.2.4-4, DSN Ringing Tone and Cadence). The station shall be connected to the preempting call after going off-hook.

If call waiting is invoked on the terminating line, it shall be ignored and the existing lower precedence call shall be preempted (refer to UCR 2008, Section 5.2.2.8.1.3, Busy with Lower Precedence Call).

5.2.2.5.1.2 Line Active with an Equal or Higher Precedence Call above ROUTINE Precedence

[Required: EOS, SMEO, DVX-C, DVX-L, MFS, PBX1] Precedence calls arriving at a station that is busy with an equal or higher precedence call shall be routed to a BPA (see Table 5.2.2-1, Announcements). If the called station has activated call forwarding, the switch shall attempt to complete the call to the forward destination.

5.2.2.6 ISDN MLPP BRI

5.2.2.6.1 General Description

[Required: EOS, SMEO, MFS – Conditional: DVX-C, DVX-L, PBX1, PBX2] The ISDN MLPP Basic Rate Interface (BRI) allows the simultaneous transmission of voice, circuit-switched data, and packet data over a single customer line connecting CPE and a digital switch. Specifically, the basic access allows the provision of two 64-kbps B channels, which may be used to carry voice, circuit-switched data, or packet data, and a one 16-kbps D channel, which can carry signaling and packet information.

MLPP requirements for this feature shall be in accordance with ANSI Standard ANSI T1.619-1992 and T1.619a-1994, and UCR 2008, Section 5.2.1.3.3, National ISDN 1/2 Basic Access.

5.2.2.6.2 Single B Channel, Single Appearance, Single Directory Number

[Required: EOS, SMEO, MFS – Conditional: DVX-C, PBX1, PBX2] The following busy line treatment at the called party's interface for precedence calls applies to digital (ISDN and non-ISDN) terminating lines. The line treatments also apply to interswitch calls and calls between stations on the same switch.

5.2.2.6.2.1 Line Active with a Lower Precedence Call

[Required: EOS, SMEO, MFS – Conditional: DVX-C, PBX1] Precedence calls arriving at a busy station that is classmarked as preemptable shall preempt the active lower precedence call. The active busy station shall receive a continuous preemption tone until an on-hook signal is received and the other party shall receive a preemption tone for a minimum of 3 seconds (see Table 5.2.4-5, DSN Information Signals). After going on-hook, the station to which the precedence call is directed shall be provided precedence ringing (Table 5.2.4-4, DSN Ringing Tone and Cadence). The station shall be connected to the preempting call after going off-hook.

If call waiting is invoked on the terminating line, it shall be ignored and the existing lower precedence call shall be preempted (refer to UCR 2008, Section 5.2.2.8.1.3, Busy with Lower Precedence Call).

5.2.2.6.2.2 Line Active with an Equal or Higher Precedence Call

[Required: EOS, SMEO, MFS – Conditional: DVX-C, PBX1] Precedence calls arriving at a station that is busy with an equal or higher precedence call shall be routed to a BPA (see Table 5.2.2-1, Announcements). If the called station has activated call forwarding, the call shall be forwarded to the new number at the same precedence level.

5.2.2.6.3 Single B Channel, Multiple Appearances, Single Directory Number

[Conditional: EOS, SMEO, DVX-C, MFS, PBX1, PBX2] This section describes the requirements for processing precedence calls over a single B channel ISDN interface with a station set that has multiple appearances and one directory number.

Incoming precedence calls to a multiple appearance ISDN station set shall provide a precedence ringing tone on the next available button as well as a visual display of the precedence level on

the station set. Then the called party shall have the option of either placing the current call on hold and picking up the incoming precedence call, or ignoring the call.

This process of placing a call on hold and answering a precedence call shall remain the same until the BRI is saturated (i.e., all call appearances are in use). When an incoming precedence call is made to a saturated BRI, the lowest precedence call, including those on hold, shall be preempted.

If a call on hold has the lowest precedence, the switch shall send a preemption tone to the call on hold caller. The switch sends a preemption tone to the corresponding appearance on the station set of the destination directory number that has placed the call on hold. After a preset time the call is cleared and the switch sends a precedence ring to the corresponding appearance on the station set of the destination directory number. Next, the destination directory number user hears the precedence ringing, indicating that the call on hold has been dropped. The directory number user sees the precedence level of this new call on the station set display also. The directory number user shall have the option of answering the call, letting it forward to an alternate party, and/or letting it divert to an attendant.

If the active call has the lowest precedence, the switch shall send a preemption tone to the active call and the destination directory number. When the destination directory number goes on hook, a precedence ring is received indicating the incoming precedence call.

In these two cases, the other calls on hold are not preempted, and they may be retrieved at any time.

5.2.2.6.4 Two B Channels, Multiple Appearances, Single Directory Number

[Conditional: EOS, SMEO, DVX-C, MFS – Conditional: PBX1, PBX2] The requirements for processing precedence calls over a two (2) B channel ISDN interface, with a station set that has multiple appearances and one directory number, shall be identical to that in UCR 2008, Section 5.2.2.6.3, Single B Channel, Multiple Appearances, Single Directory Number (i.e., precedence calls over a single B channel ISDN interface with a station set that has multiple appearances and one directory number).

In addition, this interface is limited by the number of possible appearances on the ISDN station set.

5.2.2.6.5 Two B Channels, Two Directory Numbers (Data Mode Only)

[Required: EOS, SMEO, MFS – Conditional: DVX-C, PBX1, PBX2] This section describes the requirements for processing precedence calls over a two B channel ISDN interface with two directory numbers.

When an ISDN call appearance is set up as data-mode only (i.e., one or two B channels equipped for data), preemption by incoming voice calls shall not be permitted. Any incoming higher precedence voice calls placed to a BRI in data-mode shall receive a BNEA or divert in accordance with UCR 2008, Section 5.2.2.3, Precedence Call Diversion.

5.2.2.7 ISDN MLPP PRI

[Required: TS, EOS, SMEO, DVX-C, MFS, PBX1] Requirements for ISDN MLPP PRI shall be in accordance with ANSI Standards T1.619-1992 and T1.619a-1994.

[Conditional: TS, EOS, SMEO, DVX-C, MFS, PBX1] Requirements for European Telecommunications Standards Institute (ETSI) ISDN MLPP PRI shall be in accordance with ITU-T Standard Q.955.3-1993.

5.2.2.7.1 Definitions

Definitions of terms can be found in UCR 2008, Appendix A, Section A2, Glossary and Terminology Description.

5.2.2.7.2 Precedence Level Information Elements

[Required: TS, EOS, SMEO, DVX-C, MFS, PBX1] The MLPP ISDN PRI Setup Message shall contain the Precedence Level Information Element in Code Set 5, as shown in Table 5.2.2-3.

Table 5.2.2-3. MLPP ISDN PRI Precedence Level Information Element (Code Set 5)

Octet 3:

Bit:	8	7	6	5	4	3	2	1
	Precedence Level Information							
Octet 1	0	1	0	0	0	0	0	1
	Element Identifier							
2	Length of Precedence Level Contents							
3	1 Ext	Coding Standard		Spare	Precedence Level			
4	0/1 Ext	Spare			Change Value	Spare	LFB Indication	
5	1st Network Identity Digit				2nd Network Identity Digit			
6	3rd Network Identity Digit				4th Network Identity Digit			
7	Most Significant Bit (DSN MLPP Service Domain 1st Octet)							
8	DSN MLPP Service Domain (2nd Octet)							
9	Least Significant Bit (DSN MLPP Service Domain 3rd Octet)							

Bit 8 Set to 1 as an extension bit

Bits: 7-6 (Coding standard)
0 0 CCITT standardized coding
1 0 National Standard*
*The coding standard for DSN shall be assigned as "National."

Bit 5 (Spare)

Bits 4 3 2 1 (Precedence level)
0 0 0 0 (FLASH OVERRIDE – highest)
0 0 0 1 (FLASH)
0 0 1 0 (IMMEDIATE)
0 0 1 1 (PRIORITY)
0 1 0 0 (ROUTINE – lowest)
0 1 0 1
to (Spare)
1 1 1 1

Octet 4:

Bit 8 Set to 0/1 as an extension bit

Bits 7-6-5 (Spare)

Bit 4 (Change value)
0 Precedence level coding privilege may be changed at network boundaries
1 Precedence level coding privilege may not be changed at network boundaries

Bit 3 (Spare)

Bits 2-1 (Look Forward Busy (LFB) application) 00 LFB allowed 01 LFB not allowed 10 Path preserved 11 Spare
Octets 5-6 (Network Identity (NI)):
Each digit is coded in a binary decimal representation from 0 to 9. The first NI digit is coded 0. The Telephony Country Code (TCC) follows in the second to the fourth NI digits (the most significant TCC digit is in the second NI digit). If the TCC is one or two digits long, the excess digit(s) is inserted with the code for RPOA or network identification, if necessary. If octet 6 is not required, it is coded all zeros.
Octets 7-9 (DSN MLPP Service Domain)
A code expression in pure binary, the number allocated to a DSN MLPP Service Domain to identify a customer domain uniquely across multiple ISDN networks. Bit 8 of octet 7 is the most significant bit and bit 1 of octet 9 is the least significant bit.

5.2.2.7.3 Disconnect Message Information Cause Values

[Required: TS, EOS, SMEO, DVX-C, MFS, PBX1] The MLPP ISDN PRI Q.931 Disconnect message shall contain the following cause values, shown in Table 5.2.2-4, as defined in the ANSI Standards T1.619-1992 and T1.619a-1994.

Table 5.2.2-4. Disconnect Message Cause Value

DISCONNECT MESSAGE CAUSE VALUE	DESCRIPTION
8	Answered or Unanswered Call; Circuit is Not to be Reused
9	Answered or Unanswered Call; Circuit is to be Reused
46	Unavailable Resources; Precedence Call is Blocked with Equal or Higher Precedence Calls

5.2.2.7.4 Signal Information Element

[Required: TS, EOS, SMEO, DVX-C, MFS, PBX1] For providing tones and announcements, the Signal Information Element, as described in 4.5.24 of ANSI T1.607, shall be used with the following two U.S. national codepoints for signal values, as shown in Table 5.2.2-5.

Table 5.2.2-5. U.S. National Codepoints for Signal Values

SIGNAL VALUE	EXPLANATION	NORTH AMERICAN PRACTICE
9	Preemption tone is on	Precise tone is a continuous 440 Hz tone added to a 620 Hz tone
-	Precedence call alerting ringback tone on	Ringback tone (audible ringing tone) is a 440 Hz tone added to a 480 Hz tone repeated in a 1.64 s on, 0.36 s off pattern
66		Precedence call alerting 1.64 s on, 0.36 s off
Note – No signal value is assigned to "precedence call alerting ringback tone on" since the tone is always applied by the destination exchange. This ringback tone is as indicated in the table.		
Signal value (Octet 3) Bits 8 7 6 5 4 3 2 1 0 0 0 0 1 0 0 1 (9) Preemption tone 0 1 0 0 0 0 1 0 (66) Alerting on-pattern 2 (Special/priority alerting)		

5.2.2.7.5 ANSI T1.619a Setup Message Called Party Number Format

[Required: TS, MFS, EOS, SMEO, DVX-C, PBX1] The ANSI T1.619a ISDN Setup Message called party number format shall be as shown in Table 5.2.2-6, ANSI T1.619a ISDN Setup Message Called Party Number Format.

Table 5.2.2-6. ANSI T1.619a ISDN Setup Message Called Party Number Format

ACCESS DIGIT	PRECEDENCE DIGIT	ROUTE CONTROL DIGIT	AREA CODE	SWITCH CODE	LINE NUMBER
(N)[1,3]	(P)[1]	[Y][2]	(KXX)[3]	KXX	XXXX
LEGEND N is any digit from 2–9. P is any digit 0–4. X is any digit 0–9. K is any digit 2–8. Y is any digit 0–3.					
NOTES 1. The Access and Precedence digits may only be present on CPE interfaces that do not support ANSI T1.619a interfaces (e.g., Integrated Access and Video Teleconferencing services). The switching system shall process the precedence level of the call based on the precedence digit outpulsed in the Called Party Information Element in lieu of the Precedence Information Element in Code Set 5. 2. Digits shown in brackets [ ] are required only for TS and MFS switches and are not present on all calls. 3. Digits shown in parenthesis ( ) are not present on all calls.					

5.2.2.7.6 ANSI T1.619a and Non-ANSI T1.619a Interaction

[Required: TS, EOS, SMEO, DVX-C, MFS, PBX1]

1. Trunk-to-Trunk Tandem Calls. The switch shall have the capability to assign a default DSN MLPP service domain to an ANSI T1.619a trunk (i.e., ISDN PRI, SS7) that tandems from a non-ANSI T1.619a trunk (i.e., T1/E1 CAS, analog E&M, ISDN PRI, SS7). The default DSN MLPP service domain shall be assigned by the switch via the administration terminal, and shall be a range from 00 00 00 to FF FF FF in hexadecimal.

2. Trunk-to-Line Calls. The switch shall have the capability to assign a DSN MLPP service domain on a per line basis. The switch shall have the capability to assign a default DSN MLPP service domain to a line that terminates an incoming non-ANSI T1.619a trunk call.

3. Line-to-Trunk Calls. The switch shall have the capability to assign a default DSN MLPP service domain to an ANSI T1.619a trunk that originates from a line that is not assigned a DSN MLPP service domain. The switch shall allow calls placed from a line with or without an assigned DSN MLPP service domain to route over non-ANSI T1.619a trunks.

4. Interaction between Unlike MLPP Service Domains. The following rules apply for calls placed between unlike DSN MLPP service domains:

   a. The switch shall allow connection (i.e., line-to-trunk, trunk-to-line, trunk-to-trunk, or line-to-line) between unlike DSN MLPP service domains when resources are available.

   b. When a call is placed between unlike MLPP service domains, the switch shall classmark the DSN MLPP service domain of the connection (i.e., line-to-trunk, trunk-to-line, trunk-to-trunk, or line-to-line) based on the DSN MLPP service domain that entered the switch (trunk or line).

      (1) Example 1 – Line-to-Line. If an intraswitch call is placed between two subscribers with different DSN MLPP service domains, the switch shall classmark the connection with the DSN MLPP service domain of the originator.

      (2) Example 2 – Trunk-to-Trunk. If an incoming call is placed to a switch via a non-ANSI T1.619a trunk (i.e., T1/E1 CAS, analog E&M, SS7, ISDN PRI) that tandems to an ANSI T1.619a trunk, the switch shall assign the default DSN MLPP service domain to the outbound ANSI T1.619a trunk, and

classmark the connection as the switch-assigned default DSN MLPP service domain.

(3) Example 3 – Trunk-to-Line. If an incoming call is placed to a switch via a non-ANSI T1.619a trunk (i.e., T1/E1 CAS, analog E&M, SS7, ISDN PRI) that terminates to a line, the switch shall assign the default DSN MLPP service domain to the line and classmark the connection as the switch-assigned default DSN MLPP service domain.

(4) Example 4 – Line-to-Trunk. If a call is originated from a subscriber over a non-ANSI T1.619a trunk (i.e., T1/E1 CAS, analog E&M, SS7, ISDN PRI), the switch shall classmark the DSN MLPP service domain of the connection as the DSN MLPP service domain of the originator.

5. MLPP interaction shall not be allowed between unlike DSN MLPP service domains.

5.2.2.8 MLPP Interactions with Common Optional Station Features and Services

This section describes the requirements for MLPP interactions with other station features and services. These features and services shall not interact adversely with mandatory MLPP features.

5.2.2.8.1 Precedence Call Waiting

[Required: EOS, SMEO, MFS, PBX1 – Conditional: DVX-C, DVX-L] The following Precedence Call Waiting treatment shall apply to precedence levels of PRIORITY and above.

5.2.2.8.1.1 Busy with Higher Precedence Call

[Required: EOS, SMEO, MFS, PBX1 – Conditional: DVX-C, DVX-L] If the precedence level of the incoming call is lower than the existing MLPP call, precedence call waiting shall be invoked. If the incoming call is PRIORITY precedence or above, the precedence call waiting tone (see Table 5.2.4-5, DSN Information Signals) shall be applied to the called party.

5.2.2.8.1.2 Busy with Equal Precedence Call

[Required: EOS, SMEO, MFS, PBX1 – Conditional: DVX-C, DVX-L] The switch shall provide the precedence call waiting tone (see Table 5.2.4-5, DSN Information Signals) to the called station. The switch shall apply this tone regardless of other programmed features, such as

call forwarding on busy or caller ID. The called station shall be able to place the current active call on hold, or disconnect the current active call and answer the incoming call.

5.2.2.8.1.3 Busy with Lower Precedence Call

[Required: EOS, SMEO, MFS, PBX1 – Conditional: DVX-C, DVX-] The switch shall preempt the active call. The active busy station shall receive continuous preemption tone until an on-hook signal is received and the other party shall receive preemption tone for a minimum of 3 seconds. After going on-hook, the station to which the precedence call is directed shall be provided precedence ringing. The station shall be connected to the preempting call after going off-hook.

5.2.2.8.1.4 No Answer

[Required: EOS, SMEO, MFS, PBX1 – Conditional: DVX-C, DVX-L] If, after receiving the precedence call waiting signal, the busy called station does not answer the incoming DSN call within the maximum programmed time interval, the switch shall treat the call in accordance with UCR 2008, Section 5.2.2.3, Precedence Call Diversion.

5.2.2.8.2 Call Forwarding

[Required: EOS, SMEO, MFS, PBX1 – Conditional: DVX-C, DVX-L] The Call Forwarding feature is a settable terminating feature that is subscribed to by the called party. This feature shall permit user lines to direct calls either to another line or to an attendant. This feature will be either user activated by dialing the appropriate feature code followed by the address of the line to which calls are to be forwarded or will be assigned by the switch administrator. Calls forwarded to lines (numbers) that have this feature already activated may be forwarded again. The precedence level of calls shall be preserved during the forwarding process. The forwarding address may be any telephone number, subject to the class-of-service restrictions of the line activating the feature.

5.2.2.8.2.1 Call Forwarding at a Busy Station

[Required: EOS, SMEO, MFS, PBX1 – Conditional: DVX-C, DVX-L]

1. If the incoming call is of a higher precedence level than the established call (or calls, if three-way calling is established) at the busy station being called, all calls to the busy station shall be preempted and the incoming call shall be established, i.e., the Call Forwarding service shall not be invoked.

2. If the incoming call is of an equal or lower precedence level than the established call (or calls, if three-way calling is established) at a busy station being called, the Call Forwarding service shall be invoked.

3. If the called C2 user, Special C2 user, or other DSN user is non-preemptable (i.e., is not classmarked for preemption), the Call Forwarding service shall be invoked regardless of the precedence levels of incoming calls and established calls.

4. The precedence level of calls is preserved during the forwarding process, and the forwarded-to user may be preempted.

5. If the Call Forwarding Busy feature is activated, and a precedence call (i.e., PRIORITY and above) is forwarded (including possible multiple forwarding), and if this forwarded call is not responded to by any forwarded-to party within a specified period (e.g., 30 seconds), the call shall be diverted to an attendant.

5.2.2.8.2.2 Call Forwarding – No Reply at Called Station

[Required: EOS, SMEO, MFS, PBX1 – Conditional: DVX-C, DVX-L]

1. The precedence level of calls is preserved during the forwarding process, and the forwarded-to user may be preempted.

2. If the Call Forwarding feature is activated by the called party and the called party has specified a forwarded-to party, the forwarding procedure shall be performed. If a precedence call (i.e., PRIORITY and above) is forwarded (including possible multiple forwarding) and is not responded to by any forwarded-to party (e.g., called party busy with a call of equal or higher precedence level; or called party busy and nonpreemptable) within a specified period (e.g., 30 seconds), the call shall be diverted to an attendant.

5.2.2.8.3 Call Transfer

[Required: EOS, SMEO, MFS, PBX1 – Conditional: DVX-C, DVX-L] Two types of call transfers are normal and explicit. A normal call transfer is a transfer of an incoming call to another party. An explicit call transfer happens when both calls are originated by the same subscriber. The switch shall provide the interactions described in the following paragraphs, with both normal and explicit call transfers.

5.2.2.8.3.1 Call Transfer Interaction at Different Precedence Levels

[Required: EOS, SMEO, MFS, PBX1 – Conditional: DVX-C, DVX-L] When a call transfer (i.e., line-to-line, line-to-trunk, trunk-to-line, or trunk-to-trunk) is made at different precedence levels, the switch that initiates the transfer shall classmark the connection at the highest precedence level of the two segments of the transfer.

5.2.2.8.3.2 Call Transfer Interaction at Same Precedence Levels

[Required: EOS, SMEO, MFS, PBX1 – Conditional: DVX-C, DVX-L] The switch that initiates a call transfer (i.e., line-to-line, line-to-trunk, trunk-to-line, or trunk-to-trunk) between two segments that have the same precedence level shall maintain the precedence level upon transfer.

5.2.2.8.4 Call Hold

[Required: EOS, SMEO, MFS, PBX1 – Conditional: DVX-C, DVX-L] Call Hold is a function of the serving switch and shall be invoked by going on-hook, then off-hook. Calls on hold shall retain the precedence of the originating call. All lines are subject to normal preemption procedures.

Figure 5.2.2-4, Call Hold Scenarios, illustrates three typical call hold scenarios. In each scenario, caller #3 is on hold with caller #1, and caller #1 is talking to caller #2.

In scenario 1, caller #3 receives an incoming, higher precedence call from caller #4. Caller #3 receives preemption tone. Once caller #3 acknowledges the preemption tone by going on hook, the call between caller #4 and caller #3 is established when caller #3 answers caller #4. Caller #1 will receive preemption tone also only if caller #1 attempts to retrieve caller #3 while the preemption tone is being sent to caller #3. (NOTE: The preemption tone shall not be sent to caller #1 while active with caller #2. This would give caller #1 the false indication that the active call with caller #2 is being preempted.) Caller #2 remains connected to caller #1, and caller #1 does not receive any preemption notification.

In scenario 2, caller #1 receives an incoming, higher precedence call from caller #4. Caller #1, caller #2, and caller #3 receive preemption tone (see Table 5.2.4-5, DSN Information Signals). Once caller #1 acknowledges the preemption and then goes on hook, the higher precedence call from caller #4 is offered. Callers #2 and #3 are disconnected and the call between caller #4 and caller #1 is established.

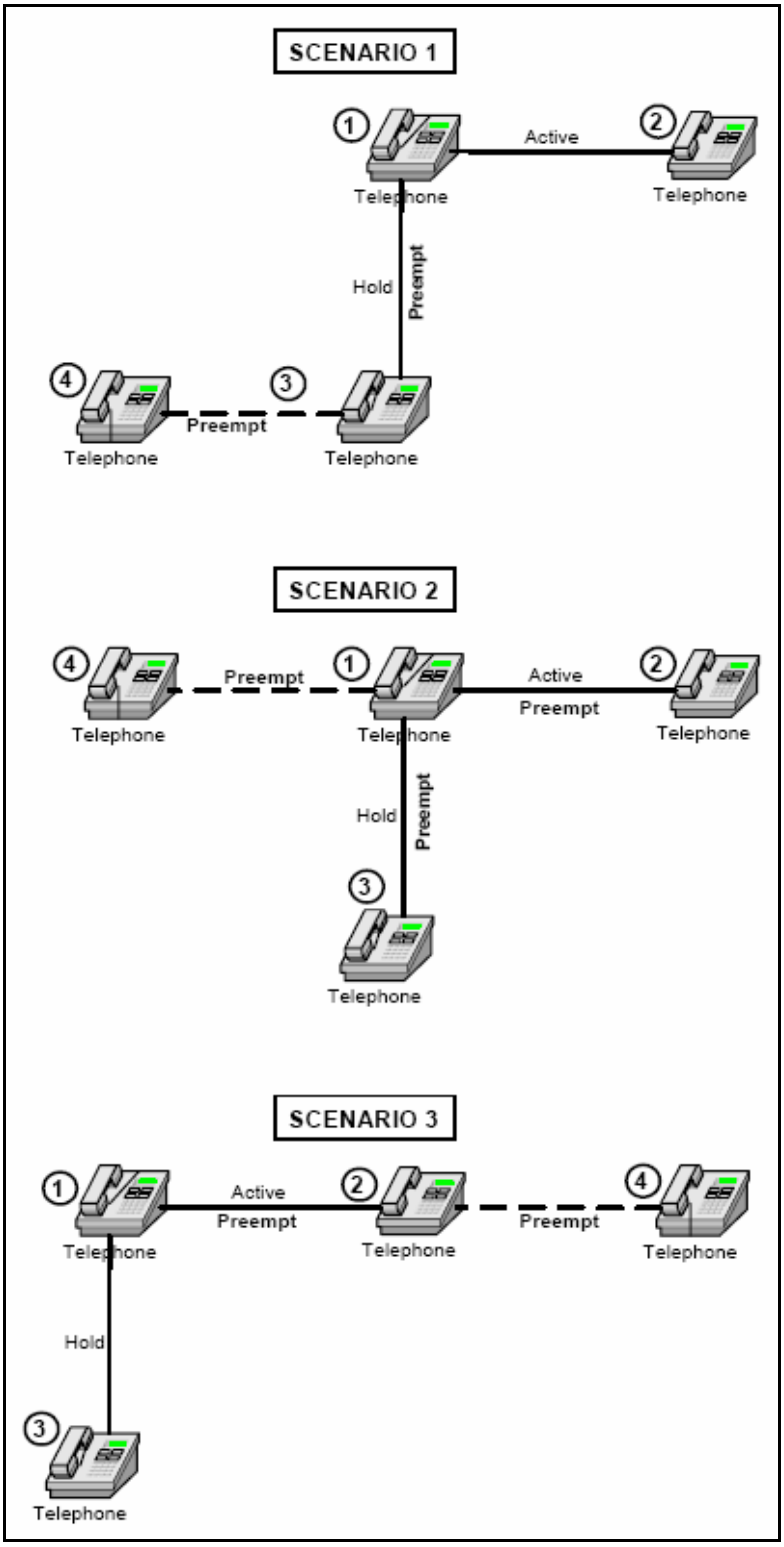


Figure 5.2.2-4. Call Hold Scenarios

In scenario 3, caller #2 receives an incoming, higher precedence call from caller #4. Caller #2 receives a preemption tone. Caller #1 receives a preemption tone. The tone indicates to caller #1 that caller #2 is being preempted. Once caller #1 goes on-hook, caller #1 receives a ringback from the call that is still on hold (caller #3).

5.2.2.8.5 Three-Way Calling

[Required: EOS, SMEO, MFS, PBX1 – Conditional: DVX-C, DVX-L] In three-way calling, each call shall have its own precedence level. When a three-way conversation is established, each connection shall maintain its assigned precedence level. Each connection of a call resulting from a split operation shall maintain the precedence level that it was assigned upon being added to the three-way conversation.

The switch shall classmark the originator of the three-way call at the highest precedence level of the two segments of the call. Incoming calls to lines participating in TWC that have a higher precedence than the highest of the two segments shall preempt unless the call is marked non-preemptable.

When a higher precedence call is placed to any one of the three-way call participants, that participant receives the preemption tone (see Table 5.2.4-5, DSN Information Signals). The other two parties shall receive a conference disconnect tone as described in Table 5.2.4-5. This tone indicates to the other parties that one of the other three-way call participants is being preempted.

In a three-way conference call where each connection is established at different precedence levels, the precedence level of the participant who initiated the three-way conference call shall be assigned the highest precedence of the two connections.

5.2.2.8.6 Call Pick-up

[Conditional: EOS, SMEO, DVX-C, DVX-L, MFS, PBX1] A user line that is equipped to answer any calls directed to other lines within the user's own preset pick-up group, as established by an administrative facility, by dialing the appropriate feature code.

1. If a call pick-up group has more than one party in an unanswered condition and the unanswered parties are at different precedence levels, a call pick-up attempt in that group shall retrieve the highest precedence call first. If multiple calls of equal precedence are ringing simultaneously, a call pick-up attempt in that group shall retrieve the longest ringing call first.

2. If a party in a call pick-up group is busy, and an incoming precedence call is placed to that number, normal MLPP rules shall apply. This call cannot be picked up within the call pick-up group unless it is an unanswered call, provided there are no additional features such as call waiting or call forwarding.

5.2.2.8.7 Conferencing

5.2.2.8.7.1 Conference Precedence Level

[Required: TS, MFS, EOS – Conditional: SMEO, DVX-C, DVX-L, PBX1] All addresses shall be processed at a precedence level equal to that precedence level dialed by the conference originator.

1. If all conference bridges are busy, ROUTINE precedence conference call attempts shall be connected to a "Line Busy" tone, and call attempts at precedence levels above the ROUTINE precedence shall re-examine all conference bridges on a preemptive basis.

2. A conference bridge that is busy at the lowest level of precedence stored for all units shall be preempted for a higher precedence conference call.

3. When a conference bridge is preempted, a 2-second burst of preemption tone shall be provided to the conferees on the existing conference. The existing connections to the bridge shall be dropped, and the bridge shall send an on-hook signal automatically to the associated switch ports to permit the new connections to be established.

4. Where the requesting precedence level is equal to, or lower than, the existing conference, the connection shall be denied and the caller shall be provided a BPA.

5.2.2.8.8 Multiline Hunt Service

[Conditional: EOS, SMEO, DVX-C, DVX-L, MFS, PBX1]

1. Pilot Line Hunt. This hunting feature is a group of access lines arranged so that a lead published number, the pilot number is called first. If the first station (pilot number) is busy, the call goes to the second and subsequent stations until an idle, or the last station in the hunt group is called. If all stations are busy, the calling party will receive a busy tone (unless other forwarding, etc., features are present on the station).

2. Distributed Hunt. This hunting feature is a group of access lines arranged so that incoming calls are sent to the station in the group that has been idle the longest.

3. Circular Hunt. This hunt feature is a group of access lines arranged so that if any station in the hunt group is busy, hunting starts at the next station, and continues through the rest of the group. This hunting feature will rotate or search the idle status of the lines in the group at least once (one cycle) before a busy tone is sent.

4. MLPP Interactions, Line Hunting. If no line is available and one or more existing calls are of lower precedence level than that of the incoming call, an existing call of the lowest precedence level within the group shall be preempted.

A BPA is returned only when all remaining lines in the hunt group are found busy with calls of equal or higher precedence.

If this feature is provided, it shall be in accordance with Telcordia Technologies GR-569-CORE, *Multiline Hunt Service*, Issue 1, June 2000.

5.2.2.8.9 Community of Interest

[Required: TS, EOS, MFS, SMEO – Conditional: DVX-C, PBX1]

The COI service enables users to form groups, to and from which access is subject to special restrictions and privileges. The service is primarily provided for users who generate the majority of their traffic to each other.

The COI service is provided as a switch based feature as opposed to a network-wide feature (i.e., no COI information is transported between switches). The COI service is provided by specific COI screening for originating and terminating call requests. The screening is based on the COI group information and user classmarks.

Members of a specific COI can communicate among themselves, but not, in general, with users external to the COI group. Specific COI members can have additional capabilities that allow them to originate calls external to the COI group and/or to receive calls external to the COI group. Specific COI groups can be configured with additional capabilities that prevent the COI members from originating calls to other members of the COI group, or from receiving calls from other members of the COI group.

The COI service also provides specific COI precedence treatment for calls originating from a COI member and/or calls received by a COI member.

5.2.2.8.9.1 Definition of Terms

1. Community of Interest Group. The Community of Interest feature enables users to form groups, to and from which access is subject to special restrictions and privileges. A COI group consists of a COI Screening list, a COI Precedence level, and COI group classmarks.

2. COI Screening List. A COI Screening list specifies individual destinations or codes representing groups of destinations. Each code in this list can be from 3 to 15 digits. Outgoing calls are screened against this list together with the COI group classmarks to either allow/deny the call request.

3. COI Precedence Level. This COI precedence level specifies a precedence level that is either required or allowed, depending upon the COI group classmarks, for calls to/from users of a COI group.

4. COI Member. A user that has a COI group assigned is defined as being a member of that COI group.

5. Calls Internal and External to COIs. The COI is a switch-based feature as opposed to a network-wide feature, i.e., no COI information is transported between switches. Calls are defined as being internal to the COI if:

   a. For an outgoing call request, the dialed destination matches a code in the user's COI screening list

   b. For local calls only, an incoming call request is to a user who is assigned to the same COI group as the calling user.

   All other local calls to/from a COI member, including incoming interswitch call requests received via trunk facilities, are treated as external calls to the COI. Call requests received via incoming trunk facilities are also deemed external but these do not undergo any COI screening and hence are not subject to the special COI restrictions and privileges.

6. COI Group Classmarks. The COI group classmarks specify the outgoing and incoming call restrictions/privileges for calls internal to the COI group. The COI group classmarks are defined as follows:

   a. COI Outgoing Classmarks. A COI group user with no outgoing classmarks limits the COI user to making calls, which are internal to the COI only, i.e., to only those destination codes which are specified within the COI screening list. The user is allowed to exercise the normal authorized precedence level for these calls.

b. Outgoing Precedence Allowed. The COI user is allowed to exercise up to and including the COI precedence for calls internal to the COI.

c. Outgoing Precedence Mandatory. Only COI precedence calls are permitted for calls internal to the COI.

d. Outgoing Calls Barred within the COI. This restriction means that a COI user cannot make calls to destination codes specified in the COI screening list.

7. COI Incoming Classmarks. A COI group user with no incoming classmarks limits the COI user to receiving local calls from members of those COIs of which the user is a member. All other local calls are restricted. There is no restriction on calls received over trunk facilities since these do not undergo COI screening.

   a. Incoming Precedence Mandatory. This COI service only permits calls internal to the COI that are at the COI precedence level. This only applies for local calls, which are internal to the COI (i.e., if the local calling user is a member of those COIs of which the user is a member).

   b. Incoming Calls Barred within the COI. This restriction means that a COI user cannot receive calls from members of those COIs of which the user is a member. Unless the member classmark incoming access option is applied, calls from other non-COI members or other COI members are also restricted.

   c. COI Member Classmarks. In addition to the COI group classmarks that are part of the COI group, specific COI members can also have COI classmarks at the subscriber level that specify the type of incoming and outgoing call restrictions/privileges for calls external to the COI.

8. COI Outgoing Access. Outgoing access allows a COI user to make calls external to the COI, i.e., to all other destination codes not specified in the COI screening list (i.e., external to the COI). The user is only allowed to exercise the normal authorized precedence level for these calls.

9. Incoming Access. Incoming access allows a COI user to receive local calls from all other non-COI users and from those other COI users who allow outgoing access.

10. Incoming Access with Precedence. Incoming access with precedence allows a COI user to receive only local COI precedence level calls from all other non-COI users and from those other COI users who allow outgoing access.

5.2.2.8.9.2 Feature Requirements

The COI feature enables users to form groups, to and from which access is subject to special restrictions and privileges. A user that has a COI group assigned is defined as being a member of that COI group. A specific user may be a member of up to eight different COI groups. The switch shall support a minimum of 24 COI groups.

Essentially, normal call establishment procedures apply, but to provide the COI service the switch screens the call request in conjunction with the COI information of the calling and/or the called user together with the COI user classmarks. As a result of this analysis, the call either fails (i.e., routed to intercept) for COI reasons or is allowed to proceed. Depending on whether the call fails due to a precedence check or a destination screening check, the intercept treatment applied is either "precedence blocked" or "destination not allowed."

5.2.2.8.9.2.1 COI Screening Treatment for Originating Call Requests

[Required: SMEO, EOS, MFS – Conditional: DVX-C, PBX1] To provide COI service for outgoing calls, the switch analyzes the call request in conjunction with the COI data, i.e., the maximum precedence level allowed and calling area of the calling user. If the call is internal to the COI, i.e., the dialed destination matches a code in the user's COI screening list, and then the COI group classmarks are used to either fail the call or allow it to proceed.

In cases where a user is a member of more than one COI, the call is screened against each COI screening list, in the order the COIs were assigned to the user, until a match of the dialed destination and precedence is found. If a match is found, the call is treated as being internal to that COI and the COI group classmarks are used to either fail the call or allow it to proceed. If there is no such match, then the first COI that has a match on the dialed destination is chosen as the COI. If there is no COI that has a match on the dialed destination, then the call is deemed external to the COI.

If the call is external to any of the COIs assigned to the user, then the user's classmarks are used to either fail the call or allow it to proceed.

Table 5.2.2-7, COI Checks for an Originating Call Request, describes the COI screening treatment for the different COI group classmarks and the COI member classmarks for an originating call request.

Table 5.2.2-7. COI Checks for an Originating Call Request

CALLING USER	INTERNAL/ EXTERNAL TO COI	COI GROUP OG CLASSMARK	CALLED PARTY COI MEMBER	DISPOSITION OF ORIGINATING CALL CLASSMARK REQUEST
COI Member	Internal	None	X	Allowed – User can exercise normally authorized precedence level
		OG Precedence Allowed	X	Allowed – User can exercise up to and including the COI precedence level
		OG Precedence Mandatory	X	Allowed – Only with the COI precedence level, else denied
		OG Calls Barred within COI	X	Denied – COI restriction
	External	X	None	Denied – COI restriction
			COI OG Access	Allowed – User can exercise normally authorized precedence level
No COI Assigned	X		X	Normal call and precedence handling
X = Don't Care				

If the COI members' classmarks indicate that incoming access is allowed only with COI precedence calls, then the called user's COI(s) precedence is used to determine if access is allowed or denied. In cases where a called user is member of more than one COI, the call is screened against each COI screening list, in the order the COIs were assigned to the user, until a match of the call precedence is found. If a match is found, the call is allowed, otherwise it is denied.

If the call is internal to the COI (i.e., calls from local users who are members of the same COI group as the called user), the COI's group classmarks are used to fail the call for COI reasons or allow the call to proceed.

Table 5.2.2-8, COI Checks for a Terminating Call Request, describes the COI screening treatment for the different COI group classmarks and the COI member classmarks for a terminating call request.

5.2.2.8.9.2.2 COI Screening Treatment for Terminating Call Requests

[Required: SMEO, EOS, MFS – Conditional: DVX-C, PBX1] To provide COI service for incoming calls, the switch analyzes the call request in conjunction with the COI data of the called user and calling user for local calls and the COI data of the called user for calls external to the switch.

Table 5.2.2-8. COI Checks for a Terminating Call Request

CALLED USER	INTERNAL / EXTERNAL TO COI	COI GROUP IC CLASSMARK	CALLED PARTY COI MEMBER CLASSMARK	DISPOSITION OF TERMINATING CALL REQUEST
No COI Assigned	X		X	Normal call and precedence handling
COI Member	Internal	None	X	Allowed – Precedence handling per normal
		IC Precedence Mandatory	X	Allowed only if call precedence matches COI precedence
		IC Calls Barred within COI	X	Denied – COI restriction
	External (Local Calls)	X	None	Denied – COI restriction
			COI IC Access	Allowed – Precedence handling per normal
			COI IC Access with Precedence	Allowed only if call precedence matches COI precedence
	External Trunk Calls	X	X	Allowed – These calls are handled as normal. No COI screening is performed for these calls.
X = Don't Care				

If the call is external to the COI, the called COI member's classmarks, are used to either fail the call for COI reasons or allow it to proceed. The following calls are external to the COI:

- Calls incoming on interswitch trunk facilities
- Calls from local users who are not members of any COI groups
- Calls from local users who are not members of the called users COI group

5.2.2.8.9.2.3 Billing

Call detail recording already records the call precedence level, which may be escalated due to the COI service. There are no additional call detail recording requirements for the COI feature.

5.2.2.8.9.2.4 Traffic

There are no additional traffic requirements for the COI service.

5.2.2.9 MLPP CCS7

[Required: TS, MFS, EOS – Conditional: SMEO, DVX-C] Requirements for MLPP CCS7 shall be in accordance with ANSI Standards T1.619-1992 and T1.619a-1994.

5.2.2.9.1 General Description

Common Channel Signaling System No. 7 (i.e., SS7 or CCS7) is a global standard for telecommunications defined by the ITU-T. The standard defines the procedures and protocol by which network elements in the PSTN exchange information over a digital signaling network to effect wireless (cellular) and wire line call setup, routing and control. The ITU definition of SS7 allows for national variants, such as the ANSI and Telcordia Technologies (Bell Communications Research) standards used in North America, and the ETSI standard used in Europe.

The SS7 network and protocol are used for the following:

- Basic call setup, management, and tear down
- Wireless services, such as personal communications services (PCS), wireless roaming, and mobile subscriber authentication
- Local number portability (LNP)
- Toll-free (800/888) and toll (900) wire line services
- Enhanced call features, such as call forwarding, calling party name/number display, and three-way calling
- Efficient and secure worldwide telecommunications

5.2.2.9.2 Definitions

Definitions of terms can be found in UCR 2008, Appendix A, Section A2, Glossary and Terminology Description.

5.2.2.9.3 Look-Ahead for Busy

[Conditional: TS, MFS, EOS, SMEO, DVX-C] Look-Ahead for Busy (LFB) is an information unit used to find out whether network resources are available to support the higher

precedence call. The switch shall provide the LFB feature in accordance with ANSI Standards T1.619-1992 and T1.619a-1994.

5.2.2.9.4 Precedence Parameters

[Required: TS, MFS, EOS – Conditional: SMEO, DVX-C] The MLPP CCS7 IAM shall contain the Precedence parameter and subfields, as shown in Table 5.2.2-9, CCS7 IAM Precedence Parameter and Subfields. The subfields in the Precedence parameter identify the precedence level, the network identification, and domain, and whether a path has been reserved or path reservation is allowed.

Table 5.2.2-9. CCS7 IAM Precedence Parameter and Subfields

OCTET BIT	8	7 6	5	4 3 2 1
1	Spare	LFB	Spare	Precedence Level
2	1st Network Identity Digit			2nd Network Identity Digit
3	3rd Network Identity Digit			4th Network Identity Digit
4	Most Significant Bit DSN MLPP Service Domain (1st Octet)			
5	DSN MLPP Service Domain (2nd Octet)			
6	Least Significant Bit DSN MLPP Service Domain (3rd Octet)			

In case of congestion, IAMs carrying FLASH or FLASH OVERRIDE precedence calls shall be assigned Level 3, IMMEDIATE precedence calls shall be assigned Level 2, PRIORITY precedence calls shall be assigned Level 1, and ROUTINE precedence calls shall be assigned Level 0 in the CCS7.

Table 5.2.2-10, Precedence Parameter Subfields Codes, shows the codes used in the Precedence parameter subfields.

5.2.2.9.4.1 Actions Required at Originating Exchange

[Required: MFS, TS, EOS – Conditional: SMEO, DVX-C] Routing information in the MLPP CCS7 shall be supplied by the originating exchange. However, the design shall not preclude requests to a remote database for routing information.

Table 5.2.2-10. Precedence Parameter Subfields Codes

Octet 1
Bit 8 (Spare)
Bits 7-6 (Look Forward Busy (LFB) application) 00 LFB allowed 10 LFB not allowed 01 Path reserved 11 Spare
Bit 5 (Spare)
Bits 4 3 2 1 (Precedence level) 0 0 0 0 (FLASH OVERRIDE – highest) 0 0 0 1 (FLASH) 0 0 1 0 (IMMEDIATE) 0 0 1 1 (PRIORITY) 0 1 0 0 (ROUTINE – lowest) 0 1 0 1 to (Spare) 1 1 1 1
Octets 2-3 contain a code for Network Identity (NI). Each digit is coded in binary coded decimal representation from 0 to 9. The first digit of this field is coded 0. The Telephony Country Code (TCC) follows in the second to fourth NI digits (the most significant TCC digit is in the second NI digit). If the TCC is one or two digits long, the excess digit(s) is inserted with the code for RPOA or network identification, if necessary. If octet 3 is not required, it is coded all zeros.
Octets 4-6 contain a code expressing in pure binary representation the number allocated to an MLPP service domain. These numbers are allocated from the set of National Business Group Identifier codes in accordance with the procedures in Annex B, in chapter T1.119.9 of ANSI T1.113.

5.2.2.9.4.2 MLPP CCS7 TCAP – Definitions and Functions of Transaction Capability Operations, Parameters, and Error Codes

[Required: MFS, TS, EOS – Conditional: SMEO, DVX-C] The MLPP CCS7 functions and encoding for the Operation, Parameter, and Error Code elements used by the Transaction Capability Application Part (TCAP) Protocol shall be as specified in ANSI T1.114.5-2000. The DSN-specific requirements not covered by the ANSI standards are specified in the following paragraphs, citing the applicable sections of the ANSI standard.

5.2.2.9.4.2.1 Parameters

[Required: MFS, TS, EOS – Conditional: SMEO, DVX-C] Several DSN-specific parameters needed to support the MLPP service are specified in the following paragraphs, citing the applicable sections in the ANSI standard if they exist:

5.2.2.9.4.2.1.1 Bearer Capability Supported – 10010011

[Required: MFS, TS, EOS – Conditional: SMEO, DVX-C] The Bearer Capability Supported parameter indicates whether a requested bearer capability is supported and is used to indicate the reason a bearer capability requested was not available. The format of the parameter is illustrated in Figure 18 of ANSI T1.114.5. The contents of this parameter are defined and coded as follows:

1	00000001	– Bearer capability is not supported.
2	00000010	– Bearer capability is supported.
3	00000011	– Bearer capability is not authorized.
4	00000100	– Bearer capability is not presently available.
5	00000101	– Bearer capability is not implemented.

5.2.2.9.4.2.1.2 Circuit Identification Code – 10011010

[Required: MFS, TS, EOS – Conditional: SMEO, DVX-C] The Circuit Identification Code parameter is used to identify the physical path between two exchanges. The parameter is coded contextual, is two octets in length, and is of the type OCTET STRING. The format and coding is as described in ANSI T1.113.3, Section 1.2.

5.2.2.9.4.2.1.3 Call Reference – 10011100

[Required: MFS, TS, EOS – Conditional: SMEO, DVX-C] The Call Reference parameter is used to identify a particular MLPP call within an exchange independent of the physical circuits. The parameter is six octets in length and is of the type OCTET STRING. The format contents are as specified in ANSI T1.113.3, Section 3.5, and Figure 7/T1.113.3.

5.2.2.9.5 RELEASE Message Cause Values

[Required: TS, MFS, EOS – Conditional: SMEO, DVX-C] The MLPP CCS7 RELEASE message shall contain the following cause values as defined in the ANSI Standards T1.619-1992 and T1.619a-1994, and shown in Table 5.2.2-11, RELEASE Message Cause Values.

Table 5.2.2-11. RELEASE Message Cause Values

RELEASE MESSAGE CAUSE VALUE	DESCRIPTION
8	Answered or Unanswered Call; Circuit is Not to be Reused
9	Answered or Unanswered Call; Circuit is to be Reused
46	Unavailable Resources; Precedence Call is Blocked with Equal or Higher Precedence Calls

5.2.2.9.6 DSN MLPP CCS7 IAM Called Party Number Format

[Required: TS, MFS, EOS – Conditional: SMEO, DVX-C] The MLPP CCS7 IAM called party number format shall be as shown in Table 5.2.2-12.

Table 5.2.2-12. DSN Switch MLPP CCS7 IAM Called Party Number Format

ROUTE DIGIT	ROUTE CONTROL DIGIT	AREA CODE	SWITCH CODE	LINE NUMBER
X	[Y]	(KXX)	KXX	XXXX
LEGEND X is any digit 0–9. K is any digit 2–8. Y is any digit 0–3.				
NOTE: Digits shown in brackets [ ] are only required for tandem and multifunction switches, and are not present on all calls. Digits shown in parenthesis ( ) are not present on all calls.				

Mixed-media backbone utilizes various modes of signaling consisting of intraswitch/interswitch terminations that will ensure clear-channel data transmission of speeds up to 56 kbps on a network basis. The DSN also supports Switched 64 kbps (SW64) clear-channel transmission through selective routing using CAS on PCM-30 (E-1) terminations and CCS protocols, such as ISDN PRI and DSN SS7 on both PCM-24 (bipolar with eight-zero substitution (B8ZS)/Extended Superframe (ESF)) and PCM-30 terminations.

The switch shall support the required circuit-switched system call-processing treatment/handling of call types (i.e., line-to-trunk, trunk-to-line, and trunk-to-trunk) in a mixed-media backbone by the use of the DSN World Wide Numbering and Dialing Plan (WWNDP), as shown in Table 5.2.2-13 and Table 5.2.2-14. The switch shall support this call-processing treatment/handling of calls with the DSN WWNDP formats, described in UCR 2008, Section 5.2.3.5.2, DSN Switch Outpulsing Digit Formats. The switch shall support the call-processing treatment/handling of calls, as shown in Table 5.2.2-13 and Table 5.2.2-14, using CAS MF(R1) 2/6 signaling. If the SMEO supports CAS MF(R1) 2/6 signaling, the call-processing treatment/handling of calls are required, as shown in Table 5.2.2-13 and Table 5.2.2-14.

Table 5.2.2-13. CAS-to-CCS Trunk Interworking Matrix (Line-to-Trunk and Trunk-to-Line)

REF NO.	ORIGINATING (TERM/TRUNK)	ROUTE DIGIT	BEARER CAPABILITY	TERMINATING (TERM/TRUNK)	ROUTE DIGIT	BEARER CAPABILITY
Line-to-Trunk						
1	Analog User	0/5	N/A	T1 CAS	0/5	N/A
2	Analog User	0/5	N/A	T1 SS7*	0/5	SP
3	Analog User	0/5	N/A	E1 CAS	0/5	N/A
4	Analog User	0/5	N/A	E1 SS7*	0/5	SP
5	Analog User	0/5	N/A	T1 PRI	N/A	SP
6	Analog User	0/5	N/A	E1 PRI	N/A	SP
7	Analog User	1/6	N/A	T1 CAS	1/6	N/A
8	Analog User	1/6	N/A	T1 SS7*	1/6	SP
9	Analog User	1/6	N/A	E1 CAS	1/6	N/A
10	Analog User	1/6	N/A	E1 SS7*	1/6	SP
11	Analog User	1/6	N/A	T1 PRI	N/A	SP
12	Analog User	1/6	N/A	E1 PRI	N/A	SP
13	ISDN BRI	0/5	SP	T1 CAS	0/5	N/A
14	ISDN BRI	0/5	SP	T1 SS7*	0/5	SP
15	ISDN BRI	0/5	SP	E1 CAS	0/5	N/A
16	ISDN BRI	0/5	SP	E1 SS7*	0/5	SP
17	ISDN BRI	0/5	SP	T1 PRI	N/A	SP
18	ISDN BRI	0/5	SP	E1 PRI	N/A	SP
19	ISDN BRI	1/6	SP	T1 CAS	1/6	N/A
20	ISDN BRI	1/6	SP	T1 SS7*	1/6	SP
21	ISDN BRI	1/6	SP	E1 CAS	1/6	N/A
22	ISDN BRI	1/6	SP	E1 SS7*	1/6	SP
23	ISDN BRI	1/6	SP	T1 PRI	N/A	SP
24	ISDN BRI	1/6	SP	E1 PRI	N/A	SP
25	ISDN BRI	0/5	56K CMD	T1 SS7*	1/6	56K CMD
26	ISDN BRI	0/5	56K CMD	E1 CAS	1/6	N/A
27	ISDN BRI	0/5	56K CMD	E1 SS7*	1/6	56K CMD
28	ISDN BRI	0/5	56K CMD	T1 PRI	N/A	56K CMD
29	ISDN BRI	0/5	56K CMD	E1 PRI	N/A	56K CMD
30	ISDN BRI	0/5	64K CMD	T1 SS7*	1/6	64K CMD
31	ISDN BRI	0/5	64K CMD	E1 CAS	1/6	N/A
32	ISDN BRI	0/5	64K CMD	E1 SS7*	1/6	64K CMD
33	ISDN BRI	0/5	64K CMD	T1 PRI	N/A	64K CMD
34	ISDN BRI	0/5	64K CMD	E1 PRI	N/A	64K CMD
35	ISDN BRI	0/5	64K CMD	T1 CAS	1/6	N/A
36	ISDN BRI	1/6	56K CMD	T1 SS7*	1/6	56K CMD
37	ISDN BRI	1/6	56K CMD	E1 CAS	1/6	N/A
38	ISDN BRI	1/6	56K CMD	E1 SS7*	1/6	56K CMD
39	ISDN BRI	1/6	56K CMD	T1 PRI	N/A	56K CMD
40	ISDN BRI	1/6	56K CMD	E1 PRI	N/A	56K CMD

REF NO.	ORIGINATING (TERM/TRUNK)	ROUTE DIGIT	BEARER CAPABILITY	TERMINATING (TERM/TRUNK)	ROUTE DIGIT	BEARER CAPABILITY
Line-to-Trunk (continued)						
41	ISDN BRI	1/6	64K CMD	T1 CAS	1/6	N/A
42	ISDN BRI	1/6	64K CMD	T1 SS7*	1/6	64K CMD
43	ISDN BRI	1/6	64K CMD	E1 CAS	1/6	N/A
44	ISDN BRI	1/6	64K CMD	E1 SS7*	1/6	64K CMD
45	ISDN BRI	1/6	64K CMD	T1 PRI	N/A	64K CMD
46	ISDN BRI	1/6	64k CMD	E1 PRI	N/A	64K CMD
Trunk-to-Line						
47	T1 CAS	0/5	N/A	Analog User	N/A	N/A
48	T1 SS7*	0/5	SP	Analog User	N/A	N/A
49	E1 CAS	0/5	N/A	Analog User	N/A	N/A
50	E1 SS7*	0/5	SP	Analog User	N/A	N/A
51	T1 PRI	0/5	SP	Analog User	N/A	N/A
52	E1 PRI	0/5	SP	Analog User	N/A	N/A
53	T1 CAS	1/6	N/A	Analog User	N/A	N/A
54	T1 SS7*	1/6	SP	Analog User	N/A	N/A
55	E1 CAS	1/6	N/A	Analog User	N/A	N/A
56	E1 SS7*	1/6	SP	Analog User	N/A	N/A
57	T1 PRI	1/6	SP	Analog User	N/A	N/A
58	E1 PRI	1/6	SP	Analog User	N/A	N/A
59	T1 CAS	0/5	N/A	ISDN BRI	N/A	SP
60	T1 SS7*	0/5	SP	ISDN BRI	N/A	SP
61	E1 CAS	0/5	N/A	ISDN BRI	N/A	SP
62	E1 SS7*	0/5	SP	ISDN BRI	N/A	SP
63	T1 PRI	N/A	SP	ISDN BRI	N/A	SP
64	E1 PRI	N/A	SP	ISDN BRI	N/A	SP
65	T1 SS7*	1/6	SP	ISDN BRI	N/A	SP
66	E1 PRI	1/6	SP	ISDN BRI	N/A	SP
67	E1 SS7*	1/6	SP	ISDN BRI	N/A	SP
68	T1 PRI	N/A	SP	ISDN BRI	N/A	SP
69	T1 SS7*	0/5	56K CMD	ISDN BRI	N/A	56K CMD
70	E1 SS7*	0/5	56K CMD	ISDN BRI	N/A	56K CMD
71	T1 PRI	0/5	56K CMD	ISDN BRI	N/A	56K CMD
72	E1 PRI	0/5	64K CMD	ISDN BRI	N/A	64K CMD
73	T1 SS7*	0/5	64K CMD	ISDN BRI	N/A	64K CMD
74	E1 SS7*	0/5	64K CMD	ISDN BRI	N/A	64K CMD
75	T1 PRI	0/5	64K CMD	ISDN BRI	N/A	64K CMD
76	E1 PRI	0/5	64K CMD	ISDN BRI	N/A	64K CMD
77	T1 CAS	1/6	N/A	ISDN BRI	N/A	56K CMD
78	T1 SS7*	1/6	56K CMD	ISDN BRI	N/A	56K CMD
79	E1 SS7*	1/6	56K CMD	ISDN BRI	N/A	56K CMD
80	T1 PRI	N/A	56K CMD	ISDN BRI	N/A	56K CMD
81	E1 PRI	N/A	56K CMD	ISDN BRI	N/A	56K CMD

REF NO.	ORIGINATING (TERM/TRUNK)	ROUTE DIGIT	BEARER CAPABILITY	TERMINATING (TERM/TRUNK)	ROUTE DIGIT	BEARER CAPABILITY
Trunk-to-Line (continued)						
82	T1 SS7*	1/6	64K CMD	ISDN BRI	N/A	64K CMD
83	E1 CAS	1/6	N/A	ISDN BRI	N/A	64K CMD
84	E1 SS7*	1/6	64K CMD	ISDN BRI	N/A	64K CMD
85	T1 PRI	N/A	64K CMD	ISDN BRI	N/A	64K CMD
86	E1 PRI	N/A	64K CMD	ISDN BRI	N/A	64K CMD
*Signaling System No.7 (SS7) for the SMEO is conditional.						
LEGEND 56K/64K = 56/64 Kilobits per Second CMD = Circuit Mode Data N/A = Not Applicable SP = Speech or 3.1K Bearer Capability						

Table 5.2.2-14. CAS-to-CCS Trunk Interworking Matrix (Trunk-to-Trunk)

REF NO.	INCOMING TRUNK	ROUTE DIGIT	BEARER CAPABILITY	OUTGOING TRUNK	ROUTE DIGIT	BEARER CAPABILITY
Trunk-to-Trunk						
1	E1 CAS	1/6	N/A	T1/E1 SS7*	1/6	64K CMD
2	E1 CAS	0/5	N/A	T1/E1 SS7*	0/5	SP
3	T1 CAS	1/6	N/A	T1/E1 SS7*	1/6	56K CMD
4	T1 CAS	0/5	N/A	T1/E1 SS7*	0/5	SP
5	E1 CAS	1/6	N/A	T1/E1 PRI	N/A	64K CMD
6	E1 CAS	0/5	N/A	T1/E1 PRI	N/A	SP
7	T1 CAS	1/6	N/A	T1.E1 PRI	N/A	56K CMD
8	T1 CAS	0/5	N/A	T1/E1 PRI	N/A	SP
9	T1/E1 PRI	N/A	56/64K CMD	E1 CAS	1	N/A
10	T1/E1 PRI	N/A	SP	E1 CAS	0	N/A
11	T1/E1 PRI	N/A	56/64K CMD	T1 CAS	1	N/A
12	T1/E1 PRI	N/A	SP	T1 CAS	0	N/A
13	T1/E1 SS7*	1/6	56/64K CMD	T1 CAS	1/6	N/A
14	T1/E1 SS7*	1/6	SP	T1 CAS	1/6	N/A
15	T1/E1 SS7*	1/6	56/64K CMD	E1 CAS	1/6	N/A
16	T1/E1 SS7*	1/6	SP	E1 CAS	1/6	N/A
17	T1/E1 SS7*	0/5	SP	E1 CAS	0/5	N/A
18	T1/E1 SS7*	0/5	56/64K CMD	E1 CAS	1/6	N/A
19	T1/E1 SS7*	0/5	SP	T1 CAS	0/5	N/A
20	T1/E1 SS7*	0/5	56/64K CMD	T1 CAS	1/6	N/A
21	T1/E1 SS7*	1/6	56/64K CMD	T1/E1 PRI	N/A	56/64K CMD
22	T1/E1 SS7*	1/6	SP	T1/E1 PRI	N/A	SP
23	T1/E1 SS7*	0/5	56/64K CMD	T1/E1 PRI	N/A	56/64K CMD
24	T1/E1 SS7*	0/5	SP	T1/E1 PRI	N/A	SP

REF NO.	INCOMING TRUNK	ROUTE DIGIT	BEARER CAPABILITY	OUTGOING TRUNK	ROUTE DIGIT	BEARER CAPABILITY
*Signaling System No.7 (SS7) for the SMEO is conditional.						
LEGEND 56K/64K 56/64 Kilobits per Second CMD Circuit Mode Data				N/A Not Applicable SP Speech or 3.1K Bearer Capability		

Route selection for CCS data routes (circuit mode data) and CAS data routes with route digits 1 (Switched Data) or 6 (Hotline Data) shall not include:

- Analog trunks
- Trunks with data compression
- A-law to µ-law and/or µ-Law to A-Law conversions – Data restrictions

If the bearer capability (BC) of speech or 3.1K audio conflicts with data route digits 1 or 6, then no A-law to µ-law or µ-Law to A-Law conversions will be performed. If a BC of 56 kbps (restricted or unrestricted) or 64 kbps (restricted or unrestricted) conflicts with a voice route digit of 0 or 5, then no conversion will be performed. ISDN PRI call handling/treatment does not use the dialed route digit in accordance with the DSN WWNDP; however, when the originator dials the data route code the switch shall assign the appropriate bearer capability (i.e., 56 kbps data, 64 kbps data). All tandem calls of the same media type (i.e., SS7-to-SS7, CAS-to-CAS, PRI-to-PRI) are transparent. Tandem calls of different media type shall follow the treatment/call handling in accordance with Table 5.2.2-13, CAS-to-CCS Trunk Interworking Matrix (Line-to-Trunk and Trunk-to-Line), and Table 5.2.2-14, CAS-to-CCS Trunk Interworking Matrix (Trunk-to-Trunk). Signaling System No.7 shall be considered conditional for the SMEO.

5.2.2.10 MLPP Interactions with Electronic Key Telephone Systems Features

5.2.2.10.1 Electronic Key Telephone Systems

[Conditional: MFS, EOS, SMEO, DVX-C, PBX1] Electronic Key Telephone Systems functions shall be provided by the switch as described in Telcordia Technologies GR-205-CORE, *Generic Requirements for ISDN Electronic Key Telephone Systems*, Issue 1, February 1996. Additional MLPP requirements are listed in the following paragraphs.

5.2.2.10.1.1 Call Appearances

[Conditional: MFS, EOS, SMEO, DVX-C, PBX1] A call appearance shall be shared by all EKTS users. There shall not be separate call appearances for MLPP calls. All users shall be able to originate the authorized precedence level and receive all levels of precedence on a single call appearance for each directory number. Each EKTS call appearance shall comply with the

MLPP functionality specified in UCR 2008, Section 5.2.2, Multilevel Precedence and Preemption.

5.2.2.10.1.2 Hold

[Conditional: MFS, EOS, SMEO, DVX-C, PBX1] The EKTS Hold function shall comply with the requirements of UCR 2008, Section 5.2.2.8.4, Call Hold.

5.2.2.10.1.3 Directory Number Bridging

[Conditional: MFS, EOS, SMEO, DVX-C, PBX1] The EKTS Directory Number Bridging function shall comply with the requirements of UCR 2008, Section 5.2.2.8.5, Three-Way Calling.

5.2.2.10.1.4 Intercom Calling

[Conditional: MFS, EOS, SMEO, DVX-C, PBX1] The EKTS Intercom Calling feature shall not prevent the offering of an MLPP call to any of the parties involved in an intercom call.

5.2.2.10.1.5 Abbreviated or Delayed Ringing Treatment on Incoming Calls

[Conditional: MFS, EOS, SMEO, DVX-C, PBX1] Incoming MLPP calls shall be considered as "distinctive alerting" and shall not be affected by the Abbreviated or Delayed Ringing Treatment. Precedence Alerting (see Table 5.2.4-4, DSN Ringing Tone and Cadence) shall be applied to the call directory number appearance and the call handled as described in UCR 2008, Section 5.2.2.6, ISDN MLPP BRI. If the call is not answered and the EKTS-T1 time expires, the call shall be diverted to an operator. If Call Forwarding-No Reply is invoked by the called directory number, then the Call Forwarding procedures of UCR 2008, Section 5.2.2.8.2.2, Call Forwarding – No Reply at Called Station, apply at the expiration of the EKTS-T1 timer.

5.2.2.10.1.6 Bridged Call Exclusion

[Conditional: MFS, EOS, SMEO, DVX-C, PBX1] The Bridged Call Exclusion (BCE) feature (automatic or manual) shall not degrade or prevent the MLPP interactions described in this section.

5.2.2.10.1.7 Non-ISDN Users

[Conditional: MFS, EOS, SMEO, DVX-C, PBX1] Non-ISDN users (analog telephone) can be assigned as members of the EKTS group. The non-ISDN user will share a call appearance

with other members of the EKTS group and shall be able to originate the authorized precedence level and receive all levels of precedence on that shared appearance.

5.2.2.11 Backward Compatibility

This section details the requirements for interoperability of the DSN utilizing the old cause values and precedence parameters. These requirements are needed only until all DSN switches have been upgraded with the ANSI T1.619a signaling.

5.2.2.11.1 Precedence Parameter

[Conditional: MFS, EOS, SMEO, DVX-C, PBX1] New DSN switches must interoperate with both the current 1992/1994 ANSI T1.113 MLPP CCS7 IAM, which contains the Precedence Parameter 6-octet field shown in Table 5.2.2-9, CCS7 IAM Precedence Parameter and Subfields.

5.2.2.11.2 Cause Values and Location Codes

[Conditional: MFS, EOS, SMEO, DVX-C, PBX1] The supplement to ANSI T1.619-1992, ANSI T1.619a-1994, revised the standard so that the exchange-to-exchange signaling is consistent with ITU-T recommendations, which were approved after the publication of ANSI T1.619-1992.

The use of cause value #45, preemption, shall continue to be used as described in ANSI T1.619-1992. This shall not conflict with the use of cause values #8 and #9 as described in ANSI T1.619a-1994 (supplement to ANSI T1.619-1992). The corresponding location code for each cause value (45, 8, and 9) shall operate as described in ANSI T1.619-1992 and ANSI T1.619a-1994.

5.2.2.12 Network Management Manual Controls

[Required: TS, EOS, MFS – Conditional: SMEO, DVX-C, DVX-L] Call gapping shall not apply to FLASH and FLASH OVERRIDE calls. In addition, FLASH and FLASH OVERRIDE calls shall be exempt from Cancel to (CANT) and Cancel from (CANF). See UCR 2008, Section 5.2.8, Network Management, for details.

5.2.2.13 Data Collection

[Required: EOS, SMEO, DVX-C, MFS – Conditional: DVX-L] The settable fields for Call Detail Recording (CDR) shall be as shown in Table 5.2.8-1, CDR Data. All DSN call data must identify the precedence level of the call.

5.2.3 Call Processing

5.2.3.0 Introduction

This section covers the call processing requirements of DSN switching systems. The section is modeled after the Telcordia GR-505-CORE, *Call Processing*, Issue 1, December 1997. It describes originating and terminating calls involving individual lines and DSN unique call processing associated with military unique features. No feature or function specifically identified in UCR 2008 or in the referenced standards shall prevent the completion or connection of a PRIORITY or higher precedence call. Call processing includes the following subject areas:

- Origination Treatments
- Termination Treatments
- Release Treatment
- Interruption Treatment
- Routing
- Dual Homing
- Spill Forward Control
- User Access Line Call Processing
- PBX Access Lines
- Preemption in the Network
- Glare Resolution
- Code Interpretation
- Screening

The requirements in GR-505-CORE shall be followed for processing DSN ROUTINE precedence calls. This section specifies the requirement for processing DSN precedence calls and other DSN-unique call processing requirements.

5.2.3.1 Call Treatments

Call treatments describe the interactions between a local switching system and a line or trunk during call processing and explains associated system actions required. The treatments are: origination, termination, release, and interruption.

5.2.3.1.1 Origination Treatment

[Required: TS, EOS, MFS, SMEO, DVX-C, DVX-L, PBX1, PBX2] Origination covers processing a call from the detection of a seizure until either the call is abandoned or complete code information has been received. Release treatments for ISDN and CCS7 lines and trunks are not required on DSN switching systems that do not include ISDN and CCS7 capabilities. DSN

origination treatment shall be as specified in Telcordia Technologies GR-505-CORE, *Call Processing*, Issue 1, December 1997, paragraph 3 and all subparagraphs. In addition, the following origination treatments are required.

5.2.3.1.1.1 Originating Busy

[Required: TS, EOS, MFS, SMEO, DVX-C, DVX-L, PBX1, PBX2] The originating line or trunk shall be marked originating busy when a seizure is recognized by the switch. Calls in an originating busy condition shall not be preempted until after the precedence level is determined. The precedence level shall be determined any time after the first digit is presented or dialed but no later than the last digit.

5.2.3.1.2 Termination Treatment

[Required: TS, EOS, MFS, SMEO, DVX-C, DVX-L, PBX1, PBX2] Termination treatment covers call processing from the point at which the system has received sufficient code information to determine the destination until either the call is answered and a transmission path is established, or until the appropriate treatment has been applied to calls that cannot be completed. Release treatments for ISDN and CCS7 lines and trunks are not required on DSN switching systems that do not include ISDN and CCS7 capabilities. DSN termination treatment shall be as specified in Telcordia Technologies GR-505-CORE, *Call Processing*, Issue 1, December 1997, paragraph 4 and all subparagraphs. In addition, the following termination treatments are required.

5.2.3.1.2.1 Busy or Idle Status

[Required: TS, EOS, MFS, SMEO, DVX-C, DVX-L, PBX1 – Conditional: PBX2] Lines or trunks preempted and marked for reuse shall be marked busy at the precedence level of the preempting call.

5.2.3.1.3 Release Treatment

[Required: TS, EOS, MFS, SMEO, DVX-C, DVX-L, PBX1, PBX2] Release treatment is the actions that the switching system shall take in response to disconnect signals when a call is in the talking state. DSN release treatment for reasons other than preemption shall be as specified in Telcordia Technologies GR-505-CORE, *Call Processing*, Issue 1, December 1997, paragraph 5. Release treatments for ISDN and CCS7 lines and trunks are not required on DSN switching systems that do not include ISDN and CCS7 capabilities.

5.2.3.1.4 Interruption Treatment

[Required: TS, EOS, MFS, SMEO, DVX-C, DVX-L, PBX1, PBX2] Interruption treatment is the response to requests for interruption of a call in progress. DSN interruption treatment shall be as specified in Telcordia Technologies GR-505-CORE, *Call Processing*, Issue 1, December 1997, paragraph 6.

5.2.3.1.5 Connections

[Required: TS, EOS, MFS, SMEO, DVX-C, DVX-L, PBX1, PBX2] DSN switches shall provide switched service connections as specified in Telcordia Technologies GR-505-CORE, *Call Processing*, Issue 1, December 1997, paragraph 2.3 and all subparagraphs.

5.2.3.1.6 Class of Service

[Required: TS, EOS, MFS, SMEO, DVX-C, DVX-L – Conditional: PBX1, PBX2] The switch shall provide classmarks to indicate each separate privilege, restriction, or special instruction for processing incoming and outgoing calls. The switch shall have the capability to assign classmarks in any combination to a single station line, access line, number code, trunk, or group of trunks. A minimum of 256 classmarks shall be provided. A subset of classmarks for trunk/trunk group shall include as a minimum the following:

1. Separate trunk/trunk group for originating and terminating, for each precedence level (i.e., ROUTINE through FLASH-OVERRIDE inclusive), traffic without local preemption. This feature shall not interfere with normal DSN network preemption and shall be allowed on DSN local adjacent access connections (i.e., VTC dedicated systems/NGN campus networks) and shall be allowed on the DSN network access connections to non-DSN networks i.e., NCN/PSTN/NGN networks).

2. All categories of trunk/trunk group listed above shall be capable of additional and independent classmarks to control voice only; data only; and, voice and data combined and additional and independent classmarks to control traffic based on the transmission medium selected i.e., Terrestrial/Satellite; Clear/Compressed; Echo Cancelled/Non-Echo Cancelled.

5.2.3.2 Primary and Alternate Routing

[Required: TS, MFS] DSN tandem level switches shall be capable of routing all calls to a primary route and up to nine alternate routes. Each route shall have the capability of including a minimum of four (4) trunk groups or subtrunk groups for separately grouping various categories of traffic such as voice, data, satellite, and terrestrial transmission.

[Required: EOS, SMEO, DVX-C – Conditional: DVX-L] DSN EOS and SMEO switches shall be capable of routing all calls to a primary route and to at least five (5) alternate routes with a minimum of one (1) trunk group per route and up to 96 trunk members per trunk group.

[Conditional: PBX-1] DSN PBX-1 switches shall be capable of routing all calls to a primary route and to at least one (1) alternate route.

5.2.3.3 User Access Line Call Processing (Non-CCS/ISDN Type)

5.2.3.3.1 E&M Lead Signaling States

[Conditional: TS, EOS, SMEO, MFS, DVX-C, DVX-L, PBX1, PBX2]

The switch shall provide E&M lead signaling states as described in Table 5.2.3-1.

Table 5.2.3-1. E&M Lead Signaling States

STATE	DESCRIPTION
E-Lead On-Hook Transitions	The DSN switch shall recognize or send an on-hook state, or the transition to the on-hook state, when: Open (represented by a ground through 20K ohms of resistance or greater) is detected or sent on a Type I E-lead, OR The E&SG lead loop is open (the full sensor voltage of the E-lead will be present) on a Type II E-lead.
E-Lead Off-Hook Transitions	The DSN switch shall recognize or send an off-hook state, or a transition to the off-hook state, when: Ground (represented by a ground through a resistance of 150 ohms or less) is detected or sent on a Type I E-lead, OR The E&SG lead loop is closed (The SG-lead will apply ground to the E-lead) on a Type II E-lead.
M-Lead On-Hook Transitions	The DSN switch shall recognize or send an on-hook state, or a transition to the on-hook state, when: Ground (the voltage between the M-lead and ground will not exceed 1 volt) is detected or sent on a Type I M-lead, OR The M&SB lead loop is open (the full sensor voltage of the M-lead will be present) on a Type II M-lead.

STATE	DESCRIPTION
M-Lead Off-Hook Transitions	The DSN switch shall recognize or send an off-hook state, or the transition to the off-hook state, when: Battery (in the range of -42.5 to -52.5 volts) is detected on the M-lead. The potential of the M-lead will not drop more than 2.5 volts under a 500 milliampere load on a Type I M-lead, OR The M&SB lead loop is closed (the SB-lead will apply battery to the M-lead) on a Type II M-lead.

5.2.3.3.2 4-Wire Analog User Access Lines

[Required: DVX-L – Conditional: TS, EOS, SMEO, MFS, DVX-C, PBX1, PBX2]

The call processing actions relative to 4-wire user lines are described in Table 5.2.3-2, and will be the same for Type I, Type II, and Type V E&M signaling. The switch shall recognize state changes on the 4-wire user access line in accordance with the criteria shown in Table 5.2.3-2.

Table 5.2.3-2. Call Processing – 4-Wire User Access Lines

CALL CASE	DESCRIPTION
Origination of ROUTINE or Precedence Calls	The DSN switch shall accept call originations from a 4-wire user access line when: The station or transmission equipment requests service via an off-hook transition on its SIG OUT leads, AND The DSN switch shall react by returning a dial tone on its VF OUT leads toward the station or transmission equipment. The DSN SIG OUT leads remain on-hook. Then station or transmission equipment the outpulses the called number (including any precedence digits) in DTMF on its VF OUT leads toward the DSN, AND If the call is blocked or unable to complete, the DSN switch shall return the proper tone or announcement on its VF OUT leads toward the station or transmission equipment. The DSN SIG OUT leads remain on-hook, AND If the call is completed, the DSN switch shall return answer supervision as an off-hook transition on its SIG OUT leads toward the station or transmission equipment.

CALL CASE	DESCRIPTION
Origination of ROUTINE or Precedence Calls (continued)	Disconnect is indicated from the station and transmission equipment end by an on-hook transition on its SIG OUT leads exceeding 180 ms. The DSN expects the station and transmission equipment to provide a release guard interval of 600–800 ms before seizing the access line for another call, OR If the 4-wire access line is connected to a 4-wire telephone and is allowed features invoked by switch hook flash (i.e., attendant recall, call waiting, three-way calling, conference), the disconnect window is extended to 2000 ms by the DSN.
Termination of ROUTINE Calls	The DSN switch shall terminate ROUTINE calls to 4-wire user access lines by: Returning ring back-tone to the calling party, AND Seizing the station or transmission equipment with an off-hook transition on the DSN SIG OUT leads, AND Applying ROUTINE alerting as on-hook and off-hook transitions on the DSN SIG OUT leads. AND The station or transmission equipment returns answer supervision as an off-hook transition on its SIG OUT leads to the DSN when the called user answers. Disconnect is indicated from either the DSN or station equipment end by an on-hook transition on the respective SIG OUT leads. The DSN switch shall invoke timed disconnect (15 seconds) on terminating calls to user access lines if the calling user remains off-hook after the access line has gone on-hook. The DSN switch shall provide a release guard interval of 600–800 ms before terminating another call to the access line.
Termination of Precedence Calls (Access Line Idle)	The DSN switch shall terminate precedence calls to an idle 4-wire user access line by: Returning precedence ringback tone to the calling user, AND Seizing the station or transmission equipment with an off-hook transition on the DSN SIG OUT leads, AND Applying precedence alerting as on-hook/off-hook transitions on the DSN SIG OUT leads until the called party answers or the call is abandoned. AND The station or transmission equipment returns answer supervision as an off-hook transition on its SIG OUT leads when the called user answers, AND

CALL CASE	DESCRIPTION
Termination of Precedence Calls (Access Line Idle) (continued)	Disconnect is indicated from either the DSN or station equipment end by an on-hook transition on the respective SIG OUT leads. The DSN switch shall invoke timed disconnect (15 seconds) on terminating calls to user access lines.
Termination of Precedence Calls (Access Line Busy)	The DSN switch shall preempt a call in progress and terminate a precedence call to a busy 4-wire user access line by: Applying a 340 to 350 ms on-hook transition toward the station or transmission equipment on the DSN SIG OUT leads. AND Then the DSN applies a preemption notification tone to its VF OUT leads until an on-hook transition is detected on the station and transmission equipment SIG OUT leads, AND When the station and transmission equipment is on-hook, the DSN switch shall terminate the preempting call as previously described for the "Access Line Idle" call case, using precedence alerting, if the preemption was for the affected 4-wire access line.

5.2.3.3.3 2-Wire User Access Lines

[Required: EOS, SMEO, DVX-C, MFS, PBX1 – Conditional: PBX2, DVX-L]

The switch shall provide the call processing actions as described in Table 5.2.3-3. The electrical characteristics assume that the connected user terminal equipment meets or exceeds the specification in Part 68 of the Federal Communications Commission (FCC) rules.

Table 5.2.3-3. Call Processing – 2-Wire User Access Lines

CALL CASE	DESCRIPTION
Idle State	While in the idle state the DSN switch shall: Provide resistance ground of a nominal 200 ohms on the tip conductor, AND Provide resistance battery of -21.5 to -56.5 volts dc on the ring conductor. The DSN expects the station equipment to provide a dc resistance across the tip and ring conductors, or from either conductor to ground, greater than 15,000 ohms.

CALL CASE	DESCRIPTION
Origination of ROUTINE Precedence Calls	The DSN switch shall accept call originations from 2-wire or user access lines when: The station equipment requests service by placing a dc resistance less than 2310 ohms (including station equipment resistance) across the T and R leads, AND The DSN switch shall react by returning dial-tone on the T and R leads when it is ready to receive address digits, AND The station equipment sends the called number (including any precedence digits) in either the DP or the DTMF mode. AND If the call is blocked or unable to be completed, the DSN switch shall return the proper tone or announcement toward the station equipment, AND The DSN shall not return reverse battery supervision when the called user answers on the 2-wire user access line. Disconnect shall be detected by the DSN switch if the dc resistance across the T and R leads exceeds 10,000 ohms for greater than 180 ms. This applies unless the access line is allowed special features that are activated by switchhook flash (i.e., attendant recall, call waiting, three-way calling, and conference). If the switchhook flash is expected, the disconnect detection interval is extended to 2000 ms by the DSN switch.
Termination of ROUTINE and Precedence Calls (Access Line Idle)	The DSN switch shall terminate ROUTINE and higher precedence calls to 2-wire users access lines by: Returning ringback-tone toward the calling user, AND Applying ringing generator toward the station equipment as an ac voltage of 92.5 ± 32.5 volts at 20 Hz ± 3 Hz, superimposed on -21.5 to -56.5 volts dc, AND The cadence of the ringing toward the station equipment is 2 seconds ON, followed by 4 seconds OFF for ROUTINE precedence calls. For precedence calls, ringing toward the station equipment is 1.64 seconds ON, followed by 0.36 seconds OFF. The appropriate cadence is continued until the called party answers or the calling party goes on-hook AND

CALL CASE	DESCRIPTION
Termination of ROUTINE and Precedence Calls (Access Line Idle) (continued)	While in the ringing state, the station equipment must: Not allow more than 3 mA of dc current to flow. Maintain an impedance across the T and R leads greater than 1400 ohms. Maintain a dc resistance across the T and R leads, or from either T and R to ground, greater than 10,000 ohms, AND Remove ringing generator (ring trip): Shall occur when a dc resistance less than 2310 ohms (including station resistance) is applied across the T and R leads. May occur during the ringing generator on interval. The DSN switch shall remove the ringing voltage within 200 ms after detecting ring trip. May occur during the ringing OFF (or silent) interval. Ringing transient and timing parameters are: Off-hook transitions from the station equipment less than 12 ms in duration shall be ignored and shall not cause ring trip, AND If ring trip occurs during the ringing generator ON period, the DSN switch shall remove ringing generator within 200 ms, AND Ring trip transitions with the DSN line interface circuitry shall not cause an open interval (or battery feed interruption) exceeding 20 ms, AND Ring trip without sustained answer supervision from the station equipment shall cause a ringback tone to remain toward the calling user. Upon detection of a valid answer from the station equipment, the DSN switch shall: Remove the ringback tone toward the calling user, AND Cut through the calling and called user. Disconnect is indicated from the station equipment when the dc resistance across the T and R leads exceeds 10,000 ohms for: 180 ms if the calling user is on-hook also, OR 15 seconds if the calling user is off-hook still. If the called user goes off-hook during this interval, normal conversation will continue,

CALL CASE	DESCRIPTION
Termination of ROUTINE and Precedence Calls (Access Line Idle) (continued)	OR 2000 ms if switchhook flash activated features are allowed.
Termination of Precedence Calls (Access Line Busy)	The DSN switch shall preempt a call in progress and terminate a precedence call to a busy 2-wire user access line by: Applying preemption notification tone to the T and R leads until the subscriber equipment goes on-hook, AND Terminating the call as previously described for a precedence call to an idle 2-wire user access line, if the preemption was for the affected 2- wire access line.

5.2.3.3.4 Termination to Analog Lines

5.2.3.3.4.1 Busy/Idle Status

[Required: EOS, SMEO, DVX-C, DVX-L, MFS, PBX1] Lines or trunks preempted and marked for reuse shall be marked busy at the precedence level of the preempting call.

5.2.3.4 DSN Interswitch Trunk Call Processing (Non-CCS/ISDN Type)

5.2.3.4.1 Originating Call Processing

[Required: TS, EOS, SMEO, DVX-C, DVX-L, MFS, PBX1] The call processing actions for originating calls to the DSN from on-net trunks are shown in Table 5.2.3-4.

Table 5.2.3-4. Originating Call Processing Toward DSN from DSN ISTs

CALL CASE	DESCRIPTION
Idle State	The DSN switch shall assume an idle state on its SIG IN leads when: Open (represented by a ground through 20K ohms of resistance or greater) is present on a Type 1 E-Lead, OR The E&SG lead loop is open (the full sensor voltage of the E lead is present) on a Type II E-lead, OR The M-lead is open (the full sensor voltage of the M-lead is present) on a Type V M-lead, OR The A and B bits of the received channel on the PCM-24 DIU are a “0.” OR

CALL CASE	DESCRIPTION
Idle State (continued)	The channel 16 supervisory bits indicate on-hook for the channel on a PCM-30 DIU.
Seizure by Connecting Office	The DSN switch shall recognize a call for service, or a transition to the off-hook state, on its SIG IN leads when: Ground (represented by a ground through a resistance of 150 ohms or less) is detected on a Type I E-lead, The E&SG lead loop is closed (the SG lead will apply ground to the E-lead) on a Type II E-lead, OR Ground is detected on a Type V M-lead, OR The A and B bits of the received channel on the PCM-24 DIU are a "1," OR The channel 16 supervisory bits indicate off-hook for the channel on a PCM-30 DIU.
Reaction by DSN Switch	When ready to receive address digits, the DSN switch shall return, as an off-hook transition on its SIG OUT leads, a wink-start or delay-dial signal, depending on the requirements of the connecting office.
Outpulsing of the Called Number by the Connecting DSN Switch	The distant office outpulses in the MF or DTMF mode. The address information required to complete the call shall be in accordance with the outpulsing formats found in Table 5.2.3-9 and Table 5.2.3-10.
Call Completion by DSN Switch	The DSN switching entity shall complete, or block, the call based on translation of the called number. If the call is blocked, or reaches a busy station not preemptable by the calling station, the DSN switch shall return the proper tone or announcement via its VF OUT leads. On-hook supervision shall remain on the DSN switch SIG OUT leads. If the desired station is idle, the DSN switch shall return a ROUTINE or PRECEDENCE ringback tone on its VF OUT leads. When the called station answers, answer supervision shall be returned as an off-hook transition on the DSN switch SIG OUT leads.
Preemption by Connecting Office (Unanswered Call)	Preemption by the connecting office on an unanswered call shall appear as a 328–to-362 ms on-hook transition, followed by off-hook supervision and another origination by the connecting office if the trunk is reused.
Preemption for Reuse by DSN Switch (Unanswered Call)	The DSN switch shall preempt for reuse an unanswered incoming call from the connecting office by returning on its SIG OUT leads: An off-hook transition of 95 to 105 ms, AND Followed by an on-hook transition of 340 to 350 ms, AND Followed by off-hook supervision.

CALL CASE	DESCRIPTION
Preemption Not for Reuse by DSN Switch (Unanswered Call)	The DSN switch expects the connecting office to make a transition to the on-hook state, followed by a wink-start or delay-dial signal when it is ready to accept the preempting call. Call processing from this point is the same as that described for Table 5.2.3-5. If a preemption is required on an unanswered incoming call from the connecting office, and the trunk shall not be reused, the DSN switch shall return on its SIG OUT leads: An off-hook transition of 95 to 105 ms, AND Followed by an on-hook transition of 340 to 350 ms, AND Followed by an off-hook transition of 95 to 105 ms, AND Followed by on-hook supervision. The DSN switch expects the connecting office to make a transition to the on-hook state.
Preemption for Reuse by Connecting Office (Answered Call)	The connecting office may preempt for reuse an answered call. The DSN switch shall detect a preemption of this type when: A 328-to-362 ms on-hook transition is detected on its SIG IN leads, AND Followed by off-hook supervision. The connecting office may preempt not for reuse an answered call. The DSN switch shall detect a preemption of this type when: A 328-to-362 ms on-hook transition is detected on its SIG IN leads, AND Followed by a 95-to-105 ms off-hook transition, AND Followed by on-hook supervision. The DSN switch shall react by preempting “not for reuse” the associated access line or trunk involved in the call, and returning on-hook supervision toward the connecting office.
Preemption for Reuse by DSN Switch (Answered Call)	The DSN switch shall initiate a preemption of this type by: Returning an on-hook transition of 340 to 350 ms toward the connecting office on the DSN switch SIG OUT leads, AND The DSN switch expects the connecting office to make a transition to the on-hook state, followed by a wink-start or delay-dial signal when it is ready to accept the preempting call. Call processing from this point is the same as that described for Table 5.2.3-5.

CALL CASE	DESCRIPTION
Preemption Not for Reuse by DSN Switch (Answered Call)	If a preemption is required on an answered call from the connecting office, and the trunk shall not be reused, the DSN switch shall return on its SIG OUT leads: An on-hook transition of 340 to 350 ms, AND Followed by an off-hook transition of 95 to 105 ms, AND The DSN switch expects the connecting office to make a transition to on-hook supervision.
Disconnect (Unanswered Call)	The DSN switch shall disconnect unanswered calls, and preemptions not for reuse on unanswered calls, if an on-hook transition exceeding 362 ms is received on the DSN switch SIG IN leads.
Disconnect (Answered Call)	The DSN switch shall provide calling party hold and timed disconnect. On-hook transitions exceeding 362 ms from the connecting office shall be considered a disconnect even though the called station is still off-hook. Calling party release shall prevail, and the DSN switch shall return on-hook supervision toward the connecting office. On-hook transitions from the called station exceeding 362 ms shall cause timed disconnect timing to commence. If the on-hook transition is less than 15 seconds, followed by off-hook supervision, conversation shall continue. If the on-hook transition exceeds 15 seconds, disconnect is assumed and the DSN switch shall commence permanent signal treatment on the incoming trunk from the connecting office.
Guard Interval	The DSN switch expects the connecting office to invoke a guard interval to allow sufficient time to release the call. For a trunk using terrestrial facilities, this guard interval must be 600 to 800 ms with a nominal value of 750 ms. For a trunk using satellite facilities, this guard interval must be 1050 to 1250 ms.

5.2.3.4.2 Terminating Call Processing

[Required: TS, EOS, SMEO, DVX-C, DVX-L, MFS, PBX1] The call processing actions for terminating calls from the DSN to on-net trunks are shown in Table 5.2.3-5, Terminating Call Processing from DSN-to-DSN ISTs.

Table 5.2.3-5. Terminating Call Processing from DSN-to-DSN ISTs

CALL CASE	DESCRIPTION
Idle State	The DSN switch shall present an idle state on its SIG OUT leads when: Ground (the voltage between the M-lead and ground shall not exceed 1 volt) is sent on a Type I M-lead, OR The M&SB lead loop is open (the full sensor voltage of the M-lead shall be present) on a Type II M-lead, OR The E-lead is open (the full sensor voltage of the E-lead shall be present) on a Type V E-lead, OR The A and B bits of the transmitted channel on the PCM-24 DIU are a "0," OR The channel 16 supervisory bits indicate on-hook for the channel on a PCM-30 DIU.
Seizure by the DSN Switch	The DSN switch shall initiate a call for service on its SIG OUT leads as an off-hook transition indicated by: Battery (in the range of -42.5 to -52.5 volts) is sent on the M-lead. The potential of the M-lead shall not drop more than 2.5 volts under a 500 milliampere load on a Type I M-lead, OR Closing the M&SB lead loop (the SB-lead shall apply battery to the M-lead) on a Type II M-lead, OR Ground is sent on a Type V E-lead, OR Setting the A and B bits of the transmitted channel on the PCM-24 DIU to a "1," OR Changing the supervisory bits on channel 16 to indicate off-hook supervision for the channel on a PCM-30 DIU.
Reaction by the Connecting Office	The DSN switch expects the connecting office, when ready to receive address digits, to return a delay-dial or wink-start signal as an off-hook transition detected by the DSN switch on its SIG IN leads.
Glare Resolution	Simultaneous seizure by the DSN switch and the connecting office results in a condition called "glare." The DSN switch shall resolve a glare condition depending on whether the trunk is wink-start or delay-dial, and whether it is to hold or release, when glare is detected, reselect once in the same trunk group. If no trunks are idle or preemptable, the DSN switch shall route advance. If a circuit is idle or preemptable and the failure occurs on the retrial, the DSN switch shall route advance.

CALL CASE	DESCRIPTION
Fault Detection and Retrial	The DSN switch shall detect fault conditions when terminating calls to the connecting office and react by reselecting another trunk.
Isolated Code Conditions	When routing encounters either of the following conditions: The complete trunk group including all routes is busied manually at either end of the circuit. or The complete trunk group including all routes is in a carrier group alarm state (e.g., red (Loss of Signal), yellow (Remote Alarm Indication), or blue (Alarm Indication Signal). The call shall be routed to an Isolated Code Announcement (ICA).
Outpulsing Called Number by DSN Switch	The DSN switch outpulses in the MF or DTMF mode. The address information required to complete the call shall be in accordance with the outpulsing formats found in Table 5.2.3-9 and Table 5.2.3-10.
Call Completion by the Connecting Office	The connecting switching entity must complete, or block, the call based on translation of the called number. If the call is blocked or reaches a busy station not preemptable by the calling station, the connecting office must return the proper tone or announcement to the DSN switch VF IN leads. On-hook supervision must remain on the DSN switch SIG IN leads. If the desired station is idle, the connecting office must return a ROUTINE or PRECEDENCE ringback tone to the DSN switch VF IN leads. When the called station answers, answer supervision must be returned as an off-hook transition on the DSN switch SIG IN leads.
Preemption by DSN Switch (Unanswered Call)	Preemption by the DSN switch on an unanswered call shall appear as a 340-to-350 ms on-hook transition, followed by off-hook supervision and another origination by the DSN switch if the trunk is reused.
Preemption for Reuse by Connecting Office (Unanswered Call)	The connecting office may preempt for reuse an unanswered outgoing call from the DSN switch by returning on the DSN switch SIG IN leads: An off-hook transition of 95 to 105 ms, AND Followed by an on-hook transition of 328 to 362 ms, AND Followed by off-hook supervision The DSN switch shall make a transition to the on-hook state, followed by a wink-start or delay-dial signal when it is ready to accept the preempting call. Call processing from this point is the same as that described for Table 5.2.3-4.

CALL CASE	DESCRIPTION
Preemption Not for Reuse by Connecting Office (Unanswered Call)	If a preemption is required by the connecting office on an unanswered outgoing call from the DSN switch, and the trunk shall not be reused, the connecting office must return on the DSN switch SIG IN leads: An off-hook transition of 95 to 105 ms, AND Followed by an on-hook transition of 328 to 362 ms, AND Followed by an off-hook transition of 95 to 105 ms, AND Followed by on-hook supervision The DSN switch shall make a transition to the on-hook state.
Preemption for Reuse by Connecting Office (Answered Call)	The connecting office may preempt for reuse an answered call. The DSN switch shall detect a preemption of this type when: A 328-to-362 ms on-hook transition is detected on its SIG IN leads, AND Followed by off-hook supervision. The DSN switch shall react by preempting "not for reuse" the associated access or trunk involved in the call. The DSN switch shall make an on-hook transition toward the connecting office, followed by a wink-start or delay-dial signal when it is conditioned to receive digits. Call processing from this point is the same as described for Table 5.2.3-4.
Preemption Not for Reuse by Connecting Office (Answered Call)	The connecting office may preempt not for reuse an answered call. The DSN switch shall detect a preemption of this type when: A 328-to-362 ms on-hook transition is detected on its SIG IN leads, AND Followed by a 95-to-105 ms off-hook transition, AND Followed by on-hook supervision. The DSN switch shall react by preempting "not for reuse" the associated access line or trunk involved in the call, and returning on-hook supervision toward the connecting office.
Preemption for Reuse by DSN Switch (Answered Call)	The DSN switch may preempt for reuse an answered call. The DSN switch shall initiate a preemption of this type by: Returning an on-hook transition of 340 to 350 ms toward the connecting office on the DSN switch SIG OUT leads, AND Followed by off-hook supervision.

CALL CASE	DESCRIPTION
	The DSN switch expects the connecting office to make a transition to the on-hook state, followed by a wink-start or delay-dial signal when it is ready to accept the preempting call. Call processing from this point is the same as described in Table 5.2.3-4.
Preemption Not for Reuse by DSN Switch (Answered Call)	If a preemption is required on an answered call to the connecting office, and the trunk shall not be reused, the DSN switch shall return on its SIG OUT leads: An on-hook transition of 340 to 350 ms, AND Followed by an off-hook transition of 95 to 105 ms, AND Followed by on-hook supervision. The DSN switch expects the connecting office to make a transition to on-hook supervision.
Disconnect (Unanswered Call)	Unanswered calls, and preemptions not for reuse or unanswered calls, shall be disconnected by the DSN switch with an on-hook transition on the DSN switch SIG OUT leads.
Disconnect (Answered Call)	The DSN switch shall provide calling party release and timed disconnect. On-hook transitions exceeding 362 ms from the DSN switch must be considered a disconnect by the connecting office even though the called station is off-hook still. Calling party release shall prevail and the connecting office must return on-hook supervision toward the DSN switch. On-hook transitions from the called station exceeding 362 ms shall cause timed disconnect timing to commence. If the on-hook transition is less than 15 seconds, followed by off-hook supervision, conversation shall continue. If the on-hook transition exceeds 15 seconds, disconnect is assumed and the DSN switch shall return on-hook supervision toward the connecting office on the DSN switch SIG OUT leads.
Guard Interval	The DSN switch shall invoke a guard interval to allow sufficient time for the connecting office to release the call. For terrestrial facilities, the guard interval shall be 600 to 800 ms (nominal value of 750 ms). For a trunk using satellite facilities, this guard interval shall be 1050 to 1250 ms.

5.2.3.5 Code Interpretation

5.2.3.5.1 DSN Worldwide Numbering and Dialing Plan

5.2.3.5.1.1 DSN User Dialing

[Required: TS, EOS, SMEO, DVX-C, DVX-L, MFS, PBX1] The switch shall operate with the dialing format illustrated in Table 5.2.3-6, DSN User Dialing Format. The parts shown in parentheses ( ) are not dialed by the DSN user on all calls.

Table 5.2.3-6. DSN User Dialing Format

ACCESS DIGIT	PRECEDENCE OR SERVICE DIGIT	ROUTE CODE	AREA CODE	SWITCH	LINE NUMBER
(N)	(P or S)	(1X)	(KXX)-	KXX	XXXX
Where: P is any precedence digit 0–4 and will be used on rotary-dial or 12-button DTMF keysets. S is the service digit 5–9. N is any digit 2–9. X is any digit 0–9. K is any digit 2–8.					
NOTES: 1. Digits shown in parentheses are not dialed by the DSN user on all calls. 2. The Access Digit plus the Precedence or Service Digit constitute the Access Code.					

5.2.3.5.1.2 Interswitch and Intraswitch Dialing

[Required: TS, EOS, SMEO, DVX-C, DVX-L, MFS, PBX1 – Conditional: PBX2] Seven-digit intraswitch dialing options as well as 7- and 10-digit interswitch dialing shall be supported by DSN switches.

5.2.3.5.1.2.1 Seven-Digit Dialing

[Required: TS, EOS, SMEO, DVX-C, DVX-L, MFS, PBX1] Seven-digit dialing shall consist of using the seven digits of the switch code and line number to establish either interswitch or intraswitch calls within the same numbering plan area. Number assignments for this plan shall be of the form KXX-XXXX, where X is any digit 0–9 and K is any digit 2–8. The specific KXX of each switch will be assigned by DISA to preclude conflicts with other switch codes. Access to the local attendant shall be obtained by dialing 0. The DSN ROUTINE precedence 7-digit interswitch or intraswitch calls are initiated by dialing the appropriate sequence of (1X) KXX-XXXX or 94 (1X) KXX-XXXX. The DSN calls above the ROUTINE precedence are initiated

by the appropriate sequence of 9P (1X) KXX-XXXX, where P is the precedence digit (0, 1, 2, or 3). Access to other Government and/or commercial services is obtained by dialing 9 followed by the appropriate service digit(s).

5.2.3.5.1.2.2 Ten-Digit Dialing

[Required: TS, EOS, SMEO, DVX-C, DVX-L, MFS, PBX1] Ten-digit dialing shall consist of using ten digits comprising the area code, switch code, and line number to establish interswitch calls where the number plan area of the calling party is different from the number plan area of the called party.

Number assignments for this plan shall be of the form KXX-KXX-XXXX, where K is any digit 2–8, and X is any digit 0–9. The DSN ROUTINE precedence 10-digit interswitch calls are initiated by dialing the appropriate sequence of (1X) KXX-KXX-XXXX or 94 (1X) KXX-KXX-XXXX. The DSN calls above the ROUTINE precedence are initiated by the appropriate sequence of 9P (1X) KXX- KXX-XXXX, where P is the precedence digit (0, 1, 2, 3 or 4). Access to other Government and/or commercial services is obtained by dialing 9 followed by the appropriate service digit(s).

5.2.3.5.1.3 Access Code

[Required: TS, EOS, SMEO, DVX-C, DVX-L, MFS, PBX1] The access code shall include the access digit, followed by the precedence digit or the service digit.

5.2.3.5.1.3.1 Access Digit

[Required: TS, EOS, SMEO, DVX-C, DVX-L, MFS, PBX1] The access digit (e.g., 9) shall provide the indication to the switch that the following digits will indicate either DSN call precedence, selected egress to the services of other systems or networks, or selected access to special DSN features, such as individual trunk tests.

5.2.3.5.1.3.2 Precedence Digit

[Required: TS, EOS, SMEO, DVX-C, DVX-L, MFS, PBX1] The precedence digit (0, 1, 2, 3, or 4) shall permit a DSN user to dial an authorized DSN precedence level from properly classmarked 12-button telephone instruments. When the 7-digit intraswitch dialing option is used, it is not necessary to dial or key the precedence access digit for ROUTINE precedence calls. The assignment of precedence digits is shown in Table 5.2.3-7, Precedence and Service Access.

5.2.3.5.1.3.3 Service Digits

[Required: TS, EOS, SMEO, DVX-C, DVX-L, MFS, PBX1] The service digits, 5 through 9, shall provide information to the switch to connect calls to government or public telephone services or networks that are not part of the DSN. The DSN switch will collect the access code and all routing and address digits before attempting to route a call to prevent numbering ambiguities between the access codes and the 2-digit abbreviated dial codes. The assignment of service access codes is shown in Table 5.2.3-7, Precedence and Service Access.

Table 5.2.3-7. Precedence and Service Access

ASSIGNMENTS FOR ROTARY DIAL, 12-BUTTON TELEPHONE KEYSETS		
ACCESS DIGIT	**PRECEDENCE DIGIT**	**PRECEDENCE**
e.g., 9	0	DSN FLASH OVERRIDE
e.g., 9	1	DSN FLASH
e.g., 9	2	DSN IMMEDIATE
e.g., 9	3	DSN PRIORITY
e.g., 9	4	DSN ROUTINE
ASSIGNMENTS FOR 15/16-BUTTON KEYSETS		
		PRECEDENCE
	FO	DSN FLASH OVERRIDE
	F	DSN FLASH
	I	DSN IMMEDIATE
	P	DSN PRIORITY
9	4	DSN ROUTINE
ASSIGNMENTS FOR SERVICE ACCESS CODES		
ACCESS DIGIT	**SERVICE DIGIT**	**PRECEDENCE**
e.g., 9	5	Off-Net 700 Services
e.g., 9	6	Not Assigned
e.g., 9	7	DSN CONUS FTS
e.g., 9	8	Not Assigned
e.g., 9	9	Local PTN

5.2.3.5.1.4 Route Code

[Required: TS, EOS, SMEO, DVX-C, DVX-L, MFS, PBX1] The route code is a special purpose DSN code that permits the customer to inform the switch of special routing or termination requirements. At the present time, the route code is used to determine whether a call will use circuit-switched data or voice-grade trunking. The route code may be used to disable echo suppressers and cancellers, and override satellite link control. It is not necessary to dial a route code for a non-hotline user voice. The first digit of the route code is a necessary part of the dialing plan to inform the switch that the next digit, the route digit, gives network instructions for specialized routing. The route code assignments are as shown in Table 5.2.3-8, Route Code

Assignments. Routing of hotline calls shall comply with Section 5.2.2.2.3, MLPP Trunk Selection (Hunting), (inclusive).

Table 5.2.3-8. Route Code Assignments

ROUTE CODE	ROUTE CODE USE
10	Voice Call (default)
11	Circuit-Switched Data
12	Satellite Avoidance (NA for CAS and Conditional for CCS)
13	Reserved
14	Reserved
*5	Hotline (Off-Hook) Voice Grade
*6	Hotline (Off-Hook) Data Grade
17	Reserved
18	Reserved
19	Reserved
*The user does not dial these route codes. The switch shall dial hotline calls automatically when an off-hook condition occurs and outpulse the appropriate route digit (i.e., hotline voice-5 or hotline data-6).	

5.2.3.5.1.5 Area Code

[Required: TS, EOS, SMEO, DVX-C, DVX-L, MFS, PBX1] The area code indicates the geographical part of the world or tactical unit (numbering plan area) in which a DSN user is assigned. It is a 3-digit code of the form KXX, assigned by DISA. The area code is used only when addressing a user outside of the originator's own numbering plan area.

5.2.3.5.1.6 Switch Code

[Required: TS, EOS, SMEO, DVX-C, DVX-L, MFS, PBX1] The switch code indicates the location of a switching center within a numbering plan area. It is a 3-digit code (see Table 5.2.3-9, DSN Switch MF(R1) Outpulsing Digit Format) in the form KXX assigned by DISA. This code must be dialed to address another switch in the same numbering plan area.

5.2.3.5.1.7 Line Number

[Required: TS, EOS, SMEO, DVX-C, DVX-L, MFS, PBX1] The line number is the switch-unique DSN user station identification. It is of the form XXXX. The line number groups cannot be assigned arbitrarily for each switch. The line number group assignments must be coordinated with the local connecting DSN or the host nation Public Telephone and Telegraph (PTT), and with DISA.

5.2.3.5.1.8 Caller ID

Caller identification (Caller ID) has two components: the caller's name and the caller's number. When a telephone has access to more than one network, confusion can occur, especially if the caller's telephone number from one network is delivered to the called party via another network. This is an important consideration when the call is for emergency services (e.g., 911) and the caller should be routed to the serving emergency service provider.

5.2.3.5.1.8.1 Calling Name Delivery

[Conditional: MFS, EOS, SMEO, DVX-C, PBX1, PBX2] The calling name delivery will remain the same for each call, regardless of the number of networks that can be accessed.

5.2.3.5.1.8.2 Calling Number Delivery

[Required: MFS, EOS, SMEO, DVX-C, PBX1 – Conditional: PBX2] The calling number provided to the called party shall be determined by the dial plan serving the calling instrument in accordance with Telcordia Technologies GR-31-CORE *"CLASS^{SM} Feature: Calling Number Delivery,"* Issue 1, June 2000. If the instrument has access to multiple networks, the network chosen for the call will determine the calling number to be delivered, except as noted in Section 5.2.1.4.1, 911 Service.

5.2.3.5.1.9 Emergency Service 911 Conflict Resolution

[Required: MFS, EOS, SMEO, PBX1 – Conditional: DVX-C, DVX-L] To prevent conflicts between 911 (emergency service) and 91-1-(KXX)-KXX-XXXX (FLASH data call), the switch shall be programmed in such a manner that 911 will be recognized. After 911 is dialed, or an access code and 911 (e.g., 9X911) is dialed and no other digits are received within 4 seconds (or after a # is dialed), the call will be treated as an emergency service call (911) and immediately processed. If additional digits are received within the 4-second period, the call will be treated as a non-emergency call and handled appropriately.

5.2.3.5.2 DSN Switch Outpulsing Digit Formats

Required: TS, EOS, MFS, DVX-C – Conditional: SMEO, PBX1, DVX-L] The switch outpulsing digit format for multifrequency R1 (MFR1) signaling shall be as shown in Table 5.2.3-9, DSN Switch MF(R1) Outpulsing Digit Format.

[Required: TS, EOS, MFS, SMEO, DVX-C, DVX-L – Conditional: PBX1] The switch outpulsing digit format for DTMF signaling shall be as shown in Table 5.2.3-10.

Table 5.2.3-9. DSN Switch MF(R1) Outpulsing Digit Format

	PRECEDENCE DIGIT	ROUTE DIGIT	ROUTE CONTROL DIGIT	AREA CODE	SWITCH CODE	LINE NUMBER	
[KP]	P	X	(Y)	(KXX)	KXX	XXXX	[ST]

Where:
P is any digit 0–4.
X is any digit 0–9.
Y is the digit 0–3 (required only for TS and MF switches). See notes.
K is any digit 2–8.
KP is the key pulse tone for MF(R1) 2/6 signaling inserted by the switch.
ST is the end of the signaling tone for MF(R1) 2/6 signaling inserted by the switch.

NOTES:
1. These switches shall have the option to send or receive a call with or without the route control digit.
2. Digits shown in parentheses ( ) are not present on all calls.

Table 5.2.3-10. DSN Switch DTMF Outpulsing Digit Format

PRECEDENCE DIGIT	ROUTE DIGIT	AREA CODE	SWITCH CODE	LINE NUMBER
(P)	(X)	(KXX)	KXX	XXXX

Where:
P is any digit 0–4 (standard digit format) or A, B, C, D (precedence digit format).
X is any digit 0–9.
K is any digit 2–8.
0 = Flash Override 1 = Flash 2 = Immediate 3 = Priority 4 = Routine
A = Flash Override B = Flash C = Immediate D = Priority

NOTES:
1. Digits shown in parentheses ( ) are not present on all calls. The switch shall have the ability to send or receive a call, with or without the route digit. Standard digit format only required for TS, EOS, and MFS.
2. Specific requirements for DTMF signaling can be found in Section 5.2.4.4.2, DTMF Signaling.

5.2.3.5.2.1 Route Control Digit

[Required: TS, MFS] The DSN Route Control Digit (RCD) provides optimum assurance, consistent with cost, for call completion, particularly of high precedence calls. Survivability is attained by exploiting the flexibility and efficiency of traffic routing capability inherent in the design of the switching system. The following assumptions and requirements apply:

1. Distribution of switching centers is consistent with traffic density and availability of transmission facilities.

2. All DSN MFS switching centers have the same classification in the network and the same operating capabilities. Each MFS switching center serves originating, terminating, and tandem traffic, exercises preemption, and provides automatic alternate routing.

3. Each DSN MFS/TS switching center is provided with inter-machine trunks from several of its immediate surrounding centers. Direct trunk groups are established between each center and other centers to provide improved accessibility and traffic handling.

4. Use of this feature shall be an additional functionality in call processing and shall not affect the call processing and treatment of calls that are classmarked for Method 1 and/or Method 2 trunk route selection for precedence calls above ROUTINE precedence.

5. Use of this feature shall not affect other routes or their associated attributes that are not assigned the RCD.

6. Use of this feature in the same switching center shall not restrict the use of other routes without the RCD.

7. Use of this feature shall be in accordance with the specified routing procedures for "exterior" and "interior" routing schemes as a minimum.

8. Use of this feature shall not affect automatic and manual network management controls.

5.2.3.5.2.1.1 Conceptual Backbone Network Structure

1. DSN Backbone Theater/Home Grid Pattern. The fundamental element of the DSN is a theater/home grid network of switching centers that are assigned as a common backbone surrounded and directly connected to a destination switching center, as shown in Figure 5.2.3-1, Theater/Home Grid Array. The number of switching centers in the grid varies with its geographical location and traffic distribution. The grid for any other switching center in Figure 5.2.3-1 has its own set of switching centers constituting an array that forms the basic polygrid pattern shown in Figure 5.2.3-2, Basic Polygrid Pattern. The hexagonal grid pattern is similar for all switching centers except for peripherally located centers that have less than a full pattern.

2. Long Haul Pattern. After the pattern of theater/home grids has been established, a pattern of long-haul trunking is developed to minimize the number of interswitch trunks that must be connected in tandem to complete long-distance calls. These trunk groups are established when there is sufficient calling between switching center pairs to economically justify a direct path.

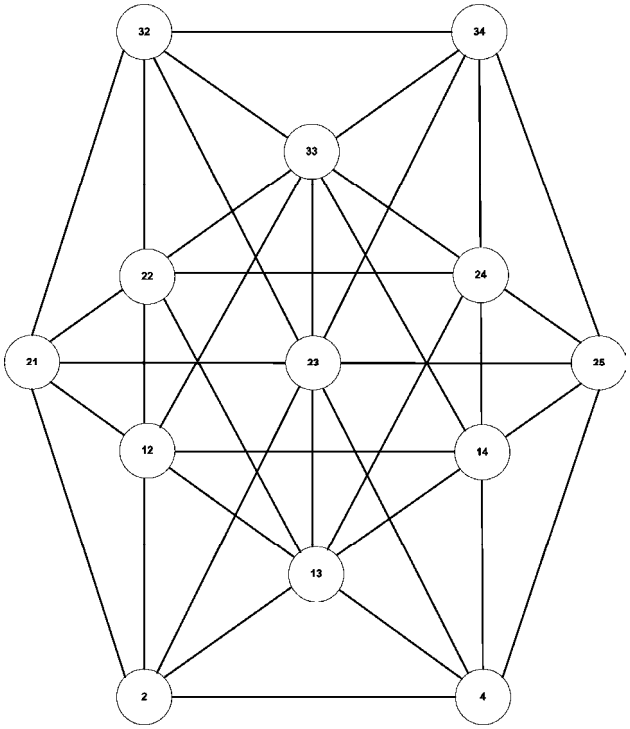


Figure 5.2.3-1. Theater/Home Grid Array

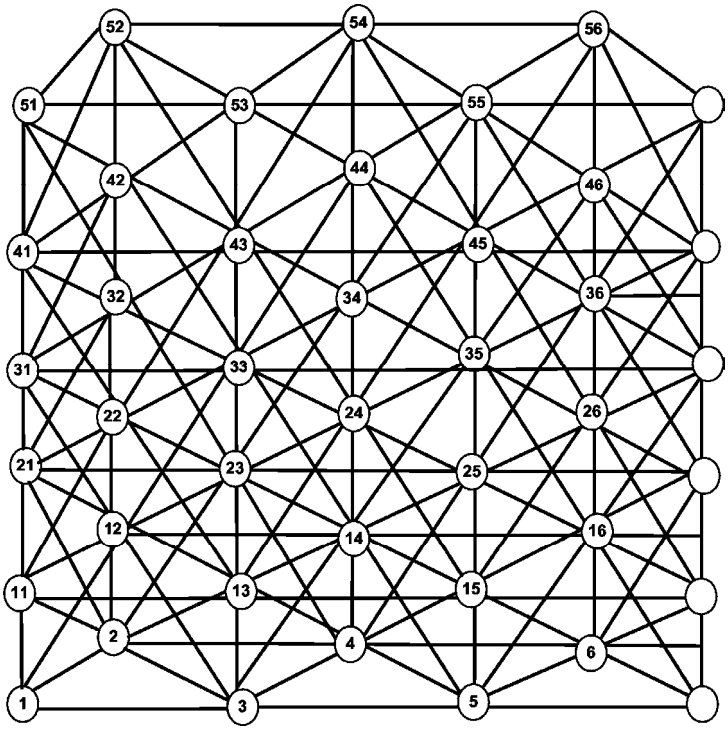


Figure 5.2.3-2. Basic Polygrid Pattern

3. Alternate Routing. The network is balanced sufficiently to enable any section of it to take on alternately routed traffic loads occasioned either by an unusual concentration of activity in suddenly created communications focal points or by sudden loss of facilities or switching centers. The alternate routing capabilities of the network enable automatic skirting of interrupted or overloaded interswitch trunk groups.

5.2.3.5.2.1.2 Routing Procedures

1. Progressive Routing. The general approach to alternate routing through the DSN Backbone is one of progressive routing. From a given originating switch to a given destination switch, all programmed route choices are examined, in turn, for the best routing to the destination, the next best, and so on until an available link is selected for transmission of the call. The selected switch then becomes the originating switch, and then the selection process begins again. Thus, a switch loses control of the routing after it passes call control to the next switch. This is the basic structure for Method 1 and Method 2 trunk route selection for calls above the ROUTINE precedence, as described in Section 5.2.2.2.3.1, Hunt Sequence for Trunks, and its subparagraphs. When the route control digit is employed for routing the rules for selecting available alternate routes change as described in item 2 and in the following subparagraphs.

2. Exterior and Interior Routing. There are two distinct forms of routing using the route control digit, which are based on the relationships of the originating switch and the theater/home grid configuration of the destination. If the originating switch is not in the theater/home grid of the destination switch, it is called “exterior” routing. If it is in the theater/home grid of the destination switch, it is called “interior” routing.

    a. If the originating switch is exterior to the destination theater/home grid, the routing plan consists of a maximum of ten possible route choices: a direct route and three alternate route triples. Alternate triples are defined as groups of up to three routes each arranged in order of preferability. The alternate triples are defined in order as the first triple (1st T), second triple (2nd T), and third triple (3rd T). In some cases, these triples may be reduced to partial triples of one or two routes due to the paucity of acceptable route choices.

    b. If the originating switch is in the theater/home grid of the destination switch, a maximum of seven possible route choices exists: a direct route followed by two triples. The two triples are designated the (1st T) and (2nd T).

5.2.3.5.2.1.3 Route Control Principles

It is necessary to make a distinction between forward and lateral routing in establishing the principles of route control. Forward routing is defined as advancing a call to a switching center that is nearer to the destination geographically. Furthermore, there must be no traffic programmed for that destination in the reverse direction over the trunk group in question.

Lateral routing is defined as routing a call to a switching center so as not to advance the call geographically as in forward routing. There may be traffic for the same destination programmed in the reverse direction of the trunk group in question. Lateral routing has to be distinguished from forward routing for the same destination to prevent "shuttle" (call routing back and forth between 2 switching centers) and no "ring-around-the-rosie" (i.e., a call returning to a switching center after routing through at least 2 other switching centers).

It is necessary, also, to establish a rule that a call arriving at a theater/home grid does not leave the theater/home grid in further routing. From this rule, it can be seen that a call that enters a theater/home grid from a switching center exterior to the theater/home grid has employed forward routing, and will not be programmed with reverse traffic.

5.2.3.5.2.1.4 Route Control Digit

Route control in the DSN Backbone network depends on the use of the RCD. The RCD is an integer, within the assigned numbering plan, that immediately precedes the address digits transmitted using CAS and/or DSN CCS7 signaling over interswitch trunks (CAS = P X Y KXX KXX XXXX; DSN CCS7 = X Y KXX KXX XXXX viz the Y digit). The RCD has the following functions to:

1. Exercise control over alternate routing at the switching center.

2. Prevent "call shuttling" and "ring-around-the-rosie."

3. Assist in limiting the number of interswitch trunk links that may be used on a call.

5.2.3.5.2.1.5 Route Control Digit Rules

1. Route control digit "0" is always used on local originating when the backbone is entered over trunks that support the route control digit.

2. Route control digit "0" is always used on forward routes (no reverse traffic programmed for the code group).

3. Route control digit "1," "2," or "3" must be used on lateral routes (reverse traffic may be programmed on these routes.)

4. Route control digit "1," "2," or "3" is used on the first lateral route; route control digit "3" is used on the second or only lateral route.

5. The direct route is always a forward route.

6. The first alternate can be a forward or lateral route.

7. The route control digit logic is shown in Table 5.2.3-11.

Table 5.2.3-11. Route Control Digit Logic

RCD RECEIVED	RCD TRANSMITTED IF SELECTED ROUTE IS	
	FORWARD	LATERAL
0	0	1, 2, or 3
1	0	3
2	0	3
3	0	3 (normally NA)

8. The search algorithm is limited to the direct and first alternate for ROUTINE precedence calls and for the friendly search for PRIORITY and higher precedence calls.

9. In the preemptive search, the trunks are tested one by one to determine if there are any idle trunks in the direct route. If so, an idle trunk in the direct route is selected; if not, the call of the lowest precedence is preempted, provided the precedence of the call selected for preemption is lower than the precedence of the call being processed. Failing to complete the call on the direct route, the preemptive search advances to the first triple and repeats the process previously described. If the call is still not completed, the process is repeated for each successive programmed triple. Complete failure shall result in a Blocked Precedence Announcement (BPA).

10. All precedence calls to selected destination centers shall be processed in one of two ways as follows:

    a. A precedence call failing to find an idle trunk in the direct route shall search in the first triple before entering a preemptive search.

    b. A precedence call failing to find an idle trunk in the direct route shall enter the preemptive search immediately and continue as described previously. This

alternative shall be used at switching centers with dedicated 4-wire subscribers and at switching centers serving as gateways to the overseas (OCONUS) areas.

11. The outgoing route control digit will be the same for all precedence levels (i.e., ROUTINE through FLASH OVERRIDE) given the same route selected and the same route control digit received.

5.2.3.5.2.1.6 Exterior Routing Rules

The route control digit logic for exterior routing is shown in Table 5.2.3-12. The rules listed in Section 5.2.3.5.2.1.5, Route Control Digit Rules, are applied to routing in routes exterior to the theater/home grid, as shown in Table 5.2.3-13, Table 5.2.3-14, and Table 5.2.3-15. (NOTE: In the following tables, the first alternate triple is shown as a lateral route. If the first alternate triple is a forward route the rules required for outpulsing RCDs on the direct route will apply.)

Table 5.2.3-12. Route Control Digit Logic for Exterior Routing

ROUTINE CALLS (P4)	
RCD	**ROUTE SELECTED**
0	Use Direct plus 1st Triple
1	Use Direct plus 1st Triple
2	Use Direct plus 1st Triple
3	Use Direct plus 1st Triple
NON ROUTINE CALLS (P0-P3)	
0	All Programmed Routes
1	Use direct route plus 1st and 2nd Triples
2	Use direct route plus 1st and 3rd Triples
3	Use direct route plus 1st Triple

Table 5.2.3-13. ROUTINE Calls

RCD IN	"DIRECT" OUT RCD	1ST ALTERNATE OUT RCD	2ND ALTERNATE OUT RCD	3RD ALTERNATE OUT RCD
0	0	1,2 or 3	NA	NA
1	0	3	NA	NA
2	0	3	NA	NA
3	0	3	NA	NA
NA = Not Allowed				

Table 5.2.3-14. Precedence Calls Above ROUTINE Precedence – Idle Search Sequence

RCD IN	"DIRECT" OUT RCD	1ST ALTERNATE OUT RCD	2ND ALTERNATE OUT RCD	3RD ALTERNATE OUT RCD
0	0	1,2 or 3	NA	NA
1	0	3	NA	NA
2	0	3	NA	NA
3	0	3	NA	NA
NA = Not Allowed				

Table 5.2.3-15. Precedence Calls Above ROUTINE Precedence – Preemptive Search Sequence

RCD IN	"DIRECT" OUT RCD	1ST ALTERNATE OUT RCD	2ND ALTERNATE OUT RCD	3RD ALTERNATE OUT RCD
0	0	1,2 or 3	3	3
1	0	3	3	NA
2	0	3	NA	3
3	0	3	NA	NA
NA = Not Allowed				

5.2.3.5.2.1.7 Interior Routing Rules

The route control digit logic for interior theater/home grid routing is shown in Table 5.2.3-16. This logic is depicted in Table 5.2.3-17, Table 5.2.3-18, and Table 5.2.3-19. (NOTE: In the following tables, the first alternate is shown as a lateral route, not a forward route. If the first alternate is a forward route, the outputted RCDs required in the direct route will apply to the first alternate also.)

Table 5.2.3-16. Route Control Digit Logic for Interior Theater/Home Grid Routing

ROUTINE CALLS (P4)	
RCD	**ROUTE SELECTED**
0	Use Direct plus 1st Triple
1	Use Direct only
2	Use Direct only
3	Use Direct only
NON-ROUTINE CALLS (P0-P3)	
0	All Programmed Routes
1	Use direct route plus 1st Triple
2	Use direct route plus 2ndTriple
3	Use direct route only

Table 5.2.3-17. ROUTINE Calls

RCD IN	"DIRECT" OUT RCD	1ST ALTERNATE OUT RCD	2ND ALTERNATE OUT RCD	3RD ALTERNATE OUT RCD
0	0	1, 2 or 3	NA	NA
1	0	NA	NA	NA
2	0	NA	NA	NA
3	0	NA	NA	NA
NA = Not Allowed				

Table 5.2.3-18. Precedence Calls Above ROUTINE Precedence – Idle Search Sequence

RCD IN	"DIRECT" OUT RCD	1ST ALTERNATE OUT RCD	2ND ALTERNATE OUT RCD	3RD ALTERNATE OUT RCD
0	0	1, 2 or 3	NA	NA
1	0	NA	NA	NA
2	0	NA	NA	NA
3	0	NA	NA	NA
NA = Not Allowed				

Table 5.2.3-19. Precedence Calls Above ROUTINE Precedence – Preemptive Search Sequence

RCD IN	"DIRECT" OUT RCD	1ST ALTERNATE OUT RCD	2ND ALTERNATE OUT RCD	3RD ALTERNATE OUT RCD
0	0	1,2 or 3	3	3
1	0	3	NA	NA
2	0	NA	3	NA
3	0	3	NA	NA
NA = Not Allowed				

5.2.3.5.2.1.8 Subscribers on a Multifunction Switch

Line originations on an MFS are not considered to be on the backbone network until they leave the MFS. As a result, route control digit limitations will not be applied to the calls until they leave the MFS. The following rules are used for this case:

1. When terminating to a trunk that uses the route control digit, a "0" will be sent out in all cases.

2. All routes shall be searched for all precedence levels (i.e., ROUTINE through FLASH OVERRIDE).

5.2.3.5.2.1.9 Dual-Theater/Homed End Offices with Single Addresses

1. Rule for Dual Homing of End Offices. The pair of switching centers serving a dual-theater/homed end office with a single address will be directly interconnected by a trunk group. This rule is necessary for transmission purposes to limit the number of additional links required on a call and to simplify the route control program.

2. Classification of Centers Relative to a Dual-Theater/Homed End Office. Figure 5.2.3-3, Dual-Homed End Office with Single Address Grid Array, illustrates a dual-homing arrangement for an end office with a single address. The two centers serving this end office are designated as D1 and D2. D1 and D2 are interconnected according to the rule stated in item 1. Each destination center has a theater/home grid determined by the basic network geometry and theater/home grid principles discussed earlier. Centers in the theater/home grid for D1 are designated as G1; those in the theater/home grid of D2 are designated as G2; while those that are in both theater/home grids are designated as G12. All other centers are programmed to use the routing program for one of the two destination centers, either D1 or D2. The bias of the dual-theater/homed routings of exterior centers toward one of the two destination centers results in efficient use of routing programs.

3. Routing Principles for Dual-Theater/Homed PABX/PBXs.

   a. Forward routing toward a dual-theater/homed end office is always used to reach any of the theater/home grid centers G1, G2, or G12. Routing from any of these three classifications of theater/home grid centers to the D1 or D2 destination center is defined as forward routing. In both instances of forward routing, route control digit "0" is sent ahead. Routing from G1 or G2 centers is conventional theater/home grid lateral routing, which follows the principles discussed previously.

      The G12 centers employ a special theater/home grid routing pattern. The route control digit logic in G12 centers is shown in Table 5.2.3-20. This logic is depicted in Table 5.2.3-21, Table 5.2.3-22, and Table 5.2.3-23. This pattern restricts lateral routings to other G12 offices, since lateral routings to G1 and G2 centers are regarded as backward routings in the context of dual-theater/homed end office programming. The reason for this is that a call reaching a G12 center has direct trunking to both serving centers D1 and D2. In contrast to this, the G1 and G2 centers have direct trunking to only one of the two serving centers.

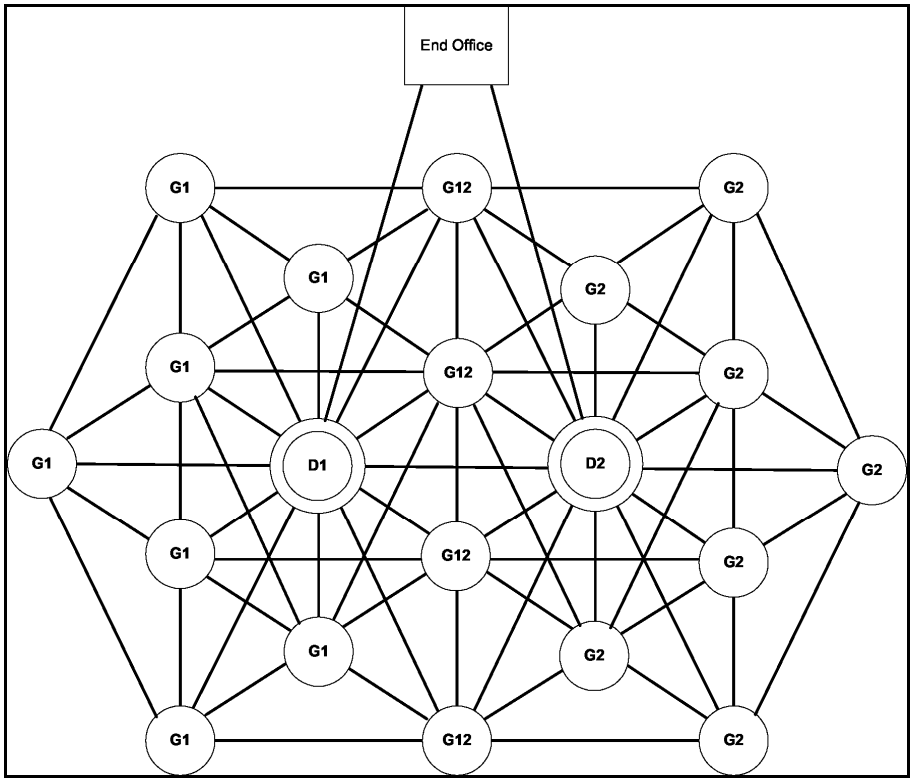


Figure 5.2.3-3. Dual-Homed End Office with Single Address Grid Array

Table 5.2.3-20. Route Control Digit Logic in G12 Centers

ROUTINE CALLS (P4)	
RCD	**ROUTE SELECTED**
0	Use direct route(s) only
1	Use direct route(s) only
2	Use direct route(s) only
3	Use direct route only
NON-ROUTINE CALLS (P0-P3)	
0	Use direct route(s) plus alternate
1	Use direct route(s) plus alternate
2	Use direct route(s) plus alternate
3	Use direct route(s) only

Table 5.2.3-21. ROUTINE Calls

RCD IN	"DIRECT" OUT RCD	ALTERNATE OUT RCD
0	0	NA
1	0	NA
2	0	NA
3	0	NA
NA = Not Allowed		

Table 5.2.3-22. Precedence Calls Above ROUTINE Precedence – Idle Search Sequence

RCD IN	"DIRECT" OUT RCD	ALTERNATE OUT RCD
0	0	NA
1	0	NA
2	0	NA
3	0	NA
NA = Not Allowed		

Table 5.2.3-23. Precedence Calls Above ROUTINE Precedence – Preemptive Search Sequence

RCD IN	"DIRECT" OUT RCD	ALTERNATE OUT RCD
0	0	3
1	0	3
2	0	3
3	0	NA
NA = Not Allowed		

Other backward routings not permitted are routings from G1, G2, and G12 centers to exterior centers and routings from D1 and D2 centers to exterior centers and routings from D1 and D2 centers to G1, G2, and G12 centers. The recommended arrangement is to employ normal theater/home grid programming in centers G1 and G2 with calls to the dual-theater/homed locations being handled in these centers as though they were single theater/homed in the respective D1 or D2 destination centers. This method also conserves routing programs.

5.2.3.5.3 Standard Directory Numbers

[Required: MFS, EOS, SMEO, DVX-C, PBX1 – Conditional: DVX-L] Standard directory numbers for the services listed in Table 5.2.3-24 shall adhere to the format and assignments specified and shall allow a network call to reach that service.

Table 5.2.3-24. Standard Directory Numbers

CALL TYPE	NUMBER ASSIGNMENT
Local Attendant Service	0
DSN Attendant Service	KXX-1110
Chief Operator	KXX-1311
Weather Announcer	KXX-1381
Time	KXX-1391
Trouble Reporting	KXX-1611
NOTES X is any digit 0–9. K is any digit 2–8.	

5.2.3.5.4 Standard Test Numbers

[Required: TS, EOS, MFS – Conditional: SMEO, DVX-C, PBX1] Standard test numbers for test and maintenance capabilities shall adhere to the format and number assignments listed in Table 5.2.3-25, Standard Test Numbers.

5.2.3.5.5 Base Services – Abbreviated Numbers

[Required: TS, EOS, SMEO, DVX-C, MFS – Conditional: PBX1, DVX-L] The format 10X is used where conflicts between DSN route codes (1X) and base service number (1XX) exist. When 7-digit intraswitch dialing is used, the switch shall be programmed in such a manner that after the 11X code is received, and no additional digits are received within approximately 4 seconds or after a # is dialed, the call shall be treated and processed as a base service call. If additional digits are received within the 4-second time period, the call shall be treated and processed as a DSN call.

5.2.3.5.6 Digit Reception Requirements

[Required: TS, EOS, SMEO, DVX-C, MFS, PBX1 – Conditional: DVX-L] Switches shall meet the digit reception requirements in Telcordia Technologies GR-505-CORE, *Call Processing*, Issue 1, December 1997, paragraph 7.2.

5.2.3.5.7 Digit Registration Capacity

[Required: TS, EOS, SMEO, DVX-C, MFS – Conditional: DVX-L] Switches shall meet the digit registration requirements in Telcordia Technologies GR-505-CORE, *Call Processing*, Issue 1, December 1997, paragraph 7.3.

Table 5.2.3-25. Standard Test Numbers

CALL TYPE	NUMBER ASSIGNMENT
Milliwatt Test	KXX-1021
Supervisory and Signal Test	KXX-1031
Far End Transmission and Noise Test	KXX-1041
Dial Speed Test	KXX-1351
DTMF Test	KXX-1361
Ringback Test	KXX-1371
Line Check Test	KXX-1301
Loop Around Termination	KXX-1061
Echo Canceller Test Loop around termination with a 0db pad inserted between receive and transmit	KXX-1062
Preemption Test	KXX-1071
Digital Loop Back Testing	KXX-1081
Bonding Mode 1 Loop	KXX-1091
NOTE: X is any digit 0–9. K is any digit 2–8.	

5.2.3.5.8 Screening

[Required: EOS, SMEO, DVX-C, MFS – Conditional: PBX1, PBX2, DVX-L] Before routing a call that is dialed from a user line, the system shall be capable of determining routing functions from class of service information associated with the line. The DSN switches shall be capable of performing screening functions as described in Telcordia Technologies GR-505-CORE, *Call Processing*, Issue 1, December 1997, paragraph 8, requirements R8-1 and R8-2. In addition, DSN switches shall be capable of performing the following screening functions.

5.2.3.5.8.1 Zone Restriction Servicing of Local Originators

[Required: EOS, SMEO, DVX-C, MFS – Conditional: PBX1, PBX2, DVX-L] Zone restriction shall be employed in the DSN to prevent a particular originator or group of originators from completing calls to specified destinations (codes). A zone can consist of an area code, office code, or any combination of these codes. If any area, specific code, service, or location is to be denied to even one user, the denial must be accomplished by zone restriction in the originating station's switching center. Zone restriction as it applies in any one switching center is independent of the zone restriction assignments in any other switching center. There shall be up to 15 zone restriction tables.

5.2.4 Signaling

5.2.4.0 Introduction

This section covers the signaling requirements for DSN switching systems. The requirements are based on Telcordia Technologies Generic Requirements GR-506-CORE, *LSSGR: Signaling for Analog Interfaces*, Issue 1, Revision 1, November 1996; "DSN Unified Capabilities Requirements 2008 (UCR 2008)"; ANSI T1.619 (1992); ANSI T1.619a (1994); ANSI T1.110 (1999); ANSI T1.116 (1996); ANSI T1.116a (1998); ANSI T1.111 (1996); ANSI T1.114 (2000); ANSI T1.112 (1996); and ANSI 1.113 (1995). Requirements for analog signaling also apply to digital circuits using channel associated signaling (CAS).

5.2.4.1 Network Power Systems for External Interfaces

[Required: TS, EOS, SMEO, MFS – Conditional: DVX-C, DVX-L] The DSN switching systems shall meet the network power systems requirements specified in the Telcordia Technologies GR-506-CORE, *LSSGR: Signaling for Analog Interfaces*, Issue 1, Revision 1, November 1996, paragraph 2.1.

5.2.4.2 Line Signaling

5.2.4.2.1 Loop Start Line

[Required: EOS, MFS, SMEO, DVX-C, PBX1 – Conditional: PBX2, DVX-L] In a loop start line arrangement, the switch supplies battery between the ring and the tip conductors. The switch detects a loop closure from the customer station as a seizure, after which it provides dial tone on the tip and ring conductors as a start dial signal.

The DSN switching systems shall meet this requirement in accordance with the "R" requirements in Telcordia Technologies GR-506-CORE, *LSSGR: Signaling for Analog Interfaces*, Issue 1, Revision 1, November 1996, Paragraphs 3 through 3.4.7, 6.2.1, 6.3.1, 13.6.1.1, 13.6.2.1, 13.6.3.1, and 13.7.1.

5.2.4.2.2 Ground Start Line

[Required: EOS, MFS, SMEO, DVX-C, PBX1 – Conditional: PBX2, DVX-L] In a ground start line arrangement, the switch provides battery through a ground detector to the ring conductor and leaves the tip conductor open. The customer station or PBX seizes the line by applying a ground to the ring conductor. The switch responds by returning ground on the tip conductor and dial tone across the tip and ring as start dial signals. When the tip ground is

detected from the switch, the customer station or PBX changes to loop closure for the off-hook state. Alerting the customer or PBX is done by connecting 20-Hz ringing to the ring conductor and ground to the tip conductor.

The DSN switching systems shall meet this requirement in accordance with the "R" requirements in Telcordia Technologies GR-506-CORE, *LSSGR: Signaling for Analog Interfaces*, Issue 1, Revision 1, November 1996, paragraphs 4 through 4.4.8, 13.2.2, 13.6.1.1, 13.6.2.2, 13.6.3.2, and 13.7.2.

5.2.4.3 Trunk Supervisory Signaling

5.2.4.3.1 Reverse Battery

[Required: EOS, MFS, SMEO, DVX-C, PBX1 – Conditional: PBX2, DVX-L] The trunk circuit at one end of a variety of loop signaling trunks applies battery and ground through suitable resistances to the tip and ring conductors. One polarity on the tip and ring leads is used for the on-hook state, and the reverse is used for the off-hook state.

The DSN switching systems shall meet this requirement in accordance with the "R" requirements in Telcordia Technologies GR-506-CORE, *LSSGR: Signaling for Analog Interfaces*, Issue 1, Revision 1, November 1996, paragraphs 7 and 8.

5.2.4.3.2 Immediate Start

[Required: TS, EOS, MFS – Conditional: SMEO, DVX-C, DVX-L, PBX1, PBX2] Immediate start (by-link) is a feature that provides intersystem address signaling between the switch and a system that transmits and/or receives address signals without special address control signals. For the reception of digits from offices requiring immediate start, the system shall be prepared to recognize the first dial pulse promptly after the connect signal is received. For transmission of address information to an office requiring immediate start, the system shall delay outpulsing after sending the connect signal to ensure that the distant office is ready. It is desirable that the transmitting office verifies that battery and ground are of the proper polarity at the time of seizure. Failure to detect the proper condition shall result in a retry of the call and a failure recorded.

The DSN switching systems shall meet this requirement in accordance with the "R" requirements in Telcordia Technologies GR-506-CORE, *LSSGR: Signaling for Analog Interfaces*, Issue 1, Revision 1, November 1996, paragraph 11.2.2.

5.2.4.3.3 Normal and Abnormal Wink Start Operation

5.2.4.3.3.1 Normal Operation

5.2.4.3.3.1.1 Normal Wink Start Operation

[Required: TS, EOS, MFS, SMEO, DVX-C, DVX-L – Conditional: PBX1, PBX2] Wink start is a feature that provides control for address signaling between systems arranged with wink start as a special address control signal. The wink start signal is applicable to specified incoming, outgoing, and two-way trunks and is used to inform the calling office that the called office is prepared to receive address signals. For wink start operation, the transmitting office shall test for the detection of the brief off-hook as a signaling integrity check.

The DSN switching systems shall provide wink start operation in accordance with the requirements in Telcordia Technologies GR-506-CORE, *LSSGR: Signaling for Analog Interfaces*, Issue 1, Revision 1, November 1996, Paragraph 11.2.1.

5.2.4.3.3.1.2 Glare Operation

[Required: TS, EOS, MFS, SMEO, DVX-C, DVX-L – Conditional: PBX1, PBX2] Glare occurs when both interfaces of switching systems connected to the same inter-switching-system facility (trunk) apply a seizure signal at approximately the same time.

The DSN switching systems shall provide glare detection and resolution in accordance with the requirements in Telcordia Technologies GR-506-CORE, *LSSGR: Signaling for Analog Interfaces*, Issue 1, Revision 1, November 1996, Paragraph 11.5.

5.2.4.3.3.2 Abnormal Operation

5.2.4.3.3.2.1 Wink Start

[Required: TS, EOS, MFS, SMEO, DVX-C, DVX-L – Conditional: PBX1, PBX2] After the connect signal is sent over the trunk, the originating office can normally expect to receive a wink start (timed off-hook) signal indicating that the terminating office is ready to receive address signaling. When the end of the wink start signal is received, the originating office may begin outpulsing. The duration of the off-hook wink returned by the terminating office will be 140 to 290 ms. However, because of distortion in the trunk facilities, the duration of the wink received by the originating office may vary (refer to Figure 5.2.2-3, DSN Preempt Signals). If the wink is shorter than the minimum allowable interval, it shall be ignored. If it is greater than the maximum interval, the call shall be considered to be in a glare condition as described in Section 5.2.4.3.3.2.2, Glare Resolution.

5.2.4.3.3.2.2 Glare Resolution

[Required: TS, EOS, MFS, SMEO, DVX-C, DVX-L – Conditional: PBX1, PBX2] The DSN switches shall meet the glare resolutions requirements defined in Telcordia Technologies GR-506-CORE, *LSSGR: Signaling for Analog Interfaces*, Issue 1, Revision 1, November 1996, paragraph 11.5 and subparagraphs.

5.2.4.3.4 Delay Dial

[Conditional: EOS, MFS, SMEO, DVX-C, DVX-L, PBX1, PBX2] If this feature is provided, it shall be in accordance with Telcordia Technologies GR-506-CORE, *LSSGR: Signaling for Analog Interfaces*, Issue 1, Revision 1, November 1996.

5.2.4.3.5 Call for Service Timing

[Required: TS, EOS, MFS, SMEO, DVX-C, DVX-L, PBX1 – Conditional: PBX2] The switching system shall ignore as a "hit" any transient off-hook signal whose duration is less than 35 milliseconds on an incoming trunk. Off-hook signals greater than 60 milliseconds shall be considered as a valid seizure. Signals that are 15 to 60 milliseconds in length are considered invalid seizures.

5.2.4.3.6 Guard Timing

[Required: TS, EOS, MFS, SMEO, DVX-C, DVX-L, PBX1 – Conditional: PBX2] The DSN switching systems shall meet guard requirements in accordance with Telcordia Technologies GR-506-CORE, *LSSGR: Signaling for Analog Interfaces*, Issue 1, Revision 1, November 1996.

5.2.4.3.7 Satellite Interface

[Required: TS, EOS, MFS, SMEO, DVX-C, DVX-L – Conditional: PBX1, PBX2] The DSN switching system shall accommodate the use of single satellite-derived trunk facilities. The only interface parameter that must be modified is the guard timing. This interval shall be extended from 1050 to 1250 milliseconds to compensate for propagation delay.

5.2.4.3.8 Disconnect Control

[Required: TS, EOS, SMEO, DVX-C, DVX-L, MFS – Conditional: PBX1, PBX2] The DSN switching systems shall meet the Disconnect Control requirements in Telcordia Technologies GR-506-CORE, *LSSGR: Signaling for Analog Interfaces*, Issue 1, Revision 1, November 1996, paragraph 13 and all subparagraphs.

5.2.4.3.9 Reselect or Retrial

[Required: TS, EOS, MFS, SMEO, DVX-C, DVX-L – Conditional: PBX1, PBX2] The actions that shall be taken by the switch are summarized below based on the direction of the circuit (outgoing or two-way), the method of controlled outpulsing (wink start or delay dial), and the method of glare resolution on two-way circuit (hold or release). The switch shall reselect or retry on circuit supervision faults as shown in Table 5.2.4-1.

Table 5.2.4-1. Reselect or Retrial

FAULT	RECOMMENDED OPERATION
1. Glare detected to glare release	Release once in same trunk group. If glare again detected or the group is all trunk busy (ATB), route advance.
2. Start signal reception timeout on glare hold	Reselect once in the same trunk group. If no circuits are idle or preemptable, route advance. If a circuit is idle or preemptable and the failure occurs on the retrial, route advance.
3. Digit sending timeout occurs on an outgoing delay dial circuit	Same as item 2.
4. Integrity check failure on a delay dial circuit	Reselect once in the same group. If fault is detected or if route is ATB, route advance.
5. No wink received on a wink start circuit	Same as item 2.
6. Wink exceeds 350 ms on an outgoing wink start circuit	Same as item 2.
7. Unexpected stop dial on an MF circuit	Same as item 2.

5.2.4.3.10 Off-Hook Supervision Transitions (Unexpected Stop)

[Required: EOS, MFS, SMEO, DVX-C, DVX-L – Conditional: PBX1, PBX2] The DSN switches shall detect and react to unexpected off-hook supervisory transitions while outpulsing on trunks, after receipt of the start-dial indication and until completion of the outpulsing. An unexpected stop is defined as an off-hook supervision transition whose duration exceeds the "hit" timing interval. When an unexpected stop is detected, the system shall reselect another trunk.

5.2.4.4 Control Signaling

Control signaling is used for the reception and outpulsing of address, precedence, and routing information. Three types of outpulsing are Dial-Pulse, DTMF, and Multifrequency 2/6. The switch shall support as applicable the following signaling combinations: DTMF 2way, DP 2way, DTMF in-DP out, DP in-DTMF out, MF(R1) 2/6 2way. Audible tones shall be in

accordance with Telcordia Technologies GR-506-CORE, *LSSGR: Signaling for Analog Interfaces*, Issue 1, June 1996, paragraph 17.

5.2.4.4.1 Dial-Pulse Signals

[Required: TS, EOS, SMEO, DVX-C, DVX-L, MFS – Conditional: PBX1, PBX2] The DSN dial-pulse (DP) signaling requirements are the same as those specified in Telcordia Technologies GR-506-CORE, *LSSGR: Signaling for Analog Interfaces*, Issue 1, June 1996, paragraph 10.

5.2.4.4.2 DTMF Signaling

[Required: TS, EOS, SMEO, DVX-C, DVX-L, MFS – Conditional: PBX1, PBX2] The DSN switching system shall be capable of outpulsing and interpretation of DTMF digits on outgoing or two-way trunks as specified in Telcordia Technologies GR-506-CORE, *LSSGR: Signaling for Analog Interfaces*, Issue 1, June 1996, paragraph 15, and Table 5.2.4-2.

Table 5.2.4-2. DTMF Generation and Reception from Users and Trunks

		HIGH GROUP FREQUENCIES NOMINAL FREQUENCY IN Hz			
		1209 Hz	**1336 Hz**	**1477 Hz**	**1633 Hz**
Low Group Frequencies	697 Hz	1	2	3	FO (A)
	770 Hz	4	5	6	F (B)
Nominal Frequency in Hz	852 Hz	7	8	9	I (C)
	941 Hz	*	0	A or #	P (D)

5.2.4.4.2.1 Standard Digit Format for Precedence

[Required: TS, EOS, MFS – Conditional: SMEO, DVX-C, DVX-L, PBX1] In addition, the DSN switching system shall be capable of outpulsing and interpretation of DTMF precedence digits in digit 0 through 4 format (i.e., 0=FLASH OVERRIDE, 1=FLASH, 2=IMMEDIATE, 3=PRIORITY, and 4=ROUTINE).

5.2.4.4.3 Multifrequency (MF(R1) 2/6) Signaling

[Required: TS, EOS, MFS, DVX-C – Conditional: SMEO, DVX-L, PBX1] The DSN switching system shall be capable of outpulsing and reception of multifrequency (MF)(R1) 2/6 signaling requirements in accordance with Telcordia Technologies GR-506-CORE, *LSSGR: Signaling for Analog Interfaces*, Issue 1, June 1996, paragraph 16 and its subparagraphs, and UCR 2008, Table 5.2.4-3, MF(R1) 2/6 Generation and Reception for Trunks.

5.2.4.5 Alerting Signals and Tones

Alerting signals are applied to an access line by the switch interface to inform the end-user of an incoming call.

5.2.4.5.1 Ringing

[Required: EOS, SMEO, DVX-C, MFS, PBX1 – Conditional: DVX-L] The DSN switching systems shall apply ringing tones and cadences as shown in Table 5.2.4-4.

Table 5.2.4-3. MF(R1) 2/6 Generation and Reception for Trunks

DIGITS AND CONTROL CODES	NOMINAL FREQUENCIES (Hz)	PRECEDENCE DIGITS
0	1300 + 1500	(FO) FLASH OVERRIDE
1	700 + 900	(F) FLASH
2	700 + 1100	(I) IMMEDIATE
3	900 + 1100	(P) PRIORITY
4	700 + 1300	(R) ROUTINE
5	900 + 1300	
6	1100 + 1300	
7	700 + 1500	
8	900 + 1500	
9	1100 + 1500	
KP	1100 + 1700	
S/T	1500 + 1700	

Table 5.2.4-4. DSN Ringing Tone and Cadence

SIGNAL	FREQUENCY (HZ)	SINGLE LEVEL TONE	COMPOSITE LEVEL	INTERRUPT RATE	TONE ON	TONE OFF
Alerting (Ringing) Normal or Routine Call						
4-Wire and 2-Wire	20	86V RMS		10 IPM	2000 ms	4000 ms
Alerting (Ringing) Precedence Call						
4-Wire and 2-Wire	20	86V RMS		30 IPM	1640 ms	360 ms

5.2.4.5.2 DSN Information Signals

[Required: EOS, SMEO, DVX-C, MFS, PBX1 – Conditional: DVX-L] The DSN switches shall implement the tone signals and cadences shown in Table 5.2.4-5.

5.2.4.6 Common Channel Signaling Number 7

The Common Channel Signaling Number 7 (CCS7) system shall perform interswitch signaling functions for the DSN. The following requirements represent the set of features standardized for CCS7 in the DSN.

Table 5.2.4-5. DSN Information Signals

SIGNAL	FREQUENCIES (Hz)	SINGLE TONE LEVEL	COMPOSITE LEVEL	INTERRUPT RATE	TONE ON	TONE OFF
Audible Ringback Precedence Call	440 + 480 (Mixed)	-19 dBm0	-16 dBm0	30 Interuptions (Pulses) Per Minute (IPM)	1640 ms	360 ms
Preemption Tone	440 + 620 (Mixed)	-19 dBm0	-16 dBm0		Steady on	
Call Waiting (Precedence Call)	440	-13 dBm0		Continuous at 6 IPM	100 ± 20 ms Three Bursts	9700 ms
Conference Connect Tone	Vendor provided ascending tones					
Conference Disconnect Tone	852 and 1336 (Alternated at 100 ms Intervals)	-24 dBm0		Steady on	2000 ms (per occurrence)	
Override Tone	440			Continuous at 6 IPM	2000 ms (followed by) 500 ms on and 7500 ms off	
Camp On	440	-13 dBm0			Single burst 0.75 to 1 second	

[Required: MFS, TS, EOS – Conditional: SMEO, DVX-C] The CCS7 shall be in accordance with the Signaling System 7 (SS7) requirements specified in the most current ANSI T1.100 series of standards and shall be capable of internetworking with ITU-T Signaling System No. 7 networks. Exceptions to these standards are explicitly noted in this section. Only those CCS7 requirements that differ from their corresponding ANSI common channel signaling standard section are included.

5.2.4.6.1 CCS7 Network Structure

[Required: MFS, TS, EOS – Conditional: SMEO, DVX-C] The CCS7 network shall serve as a separate call control and management network that is overlaid on the DSN. The CCS7 network structure is a one-level hierarchy composed of multiple mated pairs of Signal Transfer Points (STP) and their associated Service Switching Points (SSP) and signaling links in accordance with ANSI T1.110 – ANSI T1.116, all inclusive. DSN End Office, Multifunction, and Tandem switching systems shall be CCS7 Signaling Points (SP). The CCS7 network structure is shown in Figure 5.2.4-1. The CCS7 network consists of mated STP pairs connected by "C-links," these mated pairs may be grouped into "quads" with "B-links." Signal Transfer Points shall be implemented external to the switches.

5.2.4.6.2 Functional Description of the Signaling System Message Transfer Part

[Required: MFS, TS, EOS – Conditional: SMEO, DVX-C] The CCS7 message transfer part (MTP) shall be as specified in ANSI T1.111-1996, chapters 1–8. Specific requirements for DSN applications are given in the following subsections.

5.2.4.6.2.1 Signaling System Structure – Functional Levels

The fundamental principle of the signaling system structure is the division of functions into separate modules or entities.

5.2.4.6.2.1.1 Signaling Data Link Functions (Level 1)

[Required: MFS, TS, EOS – Conditional: SMEO, DVX-C] The signaling data link is a bi-directional digital transmission path comprised of digital signaling links. A maximum of 72 digital signaling links shall be supported at an individual DSN signaling point. Because of its worldwide scope, the CCS7 shall support both terrestrial and satellite transmission for the signaling data links at bit rates of 56 or 64 kbps.

5.2.4.6.2.1.2 Signaling Link Functions (Level 2)

[Required: MFS, TS, EOS – Conditional: SMEO, DVX-C] The CCS7 signaling link functions apply to both terrestrial and satellite transmission. These shall require the implementation of both types of error correction methods specified in SS7 (the basic error correction method for use on terrestrial signaling data links and the preventive cyclic retransmission method for use on satellite signaling data links).

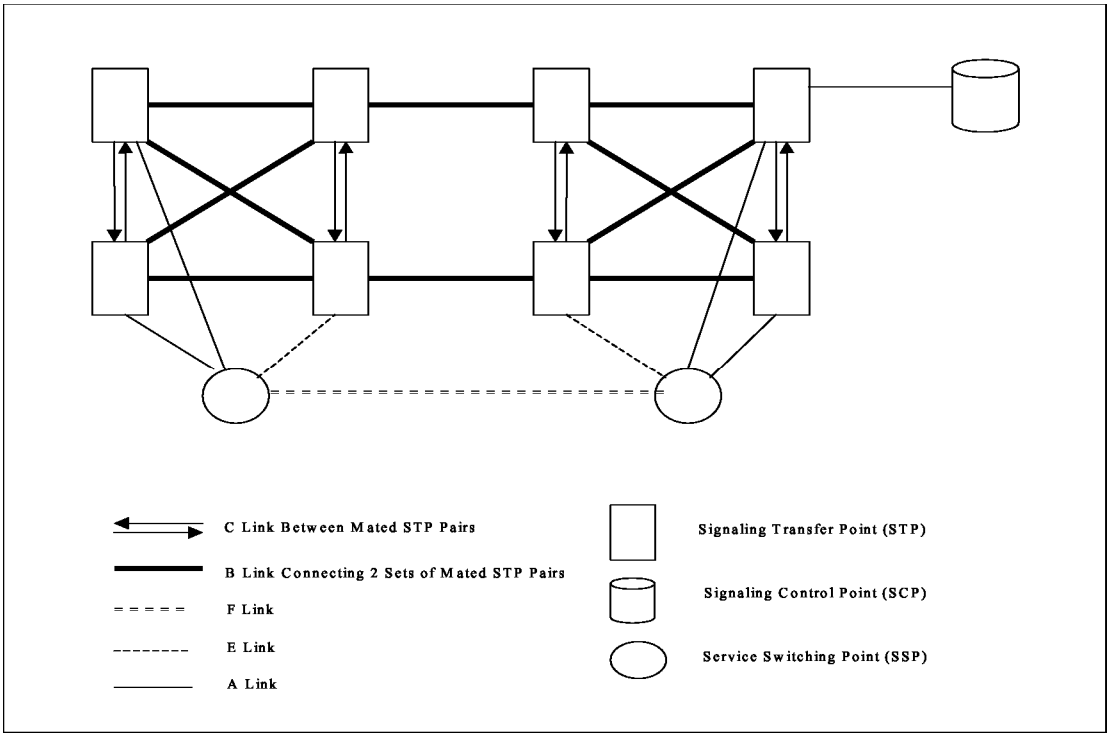


Figure 5.2.4-1. CCS7 Backbone Network Design

5.2.4.6.3 Signaling Network Functions and Messages

5.2.4.6.3.1 Routing Label

[Required: TS, MFS, EOS – Conditional: SMEO, DVX-C] The CCS7 uses the U.S. national routing label structure (specified in ANSI T1.111.4) for signaling messages between CCS7 signaling points. The routing label shall also be used for routing signaling messages to other U.S. networks that comply with the ANSI SS7 standard. The CCS7 routing label shall comply with the routing label structure for the U.S. networks as shown in Figures 3A and 3B of the T1.111.4. Signaling point codes in the CCS7 are assigned by the network administrator in accordance with ANSI guidelines.

5.2.4.6.3.2 Handling Messages Under Signaling Link Congestion

[Required: MFS, TS, EOS – Conditional: SMEO, DVX-C] Criteria for the determination of CCS7 signaling congestion status shall be as specified by ANSI T1.111.4, Section 3.8, for U.S. networks. Initial Address Messages (IAMs) carrying FLASH or FLASH OVERRIDE precedence calls shall be assigned Level 3, IMMEDIATE precedence calls shall be assigned Level 2, PRIORITY precedence calls shall be assigned Level 1, and ROUTINE precedence calls shall be assigned Level 0 in the CCS7.

5.2.4.6.3.3 Message Discrimination and Distribution Functions

[Required: MFS, TS, EOS – Conditional: SMEO, DVX-C] The message discrimination function examines the Destination Point Code (DPC) of a received signaling message to determine whether or not it is destined to the receiving signaling point. Message distribution determines to which user of the MTP a received signaling message will be directed. This function is also required in all CCS7 signaling nodes.

5.2.4.6.3.4 Signaling Network Management

[Required: MFS, TS, EOS – Conditional: SMEO, DVX-C] The DSN switching systems shall meet the Signaling Network Management requirements in the Telcordia Technologies GR-606-CORE, *Common Channel Signaling Section 6.5,* December 2000, paragraph 4.

5.2.4.6.3.4.1 Changeback

[Required: EOS, MFS, TS – Conditional: SMEO, DVX-C] The objective of the changeback procedure is to ensure that signaling is diverted from the alternative signaling link(s) to the signaling link made available as quickly as possible, while avoiding message loss or duplication. The DSN switching systems shall not use sequence control procedures to perform changeback. The last sentence of the third requirement in the Telcordia Technologies GR-606-CORE, *Common Channel Signaling Section 6.5,* December 2000, Paragraph 4.3 is changed to read as follows: The switch shall use the time-controlled diversion procedure.

5.2.4.6.4 Non-Circuit-Related Information Exchange – Signaling Connection Control Part

[Required: MFS, TS, EOS – Conditional: SMEO, DVX-C] The DSN switching systems shall meet the signaling connection control part (SCCP) requirements in the Telcordia Technologies GR-606-CORE, *Common Channel Signaling Section 6.5,* December 2000, paragraph 5 and its subparagraphs.

5.2.4.6.5 Additional Procedures for Switch-to-Switch/SCP TCAP Messages

[Required: MFS, TS, EOS – Conditional: SMEO, DVX-C] The DSN switching systems equipped for CCS7 shall meet the requirements for switch-to-switch/service control point (SCP) TCAP messaging requirements in the Telcordia Technologies GR-606-CORE, *Common Channel Signaling Section 6.5,* December 2000, paragraph 6 and its subparagraphs.

5.2.4.6.6 Message Transfer Part Restart

[Required: EOS, MFS, TS – Conditional: SMEO, DVX-C] The Message Transfer Part (MTP) Restart procedure shall be as specified in ANSI T1.111 (1996), paragraph 9 and its subparagraphs.

5.2.4.6.7 Signaling Link Management

[Required: EOS, MFS, TS – Conditional: SMEO, DVX-C] There are three signaling link management methods specified in ANSI T1.111.4: Basic signaling link management procedures, signaling link management procedures based on automatic allocation of signaling terminals, and signaling link management procedures based on automatic allocation of signaling data links and signaling terminals. The automatic allocation of signaling data links and signaling terminals shall be the method implemented in the CCS7.

5.2.4.6.8 Signaling Route Management

[Required: EOS, MFS, TS – Conditional: SMEO, DVX-C] The CCS7 signaling point nodes shall be capable of responding appropriately to the receipt of signaling route management messages. For example, a CCS7 signaling point node may be required to alter its routing information in response to a transfer prohibited, restricted, or allowed message.

5.2.4.6.9 Common Characteristics of Message Signal Unit Formats

The service information octet of the message signal unit (MSU) contains the service indicator and subservice field.

5.2.4.6.9.1 Service Indicator

[Required: EOS, MFS, TS – Conditional: SMEO, DVX-C] Requirements for the Service Indicator Codings shall be as specified in ANSI T1.111 (1996), Paragraph 14.2.1.

5.2.4.6.9.2 Subservice Field

[Required: EOS, MFS, TS – Conditional: SMEO, DVX-C] The CCS7 shall use the network code (10) as specified in ANSI T1.111.4. The CCS7 messages originating and terminating within the CCS7 or another network conforming to the ANSI standard shall be coded with the national network code (10). Requirements for the Subservice Field shall be as specified in ANSI T1.111 (1996), Paragraph 14.2.2.

5.2.4.6.10 Formats and Codes of Signaling Network Management Messages

[Required: EOS, MFS, TS – Conditional: SMEO, DVX-C] The following paragraphs specify CCS7 requirements for the formats and codes of CCS7 signaling network management messages:

1. The signal link code (SLC), used to identify one of 16 possible signaling links between each pair of adjacent (directly connected) signaling nodes, indicates the identity of a signaling link to which a network management message pertains.

2. Each pair of adjacent signaling nodes shall coordinate the assignment of SLCs to ensure compatibility.

3. The SLC may be used in the CCS7 to identify the preferred order of signaling data link selection from among the interexchange circuits. Normally, one associated signaling link between two CCS7 signaling points will be implemented and designated with an SLC at both ends of 0000. The order of selection of backup signaling data links to be obtained from the interexchange circuit group may be precoordinated and prioritized at both ends. The SLC 0001 is assigned to the circuit normally selected first as a backup signaling link. The remaining SLCs are assigned to interexchange circuits in the order of their selection as signaling data links. This order of selection shall not be interpreted as prioritizing the signaling links. Any circuit selected to serve as a signaling link remains in service for that purpose until it becomes unavailable (e.g., by failure or management withdrawal).

4. This preassignment can be overridden when communication between both CCS7 signaling points over alternative links is possible. In this case, a signaling data link connection order message may be utilized to indicate that IST will be assigned as a signaling data link and which corresponding SLC will be used.

5.2.4.6.11 Numbering of Signaling Point Codes

[Required: EOS, MFS, TS – Conditional: SMEO, DVX-C] The CCS7 numbering of signaling point codes shall be as specified in ANSI T1.111.8. The DSN meets the ANSI requirements for a large network, and it has been granted a network code value of 241. ANSI T1.111.8, Table B1, shows the current list of assigned large network codes. Signaling point codes in the CCS7 are assigned by the network administrator in accordance with ANSI guidelines.

5.2.4.6.12 Functional Descriptions of ISDN User Part

5.2.4.6.12.1 Scope, Purpose, and Application

[Required: MFS, TS – Conditional: EOS, SMEO, DVX-C] The ISDN User Part (ISUP) specifies the signaling functions, codes, messages, and procedures needed to provide services for circuit-switched voice and data services in the CCS7.

5.2.4.6.12.2 End-To-End Signaling

[Required: MFS, TS – Conditional: EOS, SMEO, DVX-C] End-to-end signaling transports signaling information between the end points of a circuit-switched connection or between any two points in the signaling network. Pass along message (PAM), ANSI T1.111, and SCCP, ANSI T1.112, end-to-end signaling methods shall be supported in CCS7.

5.2.4.6.13 Formats and Codes – ISDN User Part Parameters

[Required: MFS, TS, EOS – Conditional: SMEO, DVX-C] The ISUP specifies the signaling functions, codes, and procedures needed to provide services for circuit-switched voice and data services. The CCS7 switching services shall meet the requirements in the Telcordia Technologies, GR-317-CORE, *LSSGR: Switching System Generic Requirements for Call Control Using the Integrated Services Digital Network User Part,* November 2000, except as modified in the following subparagraphs.

5.2.4.6.13.1 Notification Indicator

[Required: MFS, TS, EOS – Conditional: SMEO, DVX-C] The following code shall be added to indicate a delay may be experienced in completing the call: 0000100 call completion delay.

5.2.4.6.13.2 ISDN User Part Messages

[Required: MFS, TS, EOS – Conditional: SMEO, DVX-C] The CCS7 shall use the messages in the Telcordia Technologies, GR-317-CORE, *LSSGR: Switching System Generic Requirements for Call Control Using the Integrated Services Digital Network User Part,* Appendix A, November 2000. In addition, CCS7 shall meet the requirements in ANSI T1.113.2 and T1.619a for messages that are not specified in the Telcordia Technologies generic requirements.

5.2.4.6.13.3 ISDN User Part Parameters

[Required: MFS, TS, EOS – Conditional: SMEO, DVX-C] The CCS7 shall use the ISUP parameters specified in the Telcordia Technologies, GR-317-CORE, *LSSGR: Switching System Generic Requirements for Call Control Using the Integrated Services Digital Network User Part,* Appendix B, November 2000. In addition, CCS7 shall use ISUP parameters specified in ANSI T1.113.3 for parameters not specified in the Telcordia Technologies requirements.

5.2.4.7 ISDN Digital Subscriber Signaling System No. 1 Signaling

5.2.4.7.1 DSN ISDN User-to-Network Signaling

The objective of this DSN ISDN user-to-network signaling requirement is to provide digital out-of-band signaling on an ISDN interface. The DSN ISDN user-to-network signaling requirement, which captures protocols under the umbrella of Digital Subscriber Signaling System No. 1 (DSS1), is intended to provide a signaling protocol that will allow signaling over an ISDN interface to support:

1. User access to DSN switches equipped with the CCS7.

2. Circuit-switched (CS) calls (both data and voice).

3. Supplementary services that include unique DSN features.

4. Future DSN access signaling requirements for other network services, including public and private network interworking in intracountry and intercountry environments, as applicable, and interoperability with other DoD Networks.

5.2.4.7.1.1 Application

[Required: MFS, EOS, SMEO, PBX1 – Conditional: DVX-C, PBX2] This section is the DSN switch requirements for user-to-network signaling over an ISDN interface. It specifies the interface signaling protocol for application throughout the DSN and defines the requirements of the DSN user-to-network signaling for exchanging information between customer premises equipment (CPE), including terminal equipment (TE) and PBXs, and DSN network switches. The exchange of signaling information between CPE and DSN network switches shall be over the D channel of the ISDN interface. The D channel may be used either for associated signaling or non-associated signaling as defined in Annex F of ANSI T1.607. In-band information and tones sent over the B channel shall be allowed, when applicable. In the DSN host countries, DSN connections may be made with public, private, and military CPE and networks. Protocol and/or signaling gateway conversions shall be required in some instances to provide the desired

DSN connections. Such translations shall be handled on a case-by-case basis as detailed in site-specific contracts.

5.2.4.7.1.2 Physical Layer

[Required: MFS, EOS, SMEO, PBX1 – Conditional: DVX-C, PBX2] The DSN user-to-network signaling physical layer specification for the BRI shall be ANSI T1.605 and ANSI T1.601 or ITU Recommendation I.430 as required for OCONUS applications. The DSN user-to-network signaling physical layer specification for the PRI operating at 1.544 Mbps shall be ANSI T1.408. The DSN user-to-network signaling specification for the PRI operating at 2.048 Mbps shall be ITU Recommendation I.431.

5.2.4.7.1.2.1 S/T Reference Point

[Required: MFS, EOS, SMEO, PBX1 – Conditional: DVX-C, PBX2] For the BRI at the S/T reference point, B channels shall have the capability of either restricted or unrestricted operation. The restricted capability is necessary for backward compatibility with networks that support the restricted 64 kbps operation. The D channel shall have unrestricted capability.

5.2.4.7.1.3 Data-Link Layer

[Required: MFS, TS, EOS, SMEO, PBX1 – Conditional: DVX-C, PBX2] The DSN user-to-network signaling data-link layer shall be as specified in the ANSI T1.602, *ISDN Data-Link Layer Signaling Specification for Application at the User-Network Interface*, which is a pointer document completely aligned with the ITU-T Recommendations Q.920 and Q.921.

5.2.4.7.1.3.1 Data-Link Connections

[Required: MFS, TS, EOS, SMEO, PBX1 – Conditional: DVX-C, PBX2] Point-to-point, broadcast, and multipoint data-link connections shall be provided for DSN applications. The ANSI T1.602 depicts examples of point-to-point and broadcast data-link connections. Other point-to-point applications of this specification shall be allowed, such as the support of multiple terminals at the user-to-network interface. A data-link layer management entity shall be provided to support DSN management.

5.2.4.7.1.3.2 Peer-to-Peer Procedures of Data-Link Layer

[Required: MFS, TS, EOS, SMEO, PBX1 – Conditional: DVX-C, PBX2] Within the DSN, peer-to-peer procedures of the data-link layer shall follow the procedures described in the ANSI T1.602, with the additions provided in this paragraph. The network administration shall have the responsibility to determine the system parameter values on the DSN user-to-network interface.

These parameters shall initially be set to the default values of the ANSI standard. A means is available in Appendix IV of Q.921 to change the assignment of the system parameters within the range of values specified by the ANSI standard. DSN terminal equipment shall support other values of T200 to allow for multiple terminals on the user side, together with satellite connections in the DSN user-to-network transmission.

5.2.4.7.1.4 Layer 3 DSN User-to-Network Signaling

[Required: MFS, TS, EOS, SMEO, PBX1 – Conditional: DVX-C, PBX2] The Layer 3 protocols specify the messages and information elements, coding and formats, and procedures employed on the user-to-network interface in order to establish, maintain, and terminate network connections across an ISDN.

5.2.4.7.1.4.1 Overview of Layer 3

The overview of Layer 3 of the DSN user-to-network signaling layer 3 shall be as specified in the ANSI T1.615. The ANSI standard is consistent with the seven-layer model described in ITU Recommendation I.320. ANSI T1.615 describes, in general terms, the D-channel Layer 3 DSS1 functions and protocol employed across an ISDN user-to-network interface.

5.2.4.7.1.4.2 DSN User-to-Network Signaling for Circuit-Switched Bearer Service

[Required: MFS, TS, EOS, SMEO, PBX1 – Conditional: DVX-C, PBX2] The DSN user-to-network signaling Layer 3 specification for Circuit-Switched (CS) bearer service (or CS-Basic Call) shall be as specified in the ANSI T1.607 for ISDN primary and basic rate interfaces. ANSI T1.607 is aligned with the ITU Recommendation Q.931 (to the extent possible), and it covers U.S. unique requirements for CS-Basic Call.

5.2.4.7.1.4.3 Sequence of Messages for DSN Circuit-Switched Calls

[Required: MFS, TS, EOS, SMEO, PBX1 – Conditional: DVX-C, PBX2] Call establishment involves SETUP, SETUP ACK, CALL PROCEEDING, ALERTING, CONNECT, and CONNECT ACK messages. The PROGRESS message shall be used with interworking or with in-band information and patterns to indicate the progress of a call. A three-step call clearing phase shall use the DISCONNECT, RELEASE, and RELEASE COMPLETE messages. The miscellaneous messages—INFORMATION, STATUS ENQUIRY (and STATUS), and NOTIFY—shall be used for the purposes described in ANSI T1.607.

5.2.4.7.1.4.4 Message Functional Definitions and Content

[Required: MFS, TS, EOS, SMEO, PBX1 – Conditional: DVX-C, PBX2] The Layer 3 messages used by the DSN user-to-network signaling for circuit-switched connections shall be as specified by the ANSI T1.607 except for messages modified in the following paragraph.

SETUP Message. The SETUP message is sent by the calling user to the network or by the network to the called user to initiate call establishment. DSN calls shall use the setup message specified in ANSI T1.607. The Channel Identification, Calling Party Number (when available), and Called Party Number are mandatory information elements (IEs). For an MLPP call (invoking MLPP feature) on the DSN user-to-network interface, the SETUP message shall include the Precedence Level information element. It shall also contain other IEs, such as the business group (BG) IE for the COI feature, when such unique DSN features are required and the call identity IE (as defined in ITU Recommendation Q.931) for the MLPP feature. The Precedence Level and MLPP service domain (both contained in the Precedence Level IE) and Calling Party Number (contained in the Calling Party Number IE), shall be used to mark the circuit (identified in the Channel Identification IE) to be preempted as "reserved" for reuse by the preempting call when the LFB option is exercised on the DSN user-to-network interface. Table 5.2.4-6, SETUP Message for MLPP Call, shows the SETUP message content for an MLPP call; important differences from the SETUP message in ANSI T1.607 are specified in the following paragraphs.

5.2.4.7.1.4.5 General Message Format and Information Elements Coding

[Required: MFS, TS, EOS, SMEO, PBX1 – Conditional: DVX-C, PBX2] The guidelines specified in the ANSI T1.607 shall be followed in this specification.

1. Application of Codesets within the DSN. The DSN unique IEs, if any, shall employ the following order of preference in using the codesets:

    a. Codeset 0 – highest
    b. Codeset 5
    c. Codeset 6 – lowest

2. Application of Information Elements in the DSN. The DSN user-to-network signaling protocol shall maximize the use of codeset "00" (ITU standardized coding) and codeset "10" (national standard) IEs (when codeset "00" is not possible). Following are guidelines for the specific use of such IEs in the DSN:

Table 5.2.4-6. SETUP Message for MLPP Call

MESSAGE TYPE: SETUP SIGNIFICANCE: GLOBAL DIRECTION: BOTH			
INFORMATION ELEMENT	**ANSI T1.607 REFERENCE**	**DIRECTION**	**TYPE**
Protocol Discriminator	4.2	both	M
Call Reference	4.3	both	M
Message Type	4.4	both	M
Repeat Indicator	4.5	both	O (Note 1)
Bearer Capability	4.5	both	M (Note 2)
Channel Identification	4.5	both	M (Note 3)
Progress Indicator	4.5	both	O (Note 4)
Network Specific Facilities	4.5	both	O (Note 5)
Display	4.5	n-u	O (Notes 6 & 7)
Keypad Facility	4.5	u-n	O (Note 8)
Signal	4.5	n-u	O (Note 9)
Calling Party Number	4.5	both	M (Note 10)
Calling Party Subaddress	4.5	both	O (Note 11)
Called Party Number	4.5	both	M (Note 12)
Called Party Subaddress	4.5	both	O (Note 13)
Transit Network Selection	4.5	u-n	O (Note 14)
Lower Layer Compatibility	4.5	both	O (Note 15)
High Layer Compatibility	4.5	both	O (Note 16)
User-User	4.5	both	O (Notes 17 & 18)
Locking Shift (Note[1])	4.5	u-n	O (Note 19)
Operator System Access	4.6	u-n	O (Note 20)
Precedence Level	Note[2]	both	M

NOTE: Notes 1 through 20 and references of the ANSI T1.607 IE are not repeated for this table but still apply. Refer to ANSI T1.607 IE for detailed notes and references.

1. The Locking Shift IE to identify IEs in U.S. National Codeset 5.
2. The Precedence Level IE is in U.S. National Codeset 5 and is defined in ANSI T1.619 (1992) and T1-619a (1994).

LEGEND
M Mandatory O Optional Elements

a. Called Party Number Information Element (IE). The Called Party Number IE, which identifies one called party of a call, shall accommodate the DSN numbering plan. The variable length number digits parameter in the information element may carry the area code, switch code, and line number from the DSN numbering plan.

b. Calling Party Number Information Element (IE). The Calling Party Number IE, which identifies the origin of a call, shall accommodate the DSN WWNDP as stated for the Called Party Number IE.

c. Keypad Facility Information Element (IE). The Keypad Facility IE, which conveys ASCII characters entered by means of a terminal keypad (when employed), shall contain the digits entered by a DSN user.

d. Channel Identification Information Element (IE). The Channel Identification IE identifies a channel within the interface(s) controlled by the signaling procedures. The channel number/slot map parameter within it identifies the B-channel controlled by a particular message. The following two methods of B-channel identification are available for use in the DSN: binary channel number assigned to the channel and a slot map that identifies the time slots used by the channel. The parameter shall be coded exclusively for one method depending upon the number/map parameter information. Both primary rate interfaces, 1.544 Mbps and 2.048 Mbps, shall be supported in accordance with the slot map in ITU-T Q.931.

e. Transit Network Selection Information Element (IE). The Transit Network Selection IE identifies one requested transit network. It may be repeated in a message to select a sequence of transit networks through which a call must pass. For example, the element may be employed in a SETUP message to specify one or a sequence of transit networks (other than the user-assigned transit network) through which a call must pass. In the case of the DSN user-to-network signaling, this IE shall be used to specify the DSN or a network other than the DSN as a transit network. (DoD networks and foreign PTTs are examples.)

f. Cause Information Element. The Cause IE shall be in accordance with ANSI T1.619a.

g. Signal Information Element. The Signal IE shall be in accordance with ANSI T1.619a. The signal shall be included in the DISCONNECT, PROGRESS, and SETUP messages as appropriate for the MLPP feature.

h. Notification Indicator Information Element. The Notification Indicator IE, which indicates information pertaining to a call, shall contain the notification description code of “0 0 0 0 1 0 0” (value 4) for the MLPP feature to indicate to the calling user a possible call completion delay when an LFB query is invoked in response to an MLPP call setup.

5.2.4.7.1.4.6 Supplementary Services

[Conditional: MFS, EOS, SMEO, DVX-C, PBX1, PBX2] If provided, Supplementary Services shall be in accordance with the following standards:

- ANSI T1.607-1998, ISDN Layer 3 Signaling Specifications for Circuit Switched Bearer Service for Digital Subscriber Signaling System No.1 (DSS1)
- ANSI T1.613-1992, ISDN Call Waiting Supplementary Service
- ANSI T1.616-1992, ISDN Call Hold Supplementary Service
- ANSI T1.621-1992, ISDN User-to-User Signaling Supplementary Service
- ANSI T1.632-1993, ISDN Normal Call Transfer Supplementary Service
- ANSI T1.642-1993, ISDN Call Deflection Supplementary Service
- ANSI T1.643-1995, ISDN Explicit Call Transfer Supplementary Service
- ANSI T1.647-1995, ISDN Conference Calling Supplementary Service

5.2.5 Transmission

5.2.5.0 DSN Transmission Interface

[Required: TS (Trunks Only), MFS, EOS, SMEO, DVX-C, DVX-L, PBX1, PBX2] The transmission characteristics of switching systems used in, or interfacing to the DSN, shall not degrade the end-to-end transmission performance of the DSN. The transmission characteristics of the switching system shall be based on the switching matrix using Pulse Code Modulation (PCM) digital technology. These interface requirements are mandatory for interfacing with DSN circuits and may also be used for connectivity between DSN switches. These transmission requirements shall be measured in accordance with IEEE Standard 743.

5.2.5.1 Input Impedance

[Required: TS (Trunks Only), MFS, EOS, SMEO, DVX-C, DVX-L, PBX1, PBX2] The input impedance seen looking into each analog line or trunk interface shall meet the requirements in Table 5.2.5-1.

Table 5.2.5-1. Input Impedance Requirements

PATH THROUGH NEAR END	SWITCH FAR END	REFERENCE IMPEDANCE	FREQUENCY RANGE	MIN. RETURN LOSS (AT INPUT POWER LEVEL OF DBM0)
Line	Digital Interface or 4-Wire Trunk	900 ohms +2.16 microfarad	200-500 Hz 500-3400Hz	20dB 26dB
Remote Line (0 dB loss)	Digital Interface or 4-Wire Trunk	900 ohms +2.16 microfarad	200-500 Hz 500-3400Hz	20dB 26dB
Remote Line (> 2 dB loss)	Digital Interface or 4-Wire Trunk	900 ohms +2.16 microfarad	200-500 Hz 500-3400Hz	14dB 20dB
2-Wire Trunk	Digital Interface or 4-Wire Trunk	900 ohms +2.16 microfarad	200-500 Hz 500-1000 Hz 1000-3400 Hz	20dB 26dB 30dB
4-Wire Trunk	Digital Interface or 4-Wire Trunk	600 ohms	200-500 Hz 500-1000 Hz 1000-3400 Hz	20dB 26dB 30dB

5.2.5.2 Inserted Connection Loss

[Required: TS (Trunks Only), MFS, EOS, SMEO, DVX-C, DVX-L, PBX1, PBX2] The connection loss inserted by the switching system shall meet the following requirements.

5.2.5.2.1 Average Loss at 1004 Hz And Loss Control

[Required: TS (Trunks Only), MFS, EOS, SMEO, DVX-C, DVX-L, PBX1, PBX2] The minimum insertion loss at 1004 Hz shall be 0.0dB. The maximum average loss measured at 1004 Hz shall be as shown in Table 5.2.5-2.

Table 5.2.5-2. Average Loss Requirements

CONNECTION TYPE	DIGITAL SYSTEM REQUIREMENT (dB)
Line or Remote Line to Line Remote Line	1
Line or Remote Line to 2-Wire, 4-Wire	0.75
Line or Remote Line to Digital Interface	0.5
2-Wire or 4-Wire trunks to 2-Wire or 4-Wire trunks	0.75
Digital Interface to 2-Wire or 4-Wire trunks	0.4
Digital Interface to Digital Interface	N/A

5.2.5.2.2 Loss Variability at 1004 Hz

[Required: TS (Trunks Only), MFS, EOS, SMEO, DVX-C, DVX-L, PBX1, PBX2] The maximum loss variability shall be as follows. This shall be met by at least 99 percent of the connections of each connection type shown in Table 5.2.5-3.

Table 5.2.5-3. Maximum Loss Variability

CONNECTION TYPE	LOSS VARIABILITY (dB)
Line to Line, 2-Wire or 4-Wire	+ 0.5
4-Wire or 2-Wire to 2-Wire or 4-Wire	+ 0.5
Digital Interface to Line, 2-Wire, or 4-Wire	+ 0.3
Remote Line to Digital Interface	+ 0.5
Digital Interface to Digital Interface	N/A

5.2.5.2.3 Attenuation Distortion

[Required: TS (Trunks Only), MFS, EOS, SMEO, DVX-C, DVX-L, PBX1, PBX2] The attenuation distortion shall be as follows. This shall be met by at least 99 percent of the connections of each connection type as defined by the minimum and maximum losses shown in Table 5.2.5-4, Attenuation Distortion.

Table 5.2.5-4. Attenuation Distortion

CONNECTION TYPE	FREQUENCY (Hz)	MIN. LOSS (dB)	MAX LOSS (dB)
Line, Remote Line, 2-Wire to Line, Remote Line, 2-Wire	200	0	5.0
	300	-0.5	1.0
	3000	-0.5	1.0
	3200	-0.5	1.5
	3400	0.0	3.0
Digital Interface to Line, Remote Line, 2-Wire and Line, Remote Line, 2-Wire to Digital Interface (2)	200	0 (1)	2.0 (1)
	300	-0.25	0.5
	3000	-0.25	0.5
	3200	-0.25	0.75
	3400	0	1.5
2-Wire, Line, Remote Line to 4-Wire	200	0	4.0
	300	-0.4	0.65
	3000	-0.4	0.65
	3200	-0.4	1.5
	3400	0	3.0
4-Wire to 4-Wire	200	0	3.0
	300	-0.3	0.3
	3000	-0.3	0.3
	3200	-0.3	1.5
	3400	0	3.0

CONNECTION TYPE	FREQUENCY (Hz)	MIN. LOSS (dB)	MAX LOSS (dB)
Digital Interface-to-4-Wire Trunk and 4-Wire Trunk-to-Digital Interface (2)	200 300 3000 3200 3400	0(1) -0.15 -0.15 -0.15 0	2.0 (1) 0.15 0.15 0.75 1.5

NOTES:
1. Value given at 200 Hz is for digital-to-analog direction. For analog-to-digital direction, add 1.0 dB of loss to the value at 200 Hz.
2. Under the assumption that the signal always passes through the equivalent of the digital interface, these two requirements control attenuation distortion in a digital EOS.

5.2.5.2.4 Tracking Error

[Required: TS (Trunks Only), MFS, EOS, SMEO, DVX-C, DVX-L, PBX1, PBX2] This requirement shall be met by at least 50 percent of the connections of each connection type. The tracking error shall be less than or equal to the values shown in Table 5.2.5-5, Tracking Error.

Table 5.2.5-5. Tracking Error

CONNECTION TYPE	INPUT LEVEL (dBM0)	TRACKING ERROR (dB)
Digital Interface to Line, Remote Line-2-Wire, or 4-Wire	-37 to +3 -50 to -37	+ 0.25 + 0.50
All others (except Digital Interface to Digital Interface)	-37 to +3 -50 to -37	+ 0.50 + 1.0

5.2.5.3 Frequency Response

[Required: TS (Trunks Only), MFS, EOS, SMEO, DVX-C, DVX-L, PBX1, PBX2]. Frequency response shall be calculated as loss relative to 1004 Hz as shown in Table 5.2.5-6 and Table 5.2.5-7. Minus (-) indicates less loss and plus (+) indicates greater loss.

Table 5.2.5-6. Trunk-to-Trunk Frequency Response

FREQUENCY (Hz)	LOSS AT 0 dBM 4-WIRE TO 4-WIRE
60	20 dB min
300-3000	-0.3 dB to +0.3 dB
3200	-0.3 dB to 1.5 dB
3400	0 dB to 3 dB
- Less Loss + Greater Loss	

Table 5.2.5-7. Line-to-Line Frequency Response

FREQUENCY (Hz)	LOSS AT 0 dBM
60	20 dB min
300-3000	-0.5 dB to 1 dB
3200	-0.5 dB to 1 dB
3400	0 dB to 3 dB
- Less Loss + Greater Loss	

5.2.5.4 Overload Level

[Required: TS (Trunks Only), MFS, EOS, SMEO, DVX-C, DVX-L, PBX1, PBX2] The overload level at 900 ohm impedance shall be +3 dBm0.

5.2.5.5 Return Loss

[Required: TS (Trunks Only), MFS, EOS, SMEO, DVX-C, DVX-L, PBX1, PBX2] Return loss for various ports shall be as specified in the following sections.

5.2.5.5.1 2-Wire Line Return Loss

[Required: TS (Trunks Only), MFS, EOS, SMEO, DVX-C, DVX-L, PBX1, PBX2] Return loss shall be measured from the 2-wire line side at 900 ohms in series with 2.16 microfarads, on a line-to-line or line-to-trunk connection. Minimum return losses shall be:

- 20 dB at 200-500 Hz
- 26 dB at 500-1000 Hz
- 30 dB at 1000-3400 Hz

5.2.5.5.2 4-Wire Trunk Return Loss (Impedance)

[Required: TS (Trunks Only), MFS, EOS, SMEO, DVX-C, DVX-L, PBX1, PBX2] Return loss shall be measured from the 4-wire trunk side at 600 ohms resistive on a trunk-to-trunk or trunk-to-line connection. Minimum return losses shall be:

- 20 dB at 200-500 Hz
- 26 dB at 500-1000 Hz
- 30 dB at 1000-3400 Hz

5.2.5.6 Longitudinal Balance

[Required: TS (Trunks Only), MFS, EOS, SMEO, DVX-C, DVX-L, PBX1, PBX2] The longitudinal balance shall meet the requirements shown in Table 5.2.5-8. At 3400 Hz, the minimum balance shall be 50 dB. The method of measurement shall be as specified in the IEEE Standard 455-1985, Standard Testing Procedures for Measuring Longitudinal Balance of Telephone Equipment Operating in the Voice Band.

Table 5.2.5-8. Longitudinal Balance

CONNECTION	LONGITUDINAL BALANCE (dB)		
	FREQ (Hz)	AVG	MIN
All connection types between analog interfaces	200	63	58
	500	63	58
	1000	63	58
	3000	58	53

5.2.5.7 60 Hertz Longitudinal Current

[Required: TS (Trunks Only), MFS, EOS, SMEO, DVX-C, DVX-L, PBX1, PBX2] Under test conditions with 60 Hz, the system noise shall be no greater than 23 dBrnC0. (This requirement shall also apply at 50 Hz.)

5.2.5.8 Idle Channel Noise

[Required: TS (Trunks Only), MFS, EOS, SMEO, DVX-C, DVX-L, PBX1, PBX2] Idle channel noise consists of C-Message Weighting and Flat Weighting.

5.2.5.8.1 C-Message Weighting

[Required: TS (Trunks Only), MFS, EOS, SMEO, DVX-C, DVX-L, PBX1, PBX2] Ninety-nine percent of the connections shall have C-message weighting noise less than or equal to the values shown in Table 5.2.5-9.

Table 5.2.5-9. C-Message Waiting

CONNECTION	AVERAGE	NOISE (dBrnC0) 99%
Analog-Analog	20	23
Analog-Digital	17	20
Digital-Analog	17	20

5.2.5.8.2 Flat-Weighting Noise

[Required: TS (Trunks Only), MFS, EOS, SMEO, DVX-C, DVX-L, PBX1, PBX2] The mean of the idle channel noise distribution (C-Message and Flat Weighting) shall be less than or equal to 35 dBrn0, as measured with a 3 kHz flat weighting. The 99% point on the idle channel noise distribution shall be less than 39 dBrn0 when measured with a 3-kHz flat weighting.

5.2.5.9 Power Line Interference

[Required: TS (Trunks Only), MFS, EOS, SMEO, DVX-C, DVX-L, PBX1, PBX2] The power line frequencies, harmonics of power line frequencies, and noise introduced through the power supply shall have an RMS sum at least 55 dB below test tone level.

5.2.5.10 Impulse Noise

[Required: TS (Trunks Only), MFS, EOS, SMEO, DVX-C, DVX-L, PBX1, PBX2] The C-notched impulse noise shall not exceed 54 dBrnc0 with tone and 47 dBrnc0 without tone in a 5-minute period on six measurements made during the busy hour. Measurement shall be taken using an impulse noise counter. The measurement shall be made by taking six random normal connections from voice frequency circuits through the switching equipment.

5.2.5.11 Crosstalk Coupling

[Required: TS (Trunks Only), MFS, EOS, SMEO, DVX-C, DVX-L, PBX1, PBX2] Worst case equal level crosstalk is to be 70 dB minimum in the range 200 to 3400 Hz. This is to be measured between any two paths through the system connecting a 0 dBm0 level tone to the disturbing pair. Crosstalk loss between the two directions of a circuit shall be 50 dB minimum in the range of 200 to 3400 Hz when measured at equal level points.

5.2.5.12 Intermodulation Distortion

[Required: TS (Trunks Only), MFS, EOS, SMEO, DVX-C, DVX-L, PBX1, PBX2] Intermodulation distortion, measured using the standard 4-tone test method, shall meet the requirements shown in Table 5.2.5-10.

Table 5.2.5-10. Intermodulation Distortion

CONNECTION	SECOND-ORDER (dB)		THIRD-ORDER (dB)	
	95%	MIN	95%	MIN
Line, Remote Line, 2-Wire to Line, Remote Line, 2-Wire	44	43	45	44
Line, Remote Line, 2-Wire to 4-Wire	46	45	48	47
4-Wire to 4-Wire	50	49	52	51
Digital Interface to Line, Remote Line, 2-Wire	47	46	50	49
Digital Interface to 4-Wire	53	52	57	56

5.2.5.13 Signal to Distortion Ratio (C-Notched Noise)

[Required: TS (Trunks Only), MFS, EOS, SMEO, DVX-C, DVX-L, PBX1, PBX2] At least 99% of the connections of each connection type shall have a signal to distortion greater than or equal to the values shown in Table 5.2.5-11.

Table 5.2.5-11. Signal-to-Noise Distortion

SINEWAVE INPUT (dBMo)	SINEWAVE FREQ. (Hz)	ANALOG TO ANALOG	ANALOG TO DIGITAL DIGITAL TO ANALOG
0 to -30	200-3400	33	35
-40	200-3400	27	29
-45	200-3400	22	25

5.2.5.14 Absolute Delay

[Required: TS (Trunks Only), MFS, EOS, SMEO, DVX-C, DVX-L, PBX1, PBX2] The absolute one-way delay through the switch, excluding delays associated with RSU switching shall not exceed 600 microseconds analog-to-analog measured at 1800 Hz.

5.2.5.15 Envelope Delay Distortion

[Required: TS (Trunks Only), MFS, EOS, SMEO, DVX-C, DVX-L, PBX1, PBX2] The envelope delay difference between any two adjacent frequencies between 1000 and 2600 Hz shall not exceed 20 µs. On any properly established connection, the envelope delay distortion shall not exceed the limits shown in Table 5.2.5-12.

Table 5.2.5-12. Envelope Delay Distortion Limits

BANDWIDTH (Hz)	MICROSECONDS (μs)
1000 to 2600	190
800 to 2800	360
600 to 3000	500
400 to 3200	700

5.2.5.15.1 Echo Path Delay

[Required: TS (Trunks Only), MFS, EOS, SMEO, DVX-C, DVX-L, PBX1, PBX2] Echo path delay is twice the one-way transit time delay of a signal through a switching system connection path. Ninety-nine percent of the connections of each connection type shall have echo path delay less than or equal to the following values. The values shown in Table 5.2.5-13 shall apply at the frequency at which the minimum delay occurs.

Table 5.2.5-13. Echo Path Delay

CONNECTION TYPE	ECHO PATH DELAY (ms)
Digital Interface to Digital Interface	1.4
Digital Interface to Line, 2-Wire, or 4-Wire	1.9
Line to Line, 2-Wire, 4-Wire; 2-Wire, 4-Wire to 2-Wire, 4-Wire; Remote Line to Remote Line (Intra)	2.4
Digital Interface to Remote Line	4
Remote Line to Line, 2-Wire, 4-Wire	4
Remote Line to Remote Line (Inter)	6.5

5.2.5.16 Bit Integrity

[Required: TS (Trunks Only), MFS, EOS, SMEO, DVX-C, DVX-L, PBX1, PBX2] The capability to transmit bit streams end-to-end through the network without inserting or deleting any bits in the digital bit stream is a requirement. Switched Data or ISDN shall not employ digital processing to insert transmission losses.

5.2.5.17 Switched Digital Bit Error Rate

[Required: TS (Trunks Only), MFS, EOS, SMEO, DVX-C, DVX-L, PBX1, PBX2] The digital switching system shall not introduce an error into the digital connections that is greater than one error in 10^9 (one billion) bits averaged over a 9 hour period measured at the DS0 rate.

5.2.5.18 Encoding and Decoding Levels

[Required: TS (Trunks Only), MFS, EOS, SMEO, DVX-C, DVX-L, PBX1, PBX2] The DSN uses a fixed loss transmission plan. To provide compatible transmission level interface to other networks, and to accommodate different Transmission Level Point (TLP) reference at analog and digital switching centers, the digital switching center shall provide the capability to selectively set the encoding and decoding levels at the A/D and D/A converters.

5.2.5.18.1 DSN Fixed Loss Plan

[Required: TS (Trunks Only), MFS, EOS, SMEO, DVX-C, DVX-L, PBX1, PBX2] A fixed loss plan provides a coherent means for implementing engineered loss into the digital network. In an all-digital network, it is no longer necessary to compute loss on a trunk-by-trunk basis, as is done in an analog network. Loss assignments on individual digital trunks require either a digital to analog to digital conversion for the use of an analog pad or a digital code conversion within the software of a switching system that implements the desired value of loss. The approach used in the DSN is to provide a fixed end-to-end loss that varies depending on the type of connection (e.g., intra-EOS or EOS to EOS). The end-to-end losses required for the various types of connections are shown in Table 5.2.5-14.

Table 5.2.5-14. End-to-End Loss

CONNECTION TYPE	END-TO-END LOSS
EOS to EOS	
Via MFS	6 dB
Via non-MFS	
< 200 miles	3 dB
> 200 miles	6 dB
Intra-EOS	0 dB

5.2.5.18.1.1 Switch Transmission Level Points

[Required: TS (Trunks Only), MFS, EOS, SMEO, DVX-C, DVX-L, PBX1, PBX2] To implement the fixed loss plan, each DSN switch shall have a specified TLP reference. A TLP is defined as a point in the transmission system at which the ratio of power of the test signal at that point to the power of the test signal at a reference point is specified. The designated reference point is the zero dB TLP or simply 0 TLP. The standard reference point for the 0 TLP is the outgoing trunk appearance, or transmit side of an end office. The transmission level for an MFS is -3 TLP, where the standard reference point is also on the transmit side of the switch.

5.2.6 System Interfaces

This section is an overview of the digital and analog interfaces required in the DSN. The digital interfaces described are applicable to all digital connections associated with the DSN switching system and subsystems. These include access lines to EOSs and PBX switching systems, and any off-network trunk connections or ISTs. The analog interfaces apply to EOS trunks, ISTs, and off-network trunk connections.

5.2.6.1 PCM-24 Digital Trunk Interface

[Required: TS, MFS, EOS, SMEO, DVX-C, DVX-L, PBX1, PBX2] DSN switches shall provide a PCM-24 channel digital interface with a 1.544 Mbps T1 bit stream configured in either the D3/D4 (Super Frame) framing format or the D5 Extended Super Frame (ESF) framing format. D5 is also referred to as Extended Frame (EF). The same framing format shall be used in both directions of transmission. Voice signals shall be encoded in the 8-bit µ (255 quantized values) pulse code modulation (PCM) encoding law. Supervisory and dial pulse (DP) signals shall utilize the A and B bits of the D3/D4 format or the A, B, C, and D bits of the D5 format for pre-CCS7 configurations. Voice channel address in-band signaling shall be provided on individual channels. The D5 format shall be the preferred and system "goal" digital framing format and shall be provided in accordance with MIL-STD-187-700.

5.2.6.1.1 Interface Characteristics

[Required: TS, MFS, EOS, SMEO, DVX-C, DVX-L, PBX1, PBX2] The DSN switching system shall use the DS1 24 channel standard interface as specified in ANSI T1.102, "Digital Hierarchy – Electrical Interfaces."

Table 5.2.6-1, PCM-24 Electrical Interface Characteristics, provides the electrical characteristics at the interface. Table 5.2.6-2 and Table 5.2.6-3 provide a listing of the framing characteristics.

Table 5.2.6-1. PCM-24 Electrical Interface Characteristics

Nominal Line Rate	1.544 Megabits per second.
Line Rate Accuracy	In a self-timed, free running mode, the line rate accuracy shall be ± 50 bits/s (± 32 parts per million) or better.
Line Code	B8ZS (Bipolar with 8-Zero Substitution) Bipolar/Alternate Mark Inversion may be used until Clear Channel Capability is required.
Frame Structure	ESF (D5) or transitionally D3/D4.
Medium	One balanced twisted pair shall be used for each direction of transmission.
Pulse Amplitude	The amplitude of an isolated pulse shall be between 2.4 volts and 3.6 volts.
Pulse Shape	The shape of every pulse that approximates an isolated pulse (is preceded by four zeros and followed by one or more zeros) shall conform to the mask in figure F10/G703 of ITU- T Recommendation G.703.
Pulse Imbalance	In any window of seventeen consecutive bits, the maximum variation in pulse amplitudes shall be less than 200mV, and the maximum variation in pulse widths (half amplitude) shall be less than 20 ns.
Power Level	For an all-ones signal, the power in a 3 kHz band centered at 772 kHz shall be between 12.6 dBm and 17.9 dBm. The power in a 3 kHz ± 1 kHz band centered at 1544 kHz shall be at least 29 dB below that at 772 kHz.
Jitter	Where one Unit Interval (UI) is equal to 648 ns, the jitter of the signal shall not exceed the following limits, in both bands simultaneously: 1) Band 1 - 5.0 UIs, peak-to-peak, and 2) Band 2 - 0.1 UIs, peak-to-peak. Band 1 equals 10 Hz to 40 kHz. Band 2 equals 8 kHz to 40 kHz.
DC Power	There shall be no dc power applied to the interface.

Table 5.2.6-2. PCM-24 D3/D4 Interface Characteristics

Frame Organization	24 8-bit PCM words, plus 1 framing bit, in 125 microseconds.
Channel PCM Word	Frames 1 through 5: 8-bit encoded voice sample.
	Frame 6: 7-bit encoded voice sample; least significant bit is the “A” signaling bit.
	Frames 7 through 11: 8-bit encoded voice sample.
	Frame 12: 7-bit encoded voice sample; least significant bit is the “B” signaling bit.
Channel Sampling Rate	8000 times per second.
Channel Time Slot	5.18 microseconds.
Bit Time Slot	648 nanoseconds.
Framing Bit Pattern	Terminal Framing Bit: “101010” in odd-numbered frames (1, 3, 5, 7, 9, 11).
	Signaling Framing Bit: “001110” in even-numbered frames (2, 4, 6, 8, 10, 12).
Maximum Reframe Time	The DSN will reframe on the average within 50 milliseconds after an error free signal is restored.

Table 5.2.6-3. PCM-24 ESF Interface Characteristics

D5 EXTENDED SUPER FRAME FORMAT FRAMING CHARACTERISTICS	
Frame Organization	24 8-bit PCM words, plus 1 framing bit, in 125 microseconds.
Channel PCM Word	Frames 1 through 5: 8-bit encoded voice sample.
	Frame 6: 7-bit encoded voice sample; least significant bit is the “A” signaling bit.
	Frames 7 through 11: 8-bit encoded voice sample.
	Frame 12: 7-bit encoded voice sample; least significant bit is the “B” signaling bit.
	Frames 13 through 17: 8-bit encoded voice sample.
	Frame 18: 7-bit encoded voice sample; least significant bit is the “C” signaling bit.
	Frames 19 through 23: 8-bit encoded voice sample.
	Frame 24: 7-bit encoded voice sample; least significant bit is the “D” signaling bit.
Channel Sampling Rate	8000 times per second.
Channel Time Slot	5.18 microseconds.
Bit Time Slot	648 nanoseconds.
Framing Bit Pattern	Frame and Super Frame Synchronization Bit: 001011 (frames 4, 8, 12, 16, 20, 24).
	CRC Bit (frames 2, 6, 10, 14, 18, 22).
	Data Channel Link Bit (odd numbered frames 1, 3, 5, 7, 9, 11, 13, 15, 17, 19, 21, 23).
Maximum Reframe Time	The DSN will reframe on the average within 50 milliseconds after an error free signal is restored.

5.2.6.1.2 Supervisory Channel Associated Signaling

[Required: TS, MFS, EOS, SMEO, DVX-C, DVX-L – Conditional: PBX1, PBX2] On-hook and off-hook status of each channel is transmitted and derived from the coding of the “A” and “B” signaling bits. Trunk seizure, answer supervision, dial pulse digits (DPs), preemption signals and all other trunk supervisory information shall be sent and received on a per-channel basis using this scheme. Per-trunk signaling in the DSN switching system shall control the value of the “A” and “B” bits to indicate an on-hook (“A” = 0, “B” = 0) or an off-hook (“A” = 1, “B” = 1) condition. When receiving supervisory status on digital trunks using the PCM-24 format, the DSN switching system shall interpret the combination of the “A” bit = 0 and the “B” bit = 0 as on-hook, and the combination bit = 1 and “B” bit = 1 as an off-hook indication. When signaling on VF channels using the PCM-24 format, the least significant bit of each channel, every six frames, shall carry signaling information. Utilizing the four-state signaling option of the Super Frame (D3) format, frame 6 shall contain the “A” channel signaling information and frame 12 shall contain the “B” channel signaling information. The switching system shall also interpret the combination of “A” bit = 1, “B” bit = 0, with bit position 2 in all 24 channels in the Super Frame (D3) format equal to “0” as a channel alarm indication and shall also interpret the combination of “A” bit = 1, “B” bit = 0 as a remote make busy.

In the Extended Super Frame (ESF) format ANSI defines a sixteen-state signaling option that labels the signaling bits "A" (frame 6), "B" (frame 12), "C" (frame 18), and "D" (frame 24). Because DSN does not require the "C" and "D" signaling channels the four-state option shall be used to allow changes in "A" and "B" signaling states to be transmitted twice as often. Utilizing Frames 6 and 18 in the 24-frame Extended Super Frame shall contain the "A" channel signaling information; frames 12 and 24 shall contain the "B" channel signaling information.

5.2.6.1.3 Clear Channel Capability

[Required: TS, MFS, EOS, SMEO, DVX-C, DVX-L, PBX1 – Conditional: PBX2] DSN switches shall be capable of transmitting and receiving B8ZS line coding in accordance with MIL-STD-187-700.

5.2.6.1.4 Alarm and Restoral Requirements

[Required: TS, MFS, EOS, SMEO, DVX-C, DVX-L, PBX1 – Conditional: PBX2] The DSN switching system shall provide the alarm and restoral features on the digital interface unit (DIU) as defined in Table 5.2.6-4, PCM-24 Alarm and Restoral Requirements.

5.2.6.2 PCM-30 Digital Trunk Interface

[Required: TS, MFS, EOS, SMEO – Conditional: DVX-C, DVX-L, PBX1, PBX2] This requirement only applies to switches implemented in Europe. The DSN switches used in DISN-E shall provide PCM-30 digital interfaces at a data rate of 2.048 Mbps. The PCM-30 interfaces shall meet the requirements of ITU-T Recommendation G.703 and ITU-T Recommendation G.732. Voice signals in the PCM-30 framing format shall utilize the A-law encoding technique in accordance with ITU-T Recommendation G.772 (REV), "*Protected Monitoring Points on Digital Transmission Systems.*" The pertinent requirements for the PCM-30 interface are summarized in Table 5.2.6-5, PCM-30 Electrical Interface Characteristics.

Table 5.2.6-4. PCM-24 Alarm and Restoral Requirements

LOCAL ALARM TIMING	The DSN PCM-24 DIU (digital interface unit) will enter the "LOCAL" or "RED" alarm state when it is unable to frame on the received PCM signal, or the received signal is lost, for 2.5 ± 0.5 seconds.
RECEPTION OF REMOTE ALARM	The DSN PCM-24 DIU will detect a "REMOTE" or "YELLOW" alarm condition when bit 2 of all 24 channels of Super Frame is set to a zero and when the "YELLOW" alarm is sent via the facility data link of Extended Super Frame. Within 35 to 1000 milliseconds after detecting the REMOTE alarm, the DSN switch will: Release all connections on the affected DIU, AND Remove the affected circuits from service.
TRANSMISSION OF REMOTE ALARM	When the DSN PCM-24 DIU enters the LOCAL alarm state, it will send REMOTE alarm toward the connecting equipment by forcing bit 2 to a zero on all 24 channels of Super Frame.
RESTORAL TO SERVICE FROM LOCAL ALARM	Within 15 ± 5 seconds after a valid PCM signal is restored, the DSN DIU will: Remove the REMOTE alarm being sent to the connecting equipment, AND Return the affected circuits to service.
RESTORAL TO SERVICE FROM REMOTE ALARM	Within 20 to 1000 milliseconds after the connecting equipment removes the REMOTE alarm, the DSN switch DIU will restore the affected circuits to service.

Table 5.2.6-5. PCM-30 Electrical Interface Characteristics

Nominal Line Rate	2.048 Megabits per second.
Line Rate Accuracy	In a self-timed, free running mode, the line rate accuracy shall be ± 102 bits/s (± 50 parts per million) or better.
Line Code	HDB3.
Frame Structure	Frame structure details appear in ITU-T RecommendationG.704.
Medium	One balanced twisted pair shall be used for each direction of transmission.
Pulse Amplitude	The amplitude of an isolated pulse shall be between 2.2 volts and 3.3 volts.
Pulse Shape	The shape of every pulse that approximates an isolated pulse (is preceded by three zeros and followed by one or more zeros) shall conform to the mask in figure 1 5/G703 of ITU-T Recommendation G.703.
Pulse Imbalance	The ratio of amplitudes of positive and negative isolated pulses shall be between 0.95 and 1.05.
Power Level	For an all-ones signal, the power in a 3 kHz ± 1 kHz band centered at 1.024 MHz shall be between 13.7 dBm and 17.5 dBm. The power in a 3 kHz ± 1 kHz band centered at 2.048 MHz shall be at least 20 dB below that at 1.024 MHz.
Jitter	Where one Unit Interval (UI) is equal to 488 ns, the jitter of the signal shall not exceed the following limits, in both bands simultaneously: 1) Band 1 - 5.0 UIs, peak-to-peak, and 2) Band 2 - 0.1 UIs, peak-to-peak. Band 1 equals 10 Hz to 40 kHz. Band 2 equals 8 kHz to 40 kHz.
dc Power	There shall be no dc power applied to the interface.
Frame	32 channels (numbered 0 to 31) with 8 bits (numbered 1 to 8) per channel.
Organization	PCM words. Frame alignment occupies bit positions 2 through 8 of channel 0, of every other frame.
Multiframe Organization	16 consecutive frames, numbered from 0 to 15.
Channel Sampling Rate	8000 times per second.
Channel PCM Word	Channel time slots 1 to 15, and 17 to 31, are assigned to telephone channels 1 to 30.
Channel Time Slot	3.91 microseconds.
Tolerance	+50 ppm on line rate of 1.544 megabits per second.
Bit Time Slot	488 nanoseconds.
Framing Bit Pattern	Bits 2 through 8 of channel 0, every other frame, contains the “0011011” frame alignment signal. To avoid falsely locking to the data contained in channel 0 for frames not containing the frame alignment signal, bit 2 of channel 0 is always a “1” in those frames.
Multiframe Alignment	The multiframe alignment signal is “0000” and occupies digit time slots 1 to 4 of channel time slot 16 in frame 0.
Framing Strategy	Frame alignment is assumed to be lost if 3 of 4 consecutive frame alignment signals are received with an error.
Reframing Algorithm	Frame alignment is assumed to be recovered if the next frame has a “1” in bit 2 of channel 0 and valid framing is present in the frame after that.
Multiframe Loss and Recovery	Multiframe alignment is assumed to be lost when two consecutive multiframe alignment signals are received in error. Multiframe alignment is assumed to be restored when the first correct multiframe alignment signal is detected.

Table 5.2.6-6 shows the allocation of time slot 16 for channel associated signaling.

Table 5.2.6-6. Allocation of Time Slot 16

CHANNEL TIME SLOT 16 OF FRAME 0	CHANNEL TIME SLOT 16 OF FRAME 1		CHANNEL TIME SLOT 16 OF FRAME 2		FR 3-14 18-29	CHANNEL TIME SLOT 16 OF FRAME 15	
0000 xyxx	ABCD Channel 1	ABCD Channel 16	ABCD Channel 2	ABCD Channel 17	3-14 18-29	ABCD Channel 15	ABCD Channel 30
NOTES When bits B, C, or D are not used they shall have the value: B = 1 C = 0 D = 1. The combination 0000 of bits A, B, C, and D shall not be used for signaling purposes for channels 1-15.							
LEGEND x = Spare bit to be made 1 if not used. y = Bit used to indicate loss of multiframe alignment (REMOTE alarm).							

5.2.6.2.1 Supervisory Channel Associated Signaling

[Required: TS, MFS, EOS, SMEO – Conditional: DVX-C, DVX-L, PBX1, PBX2] When receiving supervisory status on digital trunks using the PCM-30 format, the DSN switching system shall interpret the combination of the “A” signaling channel bit = 1 and the “B” signaling channel bit = 1 as on-hook, and shall interpret the combination of the “A” signaling channel bit = 0 and the “B” signaling channel bit = 1 as an off-hook indication. The DSN switching system shall also interpret the combination of “A” bit = 1 and “B” bit = 0 as a channel alarm indication and a remote make busy. Bits “C” and “D” are not used in the DSN for signaling or control and therefore shall be set to the values “C” = 0 and “D” =1 in accordance with ITU-T Recommendation G.704.

5.2.6.2.2 Alarm and Restoral Requirements

[Required: TS, MFS, EOS, SMEO – Conditional: DVX-C, DVX-L, PBX1, PBX2] The DSN switching system shall provide the alarm and restoral features on the DIU in order to be compatible with PCM-30 facilities and terminal equipment, as shown in Table 5.2.6-7.

Table 5.2.6-7. PCM-30 Alarm and Restoral Requirements

LOCAL ALARM TIMING	The DSN PCM-30 DIU shall enter the "LOCAL" or "RED" alarm state when framing is lost, or the incoming signal is lost, for 4.5 ± 0.5 seconds.
RECEPTION OF REMOTE ALARM	The DSN PCM-30 DIU shall detect a "REMOTE" or "YELLOW" alarm condition when bit 3 of channel time slot 0 in those frames not containing the frame alignment signal is set to a "1," and will interpret this transition as a remote alarm from the connecting equipment. Within 35 to 1000 ms after detecting the REMOTE alarm, the DSN switch will: Release all connections on the affected DIU, AND Remove the affected circuits from service.
TRANSMISSION OF REMOTE ALARM	When the DSN PCM-30 DIU enters the LOCAL alarm state, it shall send within 2 ms a REMOTE alarm toward the connecting equipment by changing bit 3 channel time slot 0 from a "0" to a "1" in those frames not containing the frame alignment signal.
RESTORAL TO SERVICE FROM LOCAL ALARM	Within 15 ± 5 seconds after a valid PCM signal is restored, the DSN switch shall: Remove the REMOTE alarm being sent to the connecting equipment, AND Return the affected circuits to service.
RESTORAL TO SERVICE FROM REMOTE ALARM	Within 20 to 1000 ms after the connecting equipment removes the REMOTE alarm, the DSN switch shall restore the affected circuits to service.

5.2.6.3 Interoperation of PCM-24 and PCM-30 Systems

[Required: TS, MFS, EOS, SMEO – Conditional: DVX-C, DVX-L, PBX1, PBX2] Interoperation of PCM-24 and PCM-30 transmission shall occur internal to DSN switching equipment. The internal design of the DSN switch shall perform the required A-law-to-µ-law conversions necessary to switch or cross-connect time slot data, regardless of the source. The conversion shall be accomplished in accordance with ITU-T Recommendation G.711.

5.2.6.4 Analog Trunk Interface

[Conditional: TS, MFS, EOS, SMEO, DVX-C, DVX-L, PBX1, PBX2] The DSN switching system shall provide analog trunk circuits that interface to industry standard signaling and facility arrangements.

5.2.6.4.1 E&M Trunk Circuits

[Conditional: TS, MFS, EOS, SMEO, DVX-C, DVX-L, PBX1, PBX2] The DSN switching system shall interface with exchange carriers using industry standard E&M signaling. The

switching system shall interface with Type I and Type II E&M signaling in accordance with paragraph 9 and subparagraphs of GR-506-CORE. The switching system shall interface with Type V E&M signaling as defined in Paragraphs 6.8.5, 6.8.6, 6.8.7.2, 6.8.8.2, and 6.8.8.3 of Telcordia Technologies Document SR-2275. The DSN switch analog trunk interface shall always originate on the M-lead.

5.2.6.4.2 Single Frequency Trunk Circuits

[Conditional: TS, MFS, EOS, SMEO, DVX-C, DVX-L, PBX1, PBX2] The DSN will interface with external SF equipment using a 4-wire E&M trunk circuit, either Type I or II. DSN in-band signaling equipment utilizing SF will place a 2600 Hz tone on the circuit to indicate the idle state (on-hook) and the tone will be removed from the circuit to indicate the busy state (off-hook). Signaling states will be conveyed via E and M leads (Type I or II) to the telephone equipment terminating the circuit on the equipment side of the interface. The SF trunk interface consists of only the voice path conductors (T, R, T1, R1), but at a point between this transmission facility interface and the switching function the SF signal will be translated back to the two-state dc signals.

5.2.6.4.3 Dual Frequency Trunk Circuits

[Conditional: TS, MFS, EOS, SMEO, DVX-C, DVX-L, PBX1, PBX2] The Dual Frequency Signaling Unit (DFSU) equipment used in the DSN operates in much the same way as an SF unit, except that whenever the 2600 Hz tone is removed from the circuit a 2800 Hz tone is applied for a short period (175 ms maximum). The 2800 Hz tone burst will serve as a confirmation tone; the receiving signaling unit will only transition from on-hook to off-hook if the loss of the 2600 Hz tone is followed by the 2800 Hz tone. This prevents false on-hook to off-hook transitions from occurring due to a break in the communications circuit. Like the SF trunk interface, the DF trunk interface will consist of only the voice path conductors (T, R, T1, R1). The DSN switch shall interface an external DFSU using a 4-wire E&M trunk circuit with Type I or II E&M signaling. This connection is on the equipment-side of a DF trunk interface.

5.2.6.5 Integrated Digital Loop Carrier

[Required: TS, MFS, EOS – Conditional: SMEO, DVX-C, PBX1, PBX2] The DSN switching system shall interface with IDLC equipment in accordance with Telcordia Technologies GR-303-CORE, *System Generic Requirements, Objectives, and Interface*, December 2000, Issue 4. The DSN switching system shall provide the capability to handle external carrier systems/equipment alarm indications from the carrier systems/equipment using the E-telemetry interface (scan points) at the DS0, DS1, and OC3 rates, and comply to the Telcordia Technologies GR-303-CORE and Telcordia Technologies TR-NWT-000057 that

specifies the use of an COT-generated DC contact closure alarm to indicate an "all-accessible-channels-busy" condition.

The DSN switch when interfaced to carrier systems/equipment that provides an E-telemetry interface type (scan points) for alarm management shall be capable of E-telemetry management that is used to minimize the effects of carrier failures on switching systems and on service. E-telemetry scan point (binary condition i.e., "closed" contact for active and "opened" for inactive states) when "closed" should busy out the failed circuits, release customers from the failed circuits, and prevent the failed circuits from seizing the DSN trunk equipment and prevent the DSN switch from seizing the failed circuits.

5.2.6.5.1 E-Telemetry Scan Point System Operation

[Required: TS, MFS, EOS – Conditional: SMEO, DVX-C, PBX1, PBX2] The DSN E-telemetry System Operation shall be divided into three parts, i.e., detection of the carrier alarm, conditioning the alarmed trunk, and reaction of the switching equipment to the processing of the alarm. Requirements for E-telemetry scan point are:

1. Sense Point Interface. The switching system shall provide sense points to which external carrier systems/equipment can be interfaced to, so that alarm of the carrier equipment shall cause the idle trunks to be removed from service.

2. Call Processing Actions. Receipt of an external carrier systems/equipment alarm shall cause additional call processing to be aborted on associated trunks that are not in the talking state.

3. Trunk Conditioning. Receipt of an external carrier systems/equipment alarm shall cause the following actions on the affected trunks:

    a. Idle trunks shall be removed from the idle list. Subsequent calls for service must be ignored for the duration of the external carrier systems/equipment alarm. Busy-back shall be returned on those incoming trunks that are optioned for busy-back while in the out-of-service state and proper MLPP treatment shall be applied.

    b. Trunks in the talking state shall be monitored for disconnect, after which they are to be placed in the same state as described above for idle trunks.

4. Restoration of Service. All trunks affected shall be returned to their previous state after the external carrier systems/equipment alarm is removed.

5.2.7 Tandem Switching

This section contains the tandem switching requirements for DSN MFSs and TSs. It is based on the Telcordia Technologies GR-540-CORE, *LSSGR: Tandem Supplement*, Issue 2, March 1999. The requirements in this section apply to systems using existing analog or digital technology. LSSGR features and capabilities that require modification for use in the DSN are described as are MUFs.

5.2.7.1 Network Plan

Tandem switching systems provide a means of routing traffic in an orderly manner and make economic use of trunks and switching equipment, where otherwise, many small separate trunk groups would be necessary. The switch performs trunk-to-trunk switching for concentrating traffic for the centralization of services.

5.2.7.2 System Design

The switching system design is largely a function of technology. DSN switching systems are digital and interface with both digital and analog access lines and trunks. The DSN system design is described in UCR 2008, Section 4.4.2, TDM-Based SBU Voice (DSN) System Design.

5.2.7.3 Tandem Capabilities

[Required: TS, MFS] DSN switching systems requiring tandem switching features and functions shall provide the features and functions shown in Table 5.2.7-1 and defined in the Telcordia Technologies GR-540-CORE, Paragraph 4.1. LSSGR features not shown in Table 5.2.7-1 are not required.

5.2.7.4 Call Processing

[Required: TS, MFS] The DSN switching systems that require tandem features and capabilities shall meet the call processing requirements in the Telcordia Technologies GR-540-CORE, Paragraph 5, and all its subparagraphs. In addition, tandem switching systems shall meet the call processing requirements in Section 4, Call Processing.

Table 5.2.7-1. Tandem Features

FEATURE DEFINITION #	DESCRIPTION	GR-540-CORE SECTION
60-00-0000	Tandem Features	Section 4.2.1
60-01-0000	Access Tandem Office Trunks	Section 4.2.2
60-01-0100	Tandem Connecting Trunks	Section 4.2.3
60-01-0101	DDD Access (DD) Trunks	Section 4.2.3.1
60-01-0104	Tandem Completing (TC) Trunks	Section 4.2.3.3
60-01-0106	Two-way Tandem connecting Trunks (Not Coded)	Section 4.2.3.4
60-01-0200	Intertandem Trunks	Section 4.2.4
60-01-0500	Special Service Trunks	Section 4.2.5
60-01-0501	Direct Inward Dial (DID)	Section 4.2.5.1
60-02-0000	Call Processing Features	Section 4.2.6
60-02-0100	Trunk-to-Trunk Test Connections	Section 4.2.6.1
60-02-0200	3-Digit Translation	Section 4.2.6.2
60-02-0202	NXX Office and Special Purpose Codes	Section 4.2.6.3
60-02-0203	NXX Area Codes	Section 4.2.6.2
60-02-0300	6-Digit Translation	Section 4.2.6.2
60-02-0400	Digit Deletion	Section 4.2.6.3
60-02-0500	Digit Prefixing	Section 4.2.6.3
60-02-0600	Code Conversion	Section 4.2.6.3
60-02-0900	Capability for Satellite Connections	Section 4.2.6.5
60-02-1000	Recorded Announcement Service (Tandem)	Section 4.2.6.6
60-02-1100	Overlap Outpulsing	Section 4.2.6.7
60-02-1200	Vacant Code Screening	Section 4.2.6.8
60-02-1300	Trunk Class Screening	Section 4.2.6.9
60-03-0000	Tandem Signaling	Section 4.2.7
60-03-0100	Common Channel Signaling	Section 4.2.7.1
60-03-0200	Inband Trunk Signaling (Tandem)	Section 4.2.7.2
60-04-0000	Line and Trunk Test Features	Section 4.2.8
60-04-0100	Test Lines	Section 4.2.8.1
60-04-0101	All 10X-Type Test Lines Used on End Offices	Section 4.2.8.1.1
60-04-0102	103-Type Tests Line	Section 4.2.8.1.2
60-04-0103	104-Type Tests Line	Section 4.2.8.1.3
60-04-0104	108-Type Tests Line	Section 4.2.8.1.4
60-04-0105	109-Type Tests Line	Section 4.2.8.1.5
60-04-0200	Multiple Trunk Test Capability	Section 4.2.8.2
60-04-0600	FX Line for ROTL in Tandem Offices	Section 4.2.8.3
60-04-0700	Two-way Trunk Maintenance	Section 4.2.8.4
60-04-0900	Continuity Check of the Switch Voice Path	Section 4.2.8.5
60-05-0000	Network Management Features	Section 4.2.9
60-05-0102	Trunk Reservation	Section 4.2.9.1.1
60-05-0105	Automatic Out-of-Chain Routing	Section 4.2.9.1.2
60-05-0200	Manual Network Management Controls	Section 4.2.9.1.3

FEATURE DEFINITION #	DESCRIPTION	GR-540-CORE SECTION
60-05-0201	Code Controls	Section 4.2.9.1.4
60-05-0202	Trunk Group Controls	Section 4.2.9.1.5
60-05-0203	Administration of Hard-to-Reach Codes	Section 4.2.9.1.6
60-05-03 00	Network Management Surveillance Data	Section 4.2.9.1.7
60-05-0400	NTM OS/NE Interface	Section 4.2.9.1.8
60-05-0401	NM Audits and Alerts	Section 4.2.9.1.9
60-05-0402	Message Administration	Section 4.2.9.1.10
60-05-0500	Backup Network Management Capabilities	Section 4.2.9.1.11
60-05-0600	Trunk Directionalization	Section 4.2.9.1.12
60-06-0000	Billing	Section 4.2.10
60-10-0200	Echo Cancellers	Section 4.2.12

5.2.7.5 Signaling

[Required: TS, MFS] The DSN switching systems that require tandem features and capabilities shall meet the signaling requirements UCR 2008, Section 5.2.4, Signaling.

5.2.7.6 Transmission

[Required: TS, MFS] The DSN switching systems that require tandem features and capabilities shall meet the transmission requirements in UCR 2008, Section 5.2.5, Transmission.

5.2.7.7 Measurements and Administration

[Required: TS, MFS] The DSN switching systems with tandem functions and capabilities shall meet the switching system maintenance, circuit and facility maintenance, and maintenance measurement requirements in the Telcordia Technologies GR-540-CORE, Paragraph 9 and all its subparagraphs, and Sections 5.2.6 and 5.2.7. Centralized Automatic Message Accounting (CAMA) shall not be required.

5.2.7.8 Service Standards

[Required: TS, MFS] The DSN switching systems with tandem features and capabilities shall meet the service standards in the Telcordia Technologies GR-540-CORE, Chapter 11 with the exception of CAMA. In addition, DSN tandem switching systems shall provide non-blocking service.

5.2.7.9 Network Management

[Required: TS, MFS] The DSN switching systems with tandem features and capabilities shall meet the network management requirements specified in UCR 2008, Section 5.2.8, Network Management.

5.2.8 Network Management

DISA has developed a network management system to monitor and control the Global DSN. This system, the Advanced DSN Integrated Management Support System (ADIMSS), is fielded and operational. It was developed by drawing on the framework setup by the LSSGR for telephone switch management, within the public telephone system network. However, DISA realizes that many of the switching systems being deployed in the DSN today were neither intended nor designed to function as part of the public telephone network infrastructure. Therefore, DISA developed the requirements in this section to specifically address the NM requirements of telephone switches to be used within the DSN.

The NM functions covered in this section are:

- Fault Management
- Configuration Management
- Accounting Management
- Performance Management
- Network Management Controls
- Remote Access to the Switch

5.2.8.1 DISA/DSN Network Management

[Required: TS, EOS, SMEO, DVX-C, DVX-L, MFS] The DSN switching systems shall provide DSN NM data to the DISA ADIMSS via one of the three following physical interfaces:

- Ethernet/TCP/IP (IEEE 802.3)
- Serial (RS-232)/Asynchronous
- Serial/Synchronous (X.25 and/or BX.25 variant)

All data that is collected shall be accessible through these interfaces. For DSN Network Management purposes, the telephone switch must provide four separate data channels. They may be physically separate (e.g., four distinct physical interface points) or logically separate (e.g., four user sessions through a single Ethernet interface). The data may be sent in ASCII, binary, or hexadecimal data or ASCII text designed for screen/printer display.

The data channels shall be used for and, as such, must be capable of providing:

- Alarm/Log Data
- Performance Data (e.g., traffic data)
- Accounting Data (e.g., Call Detail Recording)
- Switch access (to perform switch data fill administration and network controls)

5.2.8.2 Measurements and Data Generation

This section contains the measurements and data generation requirements that shall be collected by DSN switching systems. The measurements and data collected are used to maintain, manage, and engineer the DSN.

5.2.8.2.1 Common Data Requirements

5.2.8.2.1.1 Data Quality

[Required: TS, MFS, EOS, SMEO, DVX-C, DVX-L] The DSN switching systems shall meet the data quality and data presentation requirements in Telcordia Technologies, GR-478-CORE, Issue 4, February 2000, Section 2, Paragraphs 2.3 and 2.4. The SMEO is not required to meet the 30-second and 5-minute Traffic Data Reporting Requirements in GR-478-CORE, Paragraph 2.4.1, Table 5.2.1-1. However, SMEOs shall meet the 15- or 30- or 60-minute, and daily reporting requirements.

5.2.8.2.2 Circuit-Switched Network Measurements

5.2.8.2.2.1 Basic Switch Performance

The DSN switching systems shall meet the following switch performance requirements in Telcordia Technologies, GR-478-CORE, Section 3.1.

5.2.8.2.2.1.1 Traffic Measurements

[Required: TS, MFS, EOS] DSN switching systems shall meet the traffic measurement requirements in Telcordia Technologies, GR-478-CORE, Section 3, Paragraph 3.1.1.

[Required: SMEO, DVX-C, DVX-L] DSN switching systems shall provide traffic measurements for the following:

- Provide the required Traffic NM data in either 5-, 15-, 30-, or 60-minute increments
- Trunk Group Number
- Trunks Equipped
- Outgoing Attempts
- Outgoing Overflows
- Trunk Group Usage (in seconds or hundred call seconds (ccs))
- Total Trunk Group Usage or Outgoing and Incoming Trunk Group Usage
- Switch Database Access

5.2.8.2.2.1.2 Reference Data

[Required: TS, MFS, EOS – Conditional: SMEO, DVX-C, DVX-L] The DSN switching systems shall meet the reference data optional requirements in Telcordia Technologies Generic Requirements, GR-478-CORE, Section 3, Paragraph 3.1.3.

5.2.8.2.2.2 Line Servicing

[Required: TS, MFS, EOS – Conditional: SMEO, DVX-C, DVX-L] The DSN switching systems shall meet the line servicing requirements in Telcordia Technologies, GR-478-CORE, Section 3.2.

5.2.8.2.2.3 Trunk Groups

[Required: TS, MFS, EOS – Conditional: SMEO, DVX-C, DVX-L] The DSN switching systems shall meet the trunk group requirements in Telcordia Technologies, GR-478-CORE, Section 3.3.

5.2.8.2.2.4 Call Processor

[Required: TS, MFS, EOS – Conditional: SMEO, DVX-C, DVX-L] The DSN switching systems shall meet the call processor requirements in Telcordia Technologies, GR-478-CORE, Section 3.4.

5.2.8.2.2.5 Switch Services

[Required: TS, MFS, EOS – Conditional: SMEO, DVX-C, DVX-L] The DSN switching systems shall meet the switch service requirements in Telcordia Technologies, GR-478-CORE, Section 3.5.

5.2.8.2.2.6 Special Studies

[Required: TS, MFS, EOS – Conditional: SMEO, DVX-C, DVX-L] The DSN switching systems shall meet the special studies requirements in Telcordia Technologies, GR-478-CORE, Section 3.6. Requirements referring to ISDN are optional for SMEO switches.

5.2.8.2.2.7 Remote Switching Site

[Conditional: MFS, EOS, SMEO, DVX-C, DVX-L] The DSN switching systems that support remote switching sites shall meet the remote switching site traffic and reference data requirements in Telcordia Technologies, GR-478-CORE, Section 3.7, Paragraphs 3.7.1 and 3.7.2.

5.2.8.2.2.8 Features

[Conditional: MFS, EOS, SMEO, DVX-C, DVX-L] The DSN switches shall meet the traffic data requirements for features. Descriptions of the requirements are found in Telcordia Technologies, GR-478-CORE, Section 3.10.

5.2.8.2.3 Common Channel Signaling Network Measurements

[Required: TS, EOS, MFS – Conditional: SMEO, DVX-C, DVX-L] The DSN switching systems shall meet the Common Channel Signaling Network (CCSN) measurement requirements in Telcordia Technologies, GR-478-CORE, Section 4.

5.2.8.2.4 ISDN Measurements

[Required: TS, MFS, EOS, SMEO, DVX-C] The DSN switching systems providing ISDN services shall meet the ISDN measurement requirements in Telcordia Technologies, GR-478-CORE, Section 6.

5.2.8.2.5 Traffic Capacity

[Required: MFS, TS, EOS, SMEO, DVX-C] Requirements for Traffic Capacity shall be in accordance with Telcordia Technologies GR-517-CORE.

5.2.8.3 Fault Management

[Required: TS, EOS, SMEO, DVX-C, DVX-L, MFS] The DSN telephone switching systems shall detect fault (alarm) conditions and generate alarm notifications. The alarm messages must be sent to the assigned NM Alarm channel in near-real time. No alarm restriction/filtering is necessary. In addition to the data formats in Section 5.2.8.1, DISA/DSN Network Management, alarms may be sent as Simple Network Management Protocol (SNMP) traps.

If this channel is also used to output switch administrative log information, the alarm messages must be distinguishable from an administrative log message.

5.2.8.4 Configuration Management

[Required: TS, MFS, EOS, SMEO, DVX-C, DVX-L] Requirements for this feature shall be in accordance with Telcordia Technologies GR-472-CORE, Section 4.

5.2.8.5 Automated Message Accounting

The Automated Message Accounting (AMA) process in a switching system provides usage related data to perform customer billing and call detail recording (CDR).

5.2.8.5.1 DSN Call Detail Recording Fields

[Required: EOS, SMEO, MFS – Conditional: DVX-C, DVX-L] The data fields for DSN Call Detail Recording shall be as shown in Table 5.2.8-1, CDR Data. These requirements fall into one of two categories:

- "R" = REQUIRED: feature/function required and must adhere to the specific UCR 2008 requirements

Table 5.2.8-1. CDR Data

MFS	EOS	SMEO	DESCRIPTION
R	R	R	The telephone switching system must be able to generate call accounting information, CDR. The call accounting information must be able to be sent to the NM CDR channel when requested by the NM system.
R	R	R	The CDRs can be provided in any format, but as a minimum, must contain the data elements listed below:
R	R	R	1) Start Date of Call (in Julian or Calendar)
R	R	R	2) Start Time of Call (Hour + Minute + Second)
R	R	R	3) Either (or both) a) Elapsed Time of Call b) Stop Time of Call
R	R	R	4) Calling Number
R	R	R	5) Called Number (must include all dialed digits)
R	R	R	6) Precedence Level of Call (NOTE: This may be accomplished by either a specific precedence level designation field in the call record or by providing the dialed precedence level access digits in the called number field.)
R	R	R	7) Outgoing Trunk Group of the Call
R	R	R	8) Outgoing Trunk Group member of the Call
R	R	NR	9) Incoming Trunk Group of the Call
R	R	NR	10) Incoming Trunk Group Member of the Call
R	R	NR	11) Call Answered/Unanswered Indicator
R	R	NR	12) Conference Call Indicator
R	R	NR	13) Customer/Business Group Identification
R = Required NR = Not Required			

- "NR" = NOT REQUIRED: feature/function not required.

5.2.8.5.2 Call Detail Recording Data Retention

[Required: EOS, MFS – Conditional: SMEO, DVX-C, DVX-L] The DSN switching systems shall have internal storage capacity to store a minimum of 5 days of CDR data.

5.2.8.6 Performance Management

[Required/Conditional: TS, EOS, MFS, SMEO] Table 5.2.8-2, Performance Management Data, contains the minimum DSN switch performance data requirements. These requirements fall into one of three categories:

1. "R" – REQUIRED: Feature/function required in a candidate switch. Must adhere to the specific UCR 2008 requirements.

2. "R/NC" – REQUIRED – NOT CRITICAL: Feature/function is required. However, the fact that a specific switch cannot provide a specific feature/function does not necessarily mean it cannot obtain a waiver from DISA to operate in the DSN, e.g., if a particular switch cannot provide traffic measurements, DISA may elect to waive that requirement.

3. "O" – OPTIONAL: Feature/function is optional. However, if the feature/function is provided, it must adhere to the specific UCR 2008 requirements – if the UCR requirement is applicable.

NOTE: Where applicable, the requirements for the performance measurements shall be in accordance with Telcordia Technologies GR-478-CORE Section 3.3. Reference to the specific Telcordia Requirement [R], Objective [O], or Conditional Requirement [CR] are shown in the Requirements column of Table 5.2.8-2.

Table 5.2.8-2. Performance Management Data

REQUIREMENT	TS/MFS	EO	SMEO	DESCRIPTION
	R	R	R	The telephone switching system shall be able to generate switch performance measurement data. The performance measurement data must sent to the assigned NM traffic channel. Ideally, the performance measurement data is polled by the NM system, but, with DISA approval, the performance measurement data may be periodically (automatically) sent to the NMS. Performance measurement reporting intervals are placed in two categories; those supporting the NRT NM function and those supporting the Off-Line Network Performance Assessment function.
NM R2-19	R	R	R	Polling Increments The MFS and EO must be able to provide the required NM data in either 5- or 15-minute increments. Those data fields marked with "NM" in the Requirements column must be provided in either 5- or 15-minute intervals. The other data fields must be provided in accordance with the "R," "R/NC," "O" marking, but may be provided in 5-, 15-, 30-, or 60-minute intervals. The SMEO must be able to provide the required NM data. The SMEO may provide this data in either 5- or 15- or 30- or 60-minute increments.

REQUIREMENT	TS/MFS	EO	SMEO	DESCRIPTION
As a minimum, the DSN switch must be able to produce the following performance measurements:				
NM O3-237[233]	R	R	R	1) Trunk Group Number
NM O3-244[240]	R	R	O	2) Trunk Group Far End CLLI
NM O3-246[242]	R	R	R	3) Trunks Equipped
	R/NC	R/NC	O	4) Trunks In Service
NM R3-203 [219]	R	R	R	5) Outgoing Attempts
NM R3-204[220]	R	R	R	6) Outgoing Overflows
NM R3-202[218]	R	R	R	7) Incoming Attempts
NM R3 - 205[221]	R	R	R	8) Trunk Group Usage (in seconds or CCS) a) Total Trunk Group Usage or b) Outgoing Trunk Group Usage & Incoming Trunk Group Usage
R3-206[222]	R	R	R/NC	9) Maintenance Usage (in seconds or CCS)
R3-25[57]	R	O	O	10) Tandem Call Count
R3-217[1331]	R	R	O	11) Glare
By Trunk Group. The number of times outgoing calls failed due to problems such as seizure failures, signaling problems, or other outgoing failures.	O	O	O	12) Outgoing Failures
By Trunk Group. The number of times an actual (or apparent) incoming call failed.	O	O	O	13) Incoming Failures
By Trunk Group. The number of times a call incoming from either a line or incoming trunk fails to find an internal switch path to an outgoing trunk group.	O	O	O	14) Out Match Fail

REQUIREMENT	TS/MFS	EO	SMEO	DESCRIPTION
CR3-230[1344]	R/NC	R/NC	O	15) Trunk Group Preemption Failure
CR3 -231 [1345]	R/NC	R/NC	O	16) Incoming Calls Preempted
CR3-232[1346]	R/NC	R/NC	O	17) Outgoing Calls Preempted
CR3 -233 [1347]	R/NC	R/NC	O	18) Incoming Precedence Calls Preempted
CR3-234[1348]	R/NC	R/NC	O	19) Outgoing Precedence Calls Preempted

5.2.8.7 Network Management Controls

DSN switches shall provide protective, expansive, automatic, and manual controls in the network switching elements.

5.2.8.7.1 Automatic Controls

[Required: TS, EOS, MFS – Conditional: SMEO, DVX-C, DVX-L] Automatic controls are network management controls that are automatically applied by the network switching elements (NSEs) when they recognize a problem due to a shortage in call processing or call carrying resources. These automatic controls, which are programmed into the switching element and triggered by the changing switching system and trunk group congestion, keep the message network working efficiently during periods of overload. Both the predetermined condition (threshold) and the required response (action to be taken automatically) are contained in the database of each NSE. These automatic controls shall consist of Automatic Congestion Controls (ACCs), Trunk Reservation (TRE), and Selective Incoming Load Controls (SILCs). Two types of automatic controls are protective and expansive. Protective controls can be used to inhibit the spread of congestion in the network by restricting normal trunk group access and overflow (trunk group controls) or by limiting the attempts on selected destination or signaling codes (code controls). Expansive controls are used to expand routing beyond the normal in-chain routes when in-chain routes are busy or have failed and there exists idle capacity in out-of-chain routes.

5.2.8.7.1.1 Automatic Congestion Controls

[Required: TS, EOS, MFS – Conditional: SMEO, DVX-C, DVX-L] Automatic Congestion Controls provide a congested switching system with the capability to use Signaling System 7 (SS7) to notify linked switches of its level of congestion. The linked switching systems can then reduce the traffic offered to the congested switch. Controls such as this can significantly increase the throughput of completed calls through a network during periods of overload. The ACC detects and responds to two levels of switching congestion (i.e., CL1 and CL2). The ACC has two components:

- Detection and Transmission of congestion status
- Reception and Response to congestion status

Refer to GR-477-CORE, Section 4.3.1, for a detailed description of ACC.

5.2.8.7.1.2 Trunk Reservation

[Required: TS, EOS, MFS – Conditional: SMEO, DVX-C, DVX-L] Trunk Reservation is an automatic trunk group control that allows the network manager to reserve a number of trunks for a desired type of traffic. Two adjustable "reservation levels" (RL1 and RL2) are defined for this control and the number of trunks reserved can vary from 0 to 15. When the number of idle outgoing trunks is less than or equal to RL1, then a pre-selected control affects calls on the trunk group until the number of idle trunks exceeds RL1. This same scheme is used for RL2 but the control is generally more severe. In setting up trunk reservation on a trunk group, the network manager selects the following options:

- Reservation Levels (RL1 and RL2)
- Response Category (A through E)
- Control Action (skip or cancel)

Refer to GR-477-CORE, Section 4.3.2, for a detailed description of TRE.

5.2.8.7.1.3 Selective Incoming Load Controls

[Required: TS, EOS, MFS – Conditional: SMEO, DVX-C, DVX-L] Selective Incoming Load Controls is a control that, when activated on a trunk group, causes the incoming calls on that trunk group to be ignored by the receiving switch or sent to a disposition. SILC is intended as a substitute for ACC; therefore, it would only be used by switches that are not using SS7 signaling. This control allows a network manager to select trunk groups to be controlled in an office when the office itself (not one connected to it) encounters congestion levels 1 and 2. Activation is intended to occur at the same time that ACC signals are being transmitted from the office. The inhibiting of the transmission of ACC signals will also inhibit the activation of SILC. The percentages or gap rates for each congestion level are either generically defined or they can be modified via a recent change message in the network switching center. The network manager also has the option of putting up to 128 trunk groups on the SILC list for activation in congestion level.

Refer to GR-477-CORE, Section 5.3.4, for a detailed description of SILC.

5.2.8.7.1.4 Precedence Access Threshold

[Conditional: MFS] The PAT control limits the number of simultaneous calls originated by selected user stations, attendant positions, and other designated switch terminations whose traffic input into the DSN requires screening. Each precedence access threshold will set an upper limit

on the number of simultaneous calls that are allowed to enter the DSN by precedence level and calling area. There will be separate precedence access threshold settings established for each combination of precedence level and calling area. This control will allow five precedence levels (i.e., ROUTINE, PRIORITY, IMMEDIATE, FLASH, and FLASH OVERRIDE) and five progressively wider calling areas (A1, A2, A3, A4, and A5). Additional requirements and a detailed description of PAT can be found in UCR 2008, Section 5.2.1.11.1, Precedence Access Threshold.

5.2.8.7.2 Overload Controls

5.2.8.7.2.1 Essential Service Protection

[Required: TS, EOS, MFS – Conditional: SMEO, DVX-C, DVX-L] A DSN switch shall be capable of giving preference for originating service to a limited number of stations during emergencies. This feature is aimed at ensuring that a small number of lines designated as "essential" by the government receive priority originating service during periods of extreme overloads. Service to other lines should be equitably distributed when Essential Service Protection (ESP) is activated. The ESP feature is manually enabled and disabled. Essential Service Protection is automatically activated, if previously enabled, when the system detects that service has been significantly degraded. The switch shall return to normal processing when the original condition returns to a normal condition. Each switch shall have the capability to classmark up to 15 percent of the station lines for this service.

Refer to GR-741-CORE, Section 3.5.4.2.D.2, for a description of ESP.

5.2.8.7.3 Manual Controls

[Required: TS, EOS, MFS – Conditional: SMEO, DVX-C, DVX-L] Manual network management controls are those controls that are implemented by the personnel at a Network Management Center (NMC). Manual controls supplement the automatic controls, and they are used to handle the network problems that require flexibility and human judgment. Often the network manager uses manual controls to utilize less congested areas of the network to relieve the pressure in overloaded sections and fully utilize the capacity of the network. Two types of manual controls are protective and expansive. Protective controls can be used to inhibit the spread of congestion in the network by restricting normal trunk group access and overflow (trunk group controls) or by limiting the attempts on selected destination or signaling codes (code controls). Expansive controls are used to expand routing beyond the normal in-chain routes when in-chain routes are busy or have failed and there exists idle capacity in out-of-chain routes. If the characteristics of the particular call meet the criteria for the type of traffic to be affected, it will be subjected to the control. For trunk group controls, preselections are made from the route options listed below. The route options involve trunk groups, and since code controls affect a

call before it is offered to a trunk group, route options are irrelevant to code controls. The following options listed below are traffic characteristic options that can be preselected.

5.2.8.7.3.1 Trunk Group Controls

[Required: TS, EOS, MFS – Conditional: SMEO, DVX-C, DVX-L] The DSN switching elements require both protective and expansive manual trunk group (TG) controls. The protective controls (CANF, CANT, and SKIP) are those that block traffic from using a trunk group, while expansive controls (Reroute (RR)) allow other ways for traffic to complete via identified trunk groups. *The application of any TG control shall not prevent precedence calls from performing a preemptive search on all of the TG's that were previously friendly searched.* The options on the protective controls include independent direct routed and alternate routed percentages (not by gap rates) and announcement selection (NCA, EA1, or EA2 for CANF, and CANT). The disposition of calls controlled by SKIP is to the next in-chain trunk group or to NCA if the controlled trunk group is a final group. The expansive trunk group control (i.e., RR) extends call routing to trunk groups beyond the normal call routing hierarchy in those cases where the original route has congestion or fails, and spare call capacity exists on the receiving trunk group.

5.2.8.7.3.1.1 Cancel From

[Required: TS, EOS, MFS – Conditional: SMEO, DVX-C, DVX-L] Cancel From (CANF) is a protective, post hunt trunk group control. The main function of this control is to cancel traffic overflowing from a TG to the next in control only if the characteristics of the call meet the options that have been preselected for CANF. FLASH and FLASH OVERRIDE calls shall be exempted from this control.

Refer to GR-477-CORE, R6-9, for a detailed description of CANF.

5.2.8.7.3.1.2 Cancel To

[Required: TS, EOS, MFS – Conditional: SMEO, DVX-C, DVX-L] Cancel To (CANT) is a protective, prehunt trunk group control that cancels the affected traffic offered to a TG. A call is affected by this control only if the characteristics of the call meet the options that have been preselected by the network controller. FLASH and FLASH OVERRIDE calls shall be exempted from this control.

Refer to GR-477-CORE, R6-9, for a detailed description of CANT.

5.2.8.7.3.1.3 SKIP

[Required: TS, EOS, MFS – Conditional: SMEO, DVX-C, DVX-L] SKIP is a prehunt TG control that causes the affected traffic to skip over the TG that the control is applied to and to attempt to find a trunk in the remaining route sequence. The next alternative routed TG does not necessarily have to be the next in chain TG in the route advance. It could be an out-of-chain TG that is substituted for the TG that was skipped. A call is affected by this control only if the characteristics of the call meet the options that have been preselected for the SKIP control.

Refer to GR-477-CORE, R6-9, for a detailed description of SKIP.

5.2.8.7.3.1.4 Reroute

[Required: TS, EOS, MFS – Conditional: SMEO, DVX-C, DVX-L] Reroute is a TG control that can either be an expansive pre hunt TG control or an expansive post hunt TG control. Normally, it is used as an expansive post hunt TG control. Use of the RR Control restricts offered calls from those routes known to be congested or failed, and provides substitute routes that have a higher probability of call completion. The requirements for RR Control are given in GR-477-CORE. When activating an RR Control, the Network Manager can choose between the single-via or multiple-via control types.

Refer to GR-477-CORE, O6-11 .B, for a detailed description of RR.

5.2.8.7.3.1.4.1 Single-Via Reroute

[Required: TS, EOS, MFS – Conditional: SMEO, DVX-C, DVX-L] A single-via or regular RR Control explanation must begin with an originating office designated “A,” and a destination office designated “B,” which are connected by a trunk group labeled “AB.” In normal operation, calls that cannot be handled by trunk group AB are route-advanced to other trunk groups for completion in a predefined sequence known as a “Route Advance Chain.”

Calls that cannot be handled by any of the chained trunk groups will be routed to a final treatment trunk group, which is usually an announcement. To implement an RR Control, there must be another NSE trunk group designated “via,” which has the ability to route calls to destination B, but does not normally do so. (NOTE: Trunk group “via”is not required to have a direct link to office B, just the means to route calls to B.) Assuming that a RR Control is issued, if the call cannot be handled by trunk group AB, it is then offered to the via trunk group for completion. If the controlled call overflows the “A” to the “via” trunk group, it is offered to the next route in the normal chain. This is normally the first route advance if the call offered to trunk group AB is overflowed from AB and no controls are in effect. In other words, single-via-rerouting is the insertion of an out-of-chain route (trunk group) into the normal routing chain

during the control period. There is no separate limit on the number of single-via RR Controls that may be active in a switch at any one time. However, all RR Controls are counted toward the maximum limit of 128 active Manual TG Controls.

5.2.8.7.3.1.4.2 Multiple-Via Reroute

[Required: TS, EOS, MFS – Conditional: SMEO, DVX-C, DVX-L] In cases where a single trunk group (called "via," in the above example) cannot handle all of the originating A to destination B traffic, up to seven trunk groups, each having means to route traffic to B, may be used. This capability is called "Multiple-via Reroute." An overflowed call from trunk group AB is offered in succession to all designated "via," trunk groups until it is handled. If none can carry the call, it is then offered to the next route in the normal chain. If the call is handled by a "via," trunk group, the next call to destination B is offered to the "via," trunk group following the one that handled the previous call. There is a separate limit of 16 multiple-via RR Controls, each having a maximum of seven via-routes per switch, all of which contribute to the limit of 128 Manual TG Controls. The term "ordered hunt" refers to traversing the multiple-via routing patterns described above. For each of the two control types, single-via or multiple-via, the following are additional options associated with the RR Control.

5.2.8.7.3.1.4.3 Overflow Versus Immediate Reroute

[Required: TS, EOS, MFS – Conditional: SMEO, DVX-C, DVX-L] The Overflow Reroute (ORR) option modifies the normal trunk group route advance hierarchy (in-chain) by inserting another trunk group (out-of-chain) into the call routing pattern. The Immediate Reroute (IRR) option provides for traffic to be rerouted before the calls are offered to a particular trunk group. If the IRR option is not specified in the "Reroute Control Request" the ORR option will be enabled by default. Any attempt to apply both ORR and IRR options to the same RR Control will have the effect of replacing the existing option (ORR/IRR) with the most recently specified option (ORR/IRR). That is, the option specified in the original command will be replaced by the option specified in the later command.

5.2.8.7.3.2 Code Controls

[Required: TS, EOS, MFS – Conditional: SMEO, DVX-C, DVX-L] Call gap code control is a manual protective control. The call gap control governs the maximum rate of attempts to a particular code, over a period of time, out of the office in which the control is implemented. This code control provides call gapping capabilities on destination codes of 3 to 10 digits. Options for these code controls include a selection of gap interval, a call disposition (EA1, EA2, NCA), and a switching domain. FLASH and FLASH OVERRIDE calls shall be exempted from this control.

5.2.8.7.3.2.1 Code Controls – Code Gapping Controls

[Required: TS, EOS, MFS – Conditional: SMEO, DVX-C, DVX-L] Manual Code Controls are Protective Controls that restrict calls having code prefixes for destinations that have been temporarily designated as difficult or impossible to complete.

The code prefixes may be Destination Codes (NPA, Service Access Code (SAC), etc.), 7-Digit Line Number (KXX-XXXX), or a combination of them. Using this type of control allows available network resources to handle traffic to other destinations that has a better probability of completion. Code Controls are most effective for controlling "focused overloads," which are characterized by a surge of traffic from many locations within the network to a single office or destination code. This interface supports the "code-gapping" method of code control. A code-gapping control is applied by specifying the code combination, i.e., NPA, NPA + KXX, etc., and the maximum rate at which calls are forwarded. Thus, the number of offered calls to a given destination is independent of the calling rate. For example, assume that calls to a particular area code (NPA) are to be restricted. The Network Manager has the ability to allow calls with the designated NPA prefix to be offered to a destination route at a rate ranging from 6 per minute to 12 per hour. The rate at which the calls are offered for completion is independent of the number of calls generated with the NPA prefix. This code-gapping technique provides a greater call completion precision than do other non-supported methods such as "percentage blocking."

GR-477-CORE and GR-690-CORE contain the detailed requirements for Code Controls. A maximum of 64 Code Controls may be active in the NSE at any one time. The Code Control feature should allow the Network Manager to control calls all destination codes in his or connected networks

5.2.8.7.3.3 Total Office Manual Control Removal – Request/Response

[Required: TS, EOS, MFS – Conditional: SMEO, DVX-C, DVX-L] All total office controls are manual. All CANT, CANF, SKIP, or RR controls can be removed as a group on a total office basis. Code controls can also be removed on a total office basis. The capability to remove "ALL" manual controls in the entire office also exists. These commands will not remove the automatic control overrides. However, the ACC transmit/SILC override (inhibit) control can only be implemented or removed on a total office basis.

Refer to GR-747-CORE, Section 3.2.1.2 C. for a detailed description of this feature.

5.2.8.7.4 Treatment Options of Calls Terminated

[Required: TS, EOS, MFS – Conditional: SMEO, DVX-C, DVX-L] The following paragraphs describe how the termination of precedence level and ROUTINE precedence calls will be handled based on the treatment they are given. The no circuits announcement (NCA), emergency announcement 1 (EA1), and emergency announcement 2 (EA2), are prerecorded announcement options that are selected by the network management controller. Since the control, RR, is a control that allows the switch to search additional TGs outside of the in-chain sequence, RR would not cause a call to be terminated. However, some controls mentioned in this section would cause a call to be terminated because they either prevent calls from accessing or overflowing a TG or in the case of code controls, such as Code Block, they prevent calls from reaching a specified code. If a precedence level call would normally be given reorder treatment, it shall be deflected to a BPA. If a precedence level call would normally be given no circuit treatment, it shall be deflected to a BPA.

If a ROUTINE precedence call is given reorder treatment, the call shall be given 120 impulses per minute. If a ROUTINE precedence call is given no circuit treatment, it shall be given a No Circuit Announcement (NCA) if the prerecorded option is available. If the announcement is not available, the defaulting treatment is for the call to be given a 120 impulses per minute. If a ROUTINE precedence call is given emergency treatment, it shall be given either an EA1 or an EA2.

5.2.8.8 Remote Access to Switch

[Required: TS, EOS, SMEO, DVX-C, DVX-L, MFS] The DSN switching system shall be able to receive remote commands. These switch commands must be received through the switch access channel. The user interface to input these commands may be at a switch command prompt or via a switch provided user interface (e.g. graphical user interface (GUI), text screen). The DSN switching system shall be able to receive remote commands for configuring the network related entries within the switch.

5.2.9 Integrated Services Digital Network

5.2.9.1 ISDN Overview

ISDN is a digital network technology capable of providing a wide variety of user applications. National ISDN is the Telcordia Technologies recommended implementation of ISDN to provide customer access to multiple services over a set of uniform interfaces.

The first step of National ISDN-1 (NI-1) was the initial deployment of National ISDN in 1992 and addressed the Basic Rate Interface (BRI). The second step of National ISDN-2 (NI-2) which

expanded the BRI interface requirements and added Primary Rate Interface (PRI) requirements was introduced in 1993. NI-3 introduced an additional set of services for addressing "mass market" and other market needs.

DSN ISDN generic requirements are based on Telcordia Technologies National ISDN documentation summarized in Telcordia Technologies Special Report, SR-3476, Issue 1, *National ISDN 1995 and 1996*, June 1995. SR-3476 lists the features and functions NI-1 and NI-2.

5.2.9.2 DSN Generic ISDN Features and Interface Descriptions

DSN switching systems shall provide the ISDN BRI, PRI, and Packet Data capabilities shown in Tables 5.2.9-1 through 5.2.9-6. Tables 3-1 through 3-6 of Telcordia Technologies SR-3476 provide the specific requirements for features and capabilities listed in UCR 2008, Tables 5.2.9-1 through 5.2.9-6. The MLPP interactions with ISDN are identified in Section 5.2.2, Multilevel Precedence and Preemption.

Table 5.2.9-1. BRI Access, Call Control, and Signaling

TS	MFS	EOS	SMEO	PBX1	PBX2	DVX-C	DVX-L	FEATURE OR CAPABILITY
	R	R	R	C	C	C	N/A	ISDN BRI Layer 1
	R	R	R	C	C	C	N/A	4:1 Time Division Multiplex Method for ISDN Basic Access
	R	R	R	C	C	C	N/A	ISDN BRI Layer 2
	R	R	R	C	C	C	N/A	BRI Circuit-Mode Call Control Basic Call Control
	R	R	R	C	C	C	N/A	BRI Terminal initialization
	R	R	R	C	C	C	N/A	Service Profile Identifier
	R	R	R	C	C	C	N/A	Parameter Downloading
	R	R	R	C	C	C	N/A	Default Services for Terminals
	R	R	C	C	C	C	N/A	BRI Interworking with SS7
	R	R	R	C	C	C	N/A	ISDN BRI Packet User Originated, On-Demand B-Channel Packet Conditional Notification

LEGEND
R = REQUIRED: feature/function required in a candidate switch. Must adhere to the specific UCR requirements
C = CONDITIONAL: feature/function is optional. However, if the feature/function is provided, it must adhere to the specific UCR requirements.
N/A = NOT APPLICABLE

Table 5.2.9-2. Uniform Interface Configurations for BRIs

TS	MFS	EOS	SMEO	PBX1	PBX2	DVX	FEATURE OR CAPABILITY
	R	R	R	C	C	C	Uniform Interface Configs. for BRIs. Single User with Multiple Applications Two Users Sharing a BRI
	R	R	R	C	C	C	More than 2 B-Channel Terminals on a BRI (Passive Bus)
	R	R	R	C	C	C	Associated Group Indicator
	R	R	R	C	C	C	DN Sharing over Multiple Call Types on an Integrated Terminal
	R	R	R	C	C	C	Non-Initializing Terminals

LEGEND
R = REQUIRED: feature/function required in a candidate switch. Must adhere to the specific UCR requirements
C = CONDITIONAL: feature/function is optional. However, if the feature/function is provided, it must adhere to the specific UCR requirements.

Table 5.2.9-3. BRI Features

TS	MFS	EOS	SMEO	PBX1	PBX2	DVX	FEATURE OR CAPABILITY
	C	C	C	C	C	C	Electronic Key Telephone Systems Multiple DNs per Terminal Analog Member of an EKTS Group Multiple DN Appearances per Call Appearance Call Handling Hold/Retrieve Bridging/DN-Bridging Intercom Calling Membership in a Multiline Hunt Group Abbreviated and Delayed Ringing Automatic and/or Manual Bridged Call Exclusion
	C	C	C	C	C	C	Call Forwarding
	C	C	C	C	C	C	Call Forwarding Variable Courtesy Call Reminder Notification Call Forwarding Interface Busy Call Forwarding Don’t Answer Call Forwarding Intragroup Only Call Forwarding Interface Busy Incoming Only Call Forwarding Don’t Answer Incoming Only
	C	C	C	C	C	C	ISDN Call Hold Hold and Retrieve
	C	C	C	C	C	C	Flexible Calling Three-Way and Six-Way Calling Consultation Hold

TS	MFS	EOS	SMEO	PBX1	PBX2	DVX	FEATURE OR CAPABILITY
							Conference Hold and Retrieve
	C	C	C	C	C	C	ISDN Display Service Protocol and Procedures Uniform Text (for NI-2 Uniform Services)
	C	C	C	C	C	C	Basic Business Group Denied Originating Denied Terminating Distinctive Alerting Indication
	C	C	C	C	C	C	Business Group Dial Access Features
	C	C	C	C	C	C	Dial Access to Automatic Flexible Routing
	C	C	C	C	C	C	Customer Access Treatment Code Restriction
	C	C	C	C	C	C	Code Restriction and Diversion
	C	C	C	C	C	C	Direct Outward Dialing
	C	C	C	C	C	C	Direct Inward Dialing
	C	C	C	C	C	C	ISDN Call Pickup
	C	C	C	C	C	C	ISDN Directed Call Pickup
	C	C	C	C	C	C	Access To Analog Attendant Access Station Message Detail Recording Tracing of Terminating Calls Tandem Call Tracing Trace of a Call In Progress Bulk Calling Line Identification Selective Call Acceptance Selective Call Forwarding Selective Call Rejection
	C	C	C	C	C	C	Limitations and Restrictions for 911 PSAP – Call Hold Not Allowed for a 911 Call

LEGEND
R = REQUIRED: feature/function required in a candidate switch. Must adhere to the specific UCR requirements
C = CONDITIONAL: feature/function is optional. However, if the feature/function is provided, it must adhere to the specific UCR requirements

Table 5.2.9-4. PRI Access, Call Control, and Signaling

TS	MFS	EOS	SMEO	PBX1	PBX2	DVX	FEATURE OR CAPABILITY
R	R	R	R	R	C	R	PRI Layer 1
R	R	R	R	R	C	R	PRI Layer 2 (Circuit)
R	R	R	R	R	C	R	PRI Call Control and Signaling
R	R	R	R	R	C	C	Basic Call Control for Circuit Mode Calls
R	R	R	R	R	C	C	Multiple DS1 Facilities Controlled by a Single D-Channel
R	R	R	R	R	C	C	Access to Selected Primary Rate Services on a Per-Call Basis
R	R	R	C	C	C	C	PRI Interworking with SS7
R	R	R	R	R	C	C	PRI Packet-Mode Call Control

Table 5.2.9-5. PRI Features

TS	MFS	EOS	SMEO	PBX1	PBX2	DVX	FEATURE OR CAPABILITY
R	R	R	R	R	C	C	Call-by-Call Service Selection FX Non-ISDN Tie IN WATS OUT WATS Non-ISDN ETN
R	R	R	R	R	C	C	Interworking with Private Networks

LEGEND
R = REQUIRED: feature/function required in a candidate switch. Must adhere to the specific UCR requirements
C = CONDITIONAL: feature/function is optional. However, if the feature/function is provided, it must adhere to the specific UCR requirements.

Table 5.2.9-6. Packet Data Features and Capabilities

TS	MFS	EOS	SME O	PBX 1	PBX2	DVX	FEATURE OR CAPABILITY
C	C	C	C	C	C	C	PPSN Call Control and Features - X.25 Features Closed User Groups (CUG),CUG Outgoing Access, CUG Incoming Access Recognized Private Operating Administration (RPOA) CCITT DTE Facilities
C	C	C	C	C	C	C	
C	C	C	C	C	C	C	
C	C	C	C	C	C	C	
C	C	C	C	C	C	C	PPSN Call Control and Features X.75 and X.75' Utility Support All X.75 Utilities in Minimal Subset Multilink Procedures on X.75/X.75'
C	C	C	C	C	C	C	
C	C	C	C	C	C	C	
C	C	C	C	C	C	C	

TS	MFS	EOS	SME O	PBX 1	PBX2	DVX	FEATURE OR CAPABILITY
							Support of X.75 End Office Connections Selective Support of X.75' Utilities
C	C	C	C	C	C	C	X.75 Utilities on X.75' Access Characteristics
C	C	C	C	C	C	C	X.75 Interface Identifier Clearing Subnetwork Identification Transit Sub-network Count
C	C	C	C	C	C	C	Packet Numbering and Routing
C	C	C	C	C	C	C	Packet Mode Data Routing & Digit
C	C	C	C	C	C	C	Analysis Requirements Numbering Plan Interworking per TR-448 and TR-301.
C	C	C	C	C	C	C	User-to-User with Call Control (Packet)
C	C	C	C	C	C	C	Fast Select, Fast Select Acceptance
C	C	C	C	C	C	C	16 Octets of data in call request
C	C	C	C	C	C	C	ISDN X.25 Supplementary Services
C	C	C	C	C	C	C	One-Way Logical Channel
C	C	C	C	C	C	C	Outgoing/Incoming
C	C	C	C	C	C	C	Incoming/Outgoing Calls Barred
C	C	C	C	C	C	C	Default Throughput Class Alignment
C	C	C	C	C	C	C	Nonstandard Default Packet Sizes
C	C	C	C	C	C	C	Nonstandard Default Window Sizes
C	C	C	C	C	C	C	Flow Control Parameter Negotiation
C	C	C	C	C	C	C	Throughput Class Negotiation Transit Delay
C	C	C	C	C	C	C	User Testing
C	C	C	C	C	C	C	Multiline Hunt Group
C	C	C	C	C	C	C	Linear and/or Circular Hunting
C	C	C	C	C	C	C	Assignment of Non-Hunt DN to Hunt Terminals
C	C	C	C	C	C	C	ISDN Calling Number Identification Services
C	C	C	C	C	C	C	Inband Calling Number ID for Packet
C	C	C	C	C	C	C	Basic Business Group Inclusion of Packet In BBG Inclusion of Packet in Business Group Dialing Plan

LEGEND
R = REQUIRED: feature/function required in a candidate switch. Must adhere to the specific UCR requirements.
C = CONDITIONAL: feature/function is optional. However, if the feature/function is provided, it must adhere to the specific UCR requirements.

5.2.10 Synchronization

The use of digital switching systems directly interconnected with digital transmission facilities as an integral part of the DSN requires the use of techniques for synchronizing clock rates. The term synchronization refers to an arrangement for operating digital switching systems at a common (or uniform) clock rate whereby the data signal is accompanied by a phase-related clock. Improperly synchronized clock rates result in the loss of portions of the bit streams and a concomitant loss of information. The DISN Timing and Synchronization (T&S) subsystem utilizes Navigation Satellite Timing and Ranging (NAVSTAR) Global Positioning System (GPS) transmissions from which a precise frequency is derived. This precise frequency timing signal is phase related (referenced) to Universal Time Coordinated (UTC). The T&S subsystem frequency multiplier accepts precise frequency signals from primary source or, in case of failure, switches to an alternate source provided by atomic clocks, e.g., cesium beam or rubidium, if available. The Clock Distribution System disseminates timing through the equipment hierarchy. DSN switches may also receive system timing via digital transmission facilities to locations having direct access to (synchronized to) the timing sources already described. This chapter provides the requirements for network synchronization within the DSN.

5.2.10.1 Timing Modes

[Required: TS, EOS, MFS – Conditional: SMEO, DVX-C, DVX-L, PBX1] DSN switching systems shall meet the external timing mode requirements specified in the Telcordia GR-518-CORE, Paragraph 18.1. Most SMEOs and PBX1s will only support line timing.

5.2.10.1.1 External Timing Mode

5.2.10.1.1.1 External Timing Mode

[Required: TS, EOS, MFS – Conditional: SMEO, DVX-C, DVX-L] The switch shall support external timing modes as defined in Telcordia Technologies TR-NWT-001244.

5.2.10.1.1.2 Line Timing Mode

[Required: TS, EOS, SMEO, DVX-C, DVX-L, MFS, PBX1] The switch shall support line timing modes as defined in Telcordia Technologies TR-NW-001244.

5.2.10.1.2 Internal Clock Requirements

5.2.10.1.2.1 General

[Required: TS, EOS, MFS – Conditional: SMEO, DVX-C, DVX-L] The switch shall provide internal clock requirements as described in the Telcordia Technologies GR-518-CORE, Paragraph 18.2.

5.2.10.1.2.2 Stratum 4 Clock

[Required: SMEO, DVX-C, DVX-L , PBX1, PBX2] The switch shall provide a stratum 4 or better internal clock.

5.2.10.2 Synchronization Performance Monitoring Criteria

[Required: TS, EOS, MFS – Conditional: SMEO, DVX-C, DVX-L, PBX1, PBX2] The switch shall meet the synchronization performance monitoring criteria as described in the Telcordia Technologies GR-518-CORE, Paragraph 18.3.

5.2.10.3 DS1 Traffic Interfaces

[Required: TS, EOS, MFS – Conditional: SMEO, DVX-C, DVX-L, PBX1, PBX2] The switch shall meet the DS 1 Traffic Interfaces as described in the Telcordia Technologies GR-518-CORE, Paragraph 18.4.

5.2.10.4 DS0 Traffic Interconnects

[Required: TS, EOS, MFS – Conditional: SMEO, DVX-C, DVX-L, PBX1, PBX2] The switch shall meet the DS0 Traffic Interconnects as described in the Telcordia Technologies GR-518-CORE, Paragraph 18.5.

5.2.11 Reliability

5.2.11.1 Reliability Requirements

[Required: TS, MFS, EOS, SMEO – Conditional: DVX-C, DVX-L] The DSN shall meet the reliability requirements in Telcordia Technologies GR-512-CORE, Section 12; and GR-474-CORE.

5.2.11.2 System Availability

[Required: PBX1] The DSN shall meet a system availability of 0.99997. Detailed requirements are listed below. The explanation and format for these requirements are contained in Telcordia Technologies GR-512-CORE, Section 12, and Sections 1 through 5. However, the values of the below requirements have been changed from the Generic Requirement to reflect a judged reduced reliability requirement for a PBX. Also, those Termination and Capability Types specified in the Generic Requirement, but not applicable to the DSN have been deleted:

5.2.11.2.1 Vendor Reliability Model

The supplier shall provide a reliability model for the system showing all calculations and stating all assumptions.

5.2.11.2.2 Hardware Failure Detection

The system shall be able to correctly detect, reconfigure, isolate, diagnose, and report the location of virtually all single hardware failures.

5.2.11.2.3 Individual Termination Downtime

Predicted Individual Termination Downtimes shall not exceed the values in Table 5.2.11-1.

Table 5.2.11-1. Individual Termination Downtimes

TERMINATION TYPE	REQUIREMENT
Analog Line	120 minutes/year
Analog Trunk	120 minutes/year
Digital Trunk	80 minutes/year
Accumulated B-Channel Circuit (BRA and PRA)	80 minutes/year

5.2.11.2.4 Predicted Multi-Termination Downtime

Multitermination referes to any switching interface/termination unit that handles 2-W line (analog or digital), 2-W trunk (analog or digital), and 4-W trunk (analog or digital)

Predicted Multitermination Downtimes shall not exceed values in Table 5.2.11-2.

Table 5.2.11-2. Predicted Multitermination Downtime

TERMINATION TYPE	REQUIREMENT
Analog Trunk	10 minutes/year
Digital Trunk	10 minutes/year
Analog Line	10 minutes/year
ISDN Circuit Switching	10 minutes/year

5.2.11.2.5 Predicted Total Capability Downtime

Predicted Total Capability Downtimes shall not exceed the values in Table 5.2.11-3.

Table 5.2.11-3. Predicted Total Capability Downtime

CAPABILITY TYPE	REQUIREMENT
Analog Line	3 minutes/year
ISDN Circuit Switching	3 minutes/year

5.2.11.2.6 Hardware Cutoff Call Rate

Predicted Hardware Cutoff Call Rates shall not exceed the values in Table 5.2.11-4.

Table 5.2.11-4. Hardware Cutoff Call Rates

TERMINATION TYPE	REQUIREMENT
Analog Line	100,000 cutoffs per 10^9 hours of call duration
Analog Trunk	100,000 cutoffs per 10^9 hours of call duration
Digital Trunk	67,000 cutoffs per 10^9 hours of call duration
Accumulated B-Channel Circuit Mode	67,000 cutoffs per 10^9 hours of call duration

5.2.11.2.7 Operations System Interface Downtime

Predicted Operations System Interface Downtime shall not exceed 120 minutes/year.

5.2.11.2.8 Capability Downtime

Predicted Capability Downtimes shall not exceed the values in Table 5.2.11-5.

Table 5.2.11-5. Capability Downtimes

CAPABILITY TYPE	REQUIREMENT
Control	3 minutes/year
Visibility or Diagnostic Capability	3 minutes/year

5.2.11.3 Backup Power

[Required: TS, MFS, EOS, SMEO, PBX1] The DSN shall have back-up power to maintain continuous operation whenever the primary source of power is disrupted. Back-up power design and implementation shall be incorporated into the DSN design to assure the DSN meets the reliability requirements of UCR 2008, Section 5.2.11, Reliability. General power requirements are described in Telcordia Technologies GR-513-CORE. The reliability requirements in UCR 2008, Section 5.2.11 have little if any allocation for power related down time. Following the risk avoidance guidance in Telcordia Technologies GR-513-CORE the back-up power design shall minimize the probability of a complete loss of switch power.

NOTE: In the CONUS the commercial carriers, following the guidance in the LSSGR, have made a practice of implementing back-up power with a combination of battery power systems, auto start generators with at least 72 hours of fuel reserve and fuel replenishment plans, and alarm systems.

5.2.11.3.1 Power Components

[Required: TS, MFS, EOS, SMEO, PBX1] The current uninterruptible power systems (UPS) used in the DSN are comprised of three components. The first component is a battery. The second component is an engine-operated generator. The third component is an alarm system. A combination of current and other technologies in power storage and generation may be used in the implemented power design. The design goal is a power system that shall support continuous operation whenever the primary source of power is disrupted.

5.2.11.3.2 UPS Requirements

[Required: TS, MFS, EOS, SMEO, PBX1] The requirements for UPS below are bare minimum requirements and may not assure the design goal of continuous operation is attained. The requirements below should be increased following the guidance in GR-513-CORE to meet site operational requirements and extenuating characteristics of the application environment.

5.2.11.3.2.1 UPS Load Capacity

[Required: TS, MFS, EOS, SMEO] The UPS shall provide greater than 8 hours of mission busy hour current load requirements (rated in Ampere hours) plus at least 10% for DSN equipment to include switching, transport and ancillary equipments. Note: Although there is no specific requirement for UPS protection for environmental (Air handling, lighting etc.) systems, the provisions of UCR 2008, Section 5.2.11.3.3, Backup Power (Environmental), must be met.

5.2.11.3.2.2 UPS PBX1 Load Capacity

[Required: PBX1] The UPS shall provide greater than 2 hours of mission busy hour current load requirements (rated in Ampere hours) plus at least 10% for DSN equipment to include switching, transport and ancillary equipments. NOTE: Although there is no specific requirement for UPS protection for environmental (Air handling, lighting etc.) systems, the provisions of UCR 2008, Section 5.2.11.3.3, Backup Power (Environmental), must be met.

5.2.11.3.3 Backup Power (Environmental)

[Required: TS, MFS, EOS, SMEO, PBX1] The backup power system shall have the capacity to operate environmental systems required to sustain continuous operation of DSN equipment to include switching, transport, and ancillary equipments. Power to the environmental systems may not need to be continuous.

5.2.11.3.4 Alarms

[Required: TS, MFS, EOS, SMEO, PBX1] Power system alarms shall be generated to an attended monitoring location whenever there is a loss of power and shall remain until the power is restored. Power alarms shall remain active until the condition that activated the alarm is corrected.

5.2.12 Specific Circuit-Switched Peripherals

5.2.12.1 Echo Canceller Requirements

5.2.12.1.1 Background

This UCR section describes the requirements that must be met by all echo canceller (EC) devices for them to be certified and used in the DSN.

The requirements contained in this section are based on:

- DoD policy for voice networks that defines the DSN as being "an inter-base, nonsecure or secure DOD telecommunications system that provides telephone service, voice-band data, and dial-up VTC for end-to-end command use and DOD authorized C2 and non-C2 users in accordance with national security directives." The DoD further specifies, "The DSN achieves Assured Services through implementation of Military Unique Features (MUF) to support military C2 functions." such as MLPP and military NM. [DoDI 8100.3]

5.2.12.1.2 Purpose

The purpose of this section is to specify echo canceller requirements so they can be certified for use in the DSN. Echo cancellers are voice operated devices placed in the 4-wire portion of a circuit (which may be an individual circuit path or a path carrying a multiplexed signal) and are used for reducing the echo by subtracting an estimated echo from the circuit echo. In the DSN, echo cancellers are implemented in a split manner, with one on each of the two sides of a transmission path. A properly designed echo canceller does not degrade the bearer channel signal.

Echo cancellers are used to minimize echo in circuits containing hybrids that convert 4-wire to 2-wire connections. They compensate for the effect of high, end-to-end delay that results in unacceptable voice listening performance. In general, echo cancellers are needed on long terrestrial trunks and on all trunks routed via satellite. They mitigate echo mainly by estimating the voice signal's pattern, making a model of that pattern, storing it and subtracting it from the echo returning from the distant end, while leaving intact the information flow coming from the distant end. Echo cancellers may be implemented as standalone devices or integrated into the transmission interfaces of switches, or other network devices.

As a minimum, compliance to the policies and instruction given in this UCR 2008 to include the following requirements that are features and capabilities considered necessary for a particular switch type to support warfighter missions in the DoD will require certification prior to introduction into the DSN.

5.2.12.1.3 Applicability

This section applies to all echo cancellers procured or leased for installation in the DSN. In addition, this section applies to upgrades and new software loads for existing equipment.

The UCR 2008 is the governing requirements document that takes precedence over the explicit or implicit requirements of subsidiary or reference documents, standards, and specifications. In the event of conflict, the explicit requirements of the UCR take precedence over the explicit or implicit requirements of the LSSGR and Generic Requirements GR.

5.2.12.1.4 Definitions

Definitions of terms can be found in UCR 2008, Appendix A, Section A2, Glossary and Terminology Description.

5.2.12.1.5 Requirements

This section provides the requirements for echo control equipment in the DSN. All echo canceller devices are required to meet the following requirements.

5.2.12.1.5.1 Echo Canceller Functionality

[Required] The echo canceller shall meet the requirements of ITU-T Recommendation G.165, ITU-T Recommendation G.168, and Telcordia Technologies SR-2275, Section 7, "Transmission."

[Required] The echo canceller shall support at least 64 milliseconds (ms) echo tail length.

[Required] The Mean Opinion Score (MOS) technique, if applicable, and the perceptual evaluation of speech quality (PESQ) measurement, ITU-T Recommendation P.862 shall be used to assess the clarity of end-to-end voice circuits on which echo cancellers are installed. The voice quality shall have an MOS of 4.0 or better, as measured in accordance with DISR voice quality standards.

[Required] The echo canceller shall be able to determine when a new call is being established and apply echo cancellation in accordance with this section.

[Required] The echo canceller shall have, at a minimum, the following two operational states and they shall be settable by the network management system (see UCR 2008, Section 5.2.12.1.5.7, Device Management), local control interface, or front/back control panel on a per DS0 basis:

1. Normal. Echo cancellation will remain in the enabled state between calls and during calls unless it is disabled as defined in this section.

2. Forced Off. In this state the echo canceller shall not enable echo cancellation until the forced off state has been changed.

5.2.12.1.5.2 2100-Hertz EC Disabling Tone Capability

[Required] On a per-channel basis, a 2100 Hertz (Hz) disabling tone shall be recognized by the echo canceller, causing the echo canceller to disable, as specified in ITU-T Recommendation G.168.

[Required] Re-enabling the echo canceller, after the echo cancellation function has been disabled by the tone, it shall remain in a disabled state until one of the following events occurs.

1. No single-frequency sinusoid is present as defined in ITU-T Recommendation G.168, Section 7.

2. The end of the call is detected.

3. The end of data transmission is detected. This may be detected either by the lack of modem or fax tones on the channel, or by some proprietary method.

[Required] Echo cancellers shall be capable of determining when a channel is in use (i.e., a call is active on the channel) or not. This function shall not interfere in any manner with an active call.

[Required] The 2100 Hz disabling tone shall override all other control functions and shall disable echo cancellation for that particular call.

5.2.12.1.5.3 Echo Canceller Hardware

[Required] The echo canceller shall be able to be connected to either analog and/or digital transmission facilities.

[Conditional] Analog trunk interface shall be able to provide echo cancellation on a per-trunk basis.

[Conditional] Digital trunk interface shall be implemented on a digital basis without conversion to analog. The digital echo canceller shall treat all DS0 channels (PCM-24, PCM-30, or more for SONET) independently.

5.2.12.1.5.4 Echo Cancellation on PCM Circuits

[Required] The PCM-24 or PCM-30 interfaces shall be in accordance with the requirements in UCR 2008, Section 5.2.6, System Interfaces, as applicable for the interface.

[Required] When the bearer channel is used for 56 or 64 kilobits per second (kbps) digital data or submultiples of 64 kbps, the digital echo cancellers shall not cause a loss of bit integrity.
.
[Required] Echo cancellers inserted in a PCM-24 path utilizing channel-associated signaling (i.e., "robbed bit") shall have a selectable setting to exclude the signaling bits from the cancellation process.

[Required] The echo canceller shall be capable of performing echo cancellation for speech and audio bearer capability calls on the full 64 kbps signal.

[Required] Echo cancellers shall not interfere with the functionality of CCS7 continuity check tones.

5.2.12.1.5.5 External Echo Cancellers – Not Controlled

[Conditional] Echo cancellers that are placed on network facilities and are not controlled by a switch or adjunct controller shall be able to determine whether a new call is a voice or data call. For voice calls echo cancellation shall be enabled, and for data calls echo cancellation shall be disabled.

5.2.12.1.5.6 Integral Echo Cancellers – Controlled

[Conditional] Echo cancellers that are placed on network facilities and are controlled by a switch or adjunct controller shall enable or disable its echo cancellation capability based on input from the local switch or adjunct controller. The echo canceller shall receive this input via a direct connection to the switch's or adjunct controller's internal messaging pathways, or by using an external communications port. For voice calls, echo cancellation shall be enabled, and for data calls the echo cancellation shall be disabled.

5.2.12.1.5.7 Device Management

[Required] All echo canceller devices in the DSN will be monitored and managed by the Advanced DSN Integrated Management Support System (ADIMSS), as described in UCR 2008, Section 5.2.8, Network Management, Section 5.2.8.3, Fault Management, and Section 5.2.8.4, Configuration Management.

[Required] Echo cancellers shall be capable of performing a self-test diagnostic function on nonactive and active channels on a noninterference basis and report any failures to the assigned network management system.

[Conditional] If the echo canceller is not considered an integral part of the switch or larger functional entity, then a front or back panel and/or external console control capability shall be provided for local management.

[Required] The echo canceller shall program its echo cancellation capability based on input via a direct connection to the external communications port, or using the front/ back programming panel, or by switch datafill.

5.2.12.1.5.8 Reliability

[Required] The echo canceller reliability and availability shall conform to Section 5 of Telcordia Technologies Generic Requirements GR-512-CORE, as specified for individual devices. The vendor shall provide a reliability model for the system, showing all calculations along with how the overall availability will be met, if requested.

5.2.12.1.6 Echo Canceller Application Guidelines

This section describes the application of echo canceller devices in the DSN and provides information only (see Figure 5.2.12-1, Echo Canceller Applications in the DSN).

The need for echo control devices becomes apparent as the round trip delay of the facilities used totals more than 30 ms. An echo canceller is actually required at both ends of the PCM or analog transmission system when the round trip delay is greater than 20 ms. While round-trip delays of less than 30 ms are tolerable to normal telephonic speech and not perceived by the user as an echo condition, this quantity of delay results in a noticeable “hollowness” to the circuit, as though the caller were talking in a reverberant room or tunnel. If the DSN were only a fraction of its current size and complexity, individual trunks that cause the delay could be singled out and provided with echo control. Nevertheless, because of the complexity of all possible connections in a global switched network, the delay introduced by digital processing, and the physics of how an echo canceller functions, a different approach must be taken.

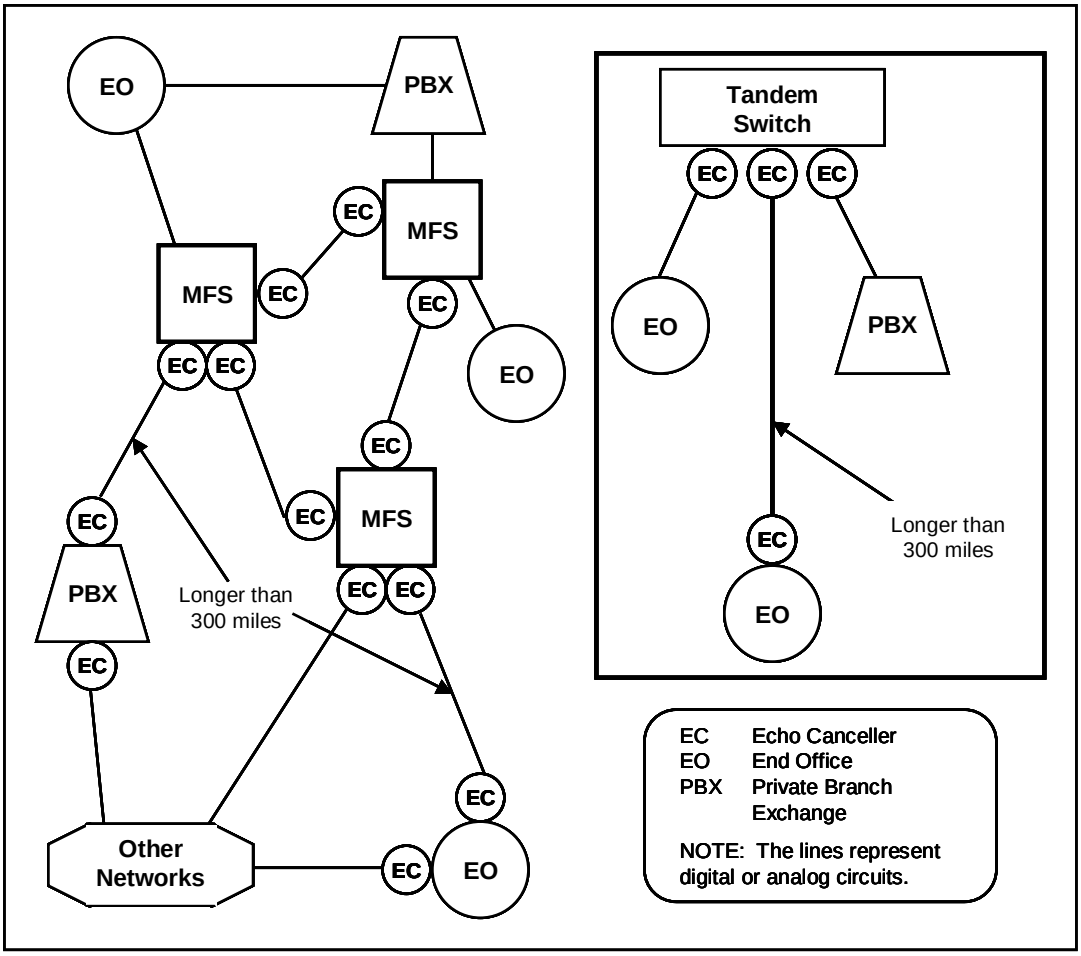


Figure 5.2.12-1. Echo Canceller Applications in the DSN

5.2.12.1.6.1 Echo Canceller Placement

Echo cancellers may be placed on the:

1. Multifunction switch end of all circuits interconnecting with MFSs or standalone switches (SAS). This configuration allows for the echo cancellation for calls terminating on the MFS or calls terminating at close-in (i.e., less than 300 miles distant) EO switches or PBXs.

    a. The tandem switch end of all circuits interconnecting EOs or PBXs with the SAS.

    b. Both ends of all circuits over 300 miles in length interconnecting or PBXs with MFSs or SASs.

c. The MFS/EO/PBX end of all circuits interconnecting with networks other than the DSN.

5.2.12.1.6.2 Additional Guidance

End office and PBX echo cancellers need minimum (typically 8 ms) end path delay capability. Each MFS configuration requires that the end path delay be computed for all subtending end offices and PBXs (other than those providing their own echo cancellers under the 300-mile rule). An end path delay capability greater than the highest end path delay figure (from the computations) will be standard for all echo cancellers on a particular MFS.

5.2.12.1.6.3 Exceptions

Best engineering judgment may be applied to echo canceller placement in special cases where numerous MFSs are in close proximity and the provisioning of echo cancellers on all MFS-to-MFS trunks is not cost effective. However, placing echo cancellers only on egress circuits to a DSN switch cluster or enclave increases the end path delay capability required for the "gateway" echo cancellers. The possibility of intraenclave circuit tandeming between the echo canceller and the furthest possible (in terms of delay) enclave hybrid complicates the determination of required end path delay capability. The added complexity is due to the numerous possible intra-enclave paths and the cumulative delay of a series of switches and multiplexers. If the longest (in terms of delay) possible end path delay route is not accurately identified, the end path delay capability calculated may be too small to effectively cancel echo for all possible circuit connections.

5.2.12.2 DSN Switch SONET Digital Trunk Interface

5.2.12.2.1 Background

This section describes the requirements that must be met by all switch SONET Digital Trunk Interface (SDTI) for them to be certified and used in the DSN.

The requirements contained in this section are based on:

- DoD policy for voice networks that defines the DSN as being "an interbase, nonsecure or secure DOD telecommunications system that provides dedicated telephone service, voice-band data, and dial-up VTC for end-to-end command use and DOD authorized C2 and non-C2 users in accordance with national security directives." The DoD further specifies "the DSN achieves Assured Services through implementation of Military Unique Features (MUFs) to support military C2 functions," such as MLPP and NM. [DoDI 8100.3]

5.2.12.2.2 Purpose

The purpose of this section is to specify the switch SDTI requirements so they can be certified for use in the DSN.

Switch digital trunk interfaces are used for bandwidth efficiency and utilization of higher density carrier systems and for reducing the need for individual DS1 switch termination hardware and software.

With the rapid growth of fiber optic transmission facilities, it has become appropriate to describe generic requirements for a high-capacity digital switch trunk interface. A high-capacity trunk interface on the digital switch that is compatible with SONET allows interconnection with SONET NEs. SONET defines Optical Carrier 3 (OC-3) signals and their equivalent electrical Synchronous Transport Signals (STS-N). These signals operate at a rate of N x 51.840 Mbps. The SONET digital switch trunk interface provides a direct termination of fiber optic transmission systems. The synchronous optical OC-3 (N x 51.84 Mbps) digital switch interface permits termination of N x 28 Virtual Tributaries (VT1.5s). The SONET digital switch trunk interface transmits an OC-3 (or STS-N signal) containing VT1.5s. These VT1.5s may terminate at another SDTI, or they may terminate on a SONET multiplex that outputs DS1 to an existing DS1 switch interface. SONET is a transmission network constructed as a progressive hierarchy of synchronously inter-leaved tributary signals.

The rapid growth in the deployment of transmission facilities at DS3 and higher rates provides motivation to seek efficient ways of handling these high-speed signals in the central office. A high capacity digital switch interface, such as the SDTI, will be integral to defining the future DSN network designs that are intended to make efficient use of transmission facilities and offer potential for new services. However, because the current, typical switch-to-switch cross-section is smaller than the capacity of an OC-1, additional transmission equipment such as a SONET Add-Drop Multiplexing (ADM) and Wideband Digital Cross-Connect System (WDCS) may be required to build up suitably sized bundles for the high-capacity switch termination. The value of N for an efficient high-capacity OC-3 signal termination on the SONET digital switch interface depends on the evolution of SONET. Also, different vendors may have different switching designs that may be optimized for different OC-3s. Because the current, typical switch-to-switch cross-section is smaller than the capacity of an OC-1, a high-capacity OC-N signal, with N greater than 3, may be under-utilized and inefficient to terminate on the digital switch.

5.2.12.2.3 Applicability

This section applies to all switch SDTIs procured or leased for installation in the DSN. All services, features and functions (both unique military and standard commercial) identified in this

UCR section are to be implemented in DSN SDTI. This requirement also applies to upgrades and new software loads for existing SDTI equipment.

This UCR 2008 section complies to the Telcordia Technologies GR-782-CORE, *SONET Digital Switch Trunk Interface Criteria,* A Module of TSGR, FR-440 and LSSGR, FR-64, Telcordia Technologies, GR-782-CORE for an OC-3 (or STS-N) interface to a DSS to be used in the DSN trunk networks. The typical SDTI functions are described as pertaining to the DSN intraoffice environment. The DSN intraoffice environment is viewed as a facility that contains at least one DSN center. Unless otherwise specified, it is assumed that the SDTI is in the intraoffice environment. An interoffice SONET digital switch trunk interface is optional. It is assumed that, most of the time, the SONET digital switch trunk interface will be connected to an ADM or WDCS in the same office, via an intraoffice connection. It is further assumed that the majority of the performance monitoring will be done within the transport network (i.e., at ADMs and WDCSs). Thus, for an intraoffice connection, the switch interface unit will not need to process several of the overhead bytes because they will have already been processed by an ADM or WDCS before the signal arrives at the switch. Therefore, this section takes into account two switch interface types: an intraoffice interface and an interoffice interface, where the latter processes the overhead as in the transport network. This document complements Telcordia Technologies GR-253-CORE, which describes the SONET signal hierarchy and formats, that includes common criteria for the SDTI and other SONET network elements. Therefore, common criteria are referenced in GR-253-CORE, and are not repeated in this section unless it is considered to be a part of the required MUF features and functionalities. The criteria for the interoffice switch interface comply with GR-253-CORE; however, the criteria for the intraoffice switch interface differ from GR-253-CORE because the switch interface is not addressed as a transport device. This section, which addresses the SONET interface for the trunk side of a digital switch, is distinct from Telcordia Technologies GR-303-CORE.

The UCR 2008 is the governing requirements document that takes precedence over the explicit or implicit requirements of subsidiary or reference documents, standards, and specifications. In the event of conflict, the explicit requirements of the UCR take precedence over the explicit or implicit requirements of the LSSGR and Generic Requirements.

5.2.12.2.4 Definitions

Definitions of terms can be found in UCR 2008, Appendix A, Section A2, Glossary and Terminology Description.

5.2.12.2.5 Requirements

This section provides the requirements for switch SDTIs in the DSN. All switch SDTIs are required to meet the below requirements.

5.2.12.2.5.1 Military Unique Features

[Required] The features and functions identified in this document shall support the full complement of MUFs to include Channel Associated Signaling (CAS), ISDN NI-1/2, and DSN backbone using CCS7.

5.2.12.2.5.2 Interface

[Required] The SONET interface shall be in compliance to Telcordia Technologies GR-303-CORE for an OC-3 interface between an Integrated Digital Loop Carrier (IDLC) system's remote digital terminal and the line side of a local digital switch.

[Required] The SONET interface shall meet the requirements of Telcordia Technologies GR-253-CORE and GR-782-CORE.

[Required] The criteria for the various SONET optical and electrical interfaces shall conform to GR-253-CORE. Such an interface shall also comply with Telcordia Technologies GR-303-CORE.

[Required] The SDTI shall, as a minimum, comply with ANSI T1.105-2001.

[Required] All features and functions that are defined in the UCR 2008 to operate at a DS1 rate shall work transparently at the VT1.5 rate over the SONET interface.

[Required] SONET digital interface shall support provisioning of transport levels as low as the DS1 rate for separately grouping of various categories of traffic such as voice, data, satellite, and terrestrial transmission.

[Required] The SONET digital switch trunk interface shall be capable of DS0 call processing and routing and shall route the DS0s within a VT1.5 in a way that presents the DS0s to the DSN for processing.

5.2.12.2.5.3 ROUTE Assignment

[Required] SDTI shall support "ROUTE" assignment of trunk group(s) at the OC-3 (highest) and down to DS0 (lowest) rates as defined in UCR 2008, Section 5.2.3.2, Primary and Alternate Routing, and shall support the signaling requirements as shown in Table 5.2-1.

5.2.12.2.5.4 Facility Alarms

[Required] SONET digital trunk interface shall provide maintenance signals that include the following failure states as defined in Telcordia Technologies GR-253-CORE for loss of signal, loss of frame, loss of pointer, and equipment failures.

- Line AIS
- Line RDI-L
- STS Path AIS
- STS path Yellow
- VT Path AIS
- VT path Yellow

Code processing is necessary for all applications for maintenance related activities.

[Required] SONET digital trunk interface shall conform to Telcordia Technologies GR-782-CORE, Section 7.2, for AIS and Yellow signal processing to include signal processing for rates as low as DS1.

[Required] SONET digital trunk interface shall process DS0 AIS and transmit DS0 RAI (Yellow) in accordance with Telcordia Technologies GR-253-CORE.

5.2.12.2.5.5 Synchronization

[Required] SDTI shall meet the common synchronization requirements specified in Telcordia Technologies GR-253-CORE, GR-518-CORE, and GR-436-CORE.

[Required] SDTI shall meet the Sinusoidal Jitter Tolerance requirements specified in Telcordia Technologies GR-253-CORE. The SDTI falls under Category II in GR-253-CORE.

[Required] SDTI shall meet the Jitter Generation requirements specified in Telcordia Technologies GR-253-CORE.

[Required] SDTI shall meet the generic Wander requirements per Telcordia Technologies GR-253-CORE, and shall be able to accommodate at least 10-µsec of wander over a 24-hour period (the maximum amount of wander expected to appear at these interfaces).

[Required] As defined in Telcordia Technologies GR-782-CORE, Section 6.6, the 24 DS0 (VT1.5) signals not using out-slot signaling shall have an all “zeros” idle code inserted into the appropriate signaling bit positions within the VT1.5 stream. A mixture of DSN CCS and out-slot

signaling may exist on a VT1 .5 basis in an OC-3 interface as DSN CCS evolves. Therefore, both DSN CCS and out-slot signaling are required.

5.2.12.2.5.6 Reliability

[Required] The SDTI shall meet the requirements contained in Telcordia Technologies GR-874-CORE, and the requirements for switching systems specified in TR-NWT-000284, *Reliability and Quality Switching Systems Generic Requirements (RQSSGR)*, Issue 2, October 1990. Additionally, the SDTI shall conform to the reliability objectives for switching systems, including integrated digital terminations, as specified in GR-512-CORE.

5.2.12.3 Customer Premises Equipment Requirements

5.2.12.3.1 Background

This section describes the requirements that must be met by all Customer Premise Equipment (CPE) for them to be certified and used in the DSN.

5.2.12.3.2 Purpose

The purpose for developing this Section is to specify the CPE requirements so they can be certified for use in the DSN.

5.2.12.3.3 Applicability

This section applies to all DSN CPEs identified below, procured or leased for installation in the DSN. All services, features and functions (both unique military and standard commercial) identified in this section and associated sections are to be implemented in DSN assets including switches, trunks, lines, and ancillary equipment. This requirement also applies to upgrades and new software loads for existing equipment.

The UCR 2008 is the governing requirements document that takes precedence over the explicit or implicit requirements of subsidiary or reference documents, standards, and specifications. In the event of conflict, the explicit requirements of the UCR take precedence over the explicit or implicit requirements of the LSSGR and Generic Requirements.

A wide variety of CPE manufactured and sold by many sources can be connected to the line/subscriber and/or carrier/network side of a DSN switching center. Such varieties include Industry “ANSI-ETSI STANDARDS” based digital and analog devices and non-STANDARDS based proprietary digital devices. The efficiency of such analog devices/equipment in converting an acoustic signal into an electric signal (and the reverse) is an important consideration in the

development of the DSN transmission plan. The efficiency of the analog or digital CPE equipment affects the quality, loudness, noise, and echo performance of the overall connection.

This section covers those devices that are connected to a DSN switch via a 2 wire analog, 2 wire digital, or 4 wire digital interface (as illustrated in Figure 5.2.12-2, Typical CPE Connections to the DSN) and that such devices are not required to have network management features/functionality. This covers devices such as answering machines, voice mail, automated call distributors, proprietary telephone sets, standards based telephone sets, facsimile machines, voice band modems, ISDN network termination 1 (NT1) devices and terminal adapters (TA), and certain devices that are deemed mandatory for local or host nation telecommunications network compliance (i.e., 911 Emergency Service).

The original interface requirement for a 911 Emergency Service system is typically an analog protocol that requires R2 signaling. Since the basic requirements of the UCR did not mandate the R2 signaling it is therefore not a DSN requirement for such a system that uses the R2 protocol. The DSN however supports such a system via the ISDN BRI/PRI protocol and this Section applies to all 911 Emergency Service system(s) using the ISDN protocol.

The interfaces listed are further described below with the minimum features that are essential for maintaining the DSN quality of service. CPE's that are designed to actively control the interaction of switch supervision are further described to make a distinction between manual and automated CPE supervision control (i.e., fax, modems, versus analog and digital 2 wire subscriber instruments) to ensure MLPP transparent operation.

5.2.12.3.4 Definitions

Definitions of terms can be found in UCR 2008, Appendix A, Section A2, Glossary and Terminology Description.

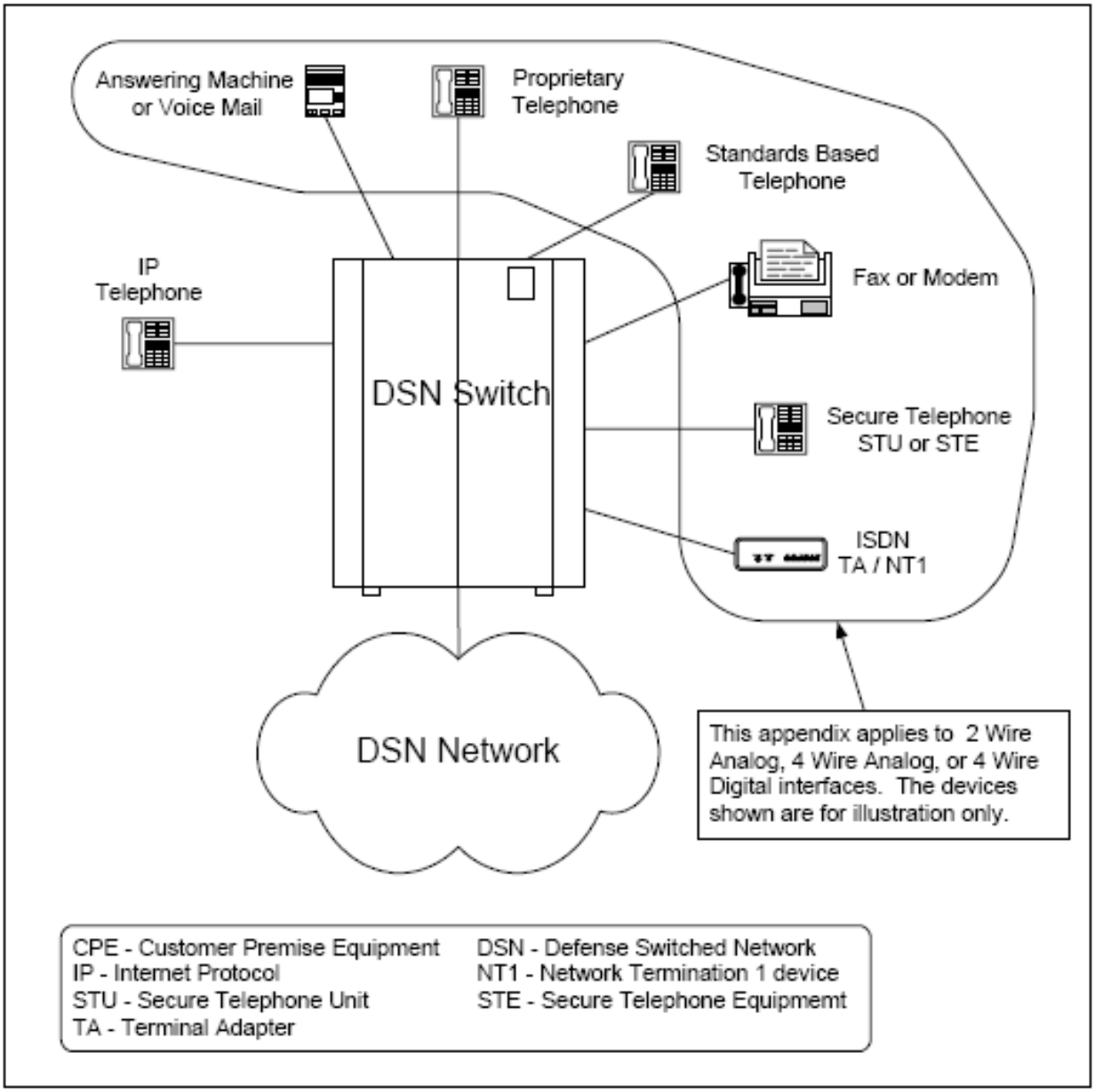


Figure 5.2.12-2. Typical CPE Connections to the DSN

Figure 5.2.12-3, ISDN Reference Points, illustrates the ISDN specified reference points and the arrangement of terminal equipment. The reference points applicable for DSN CPE are:

U The reference point for a Basic Rate Interface (BRI) connection between a local loop and a customer premise. The U interface specifies a single pair loop over which a logical 4-wire circuit is derived.

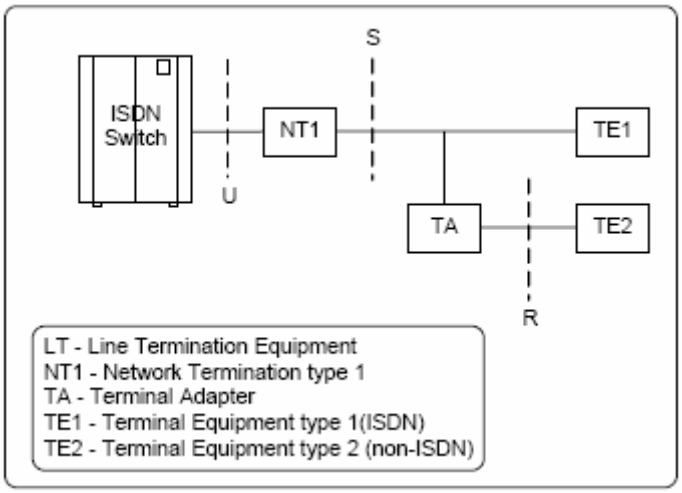


Figure 5.2.12-3. ISDN Reference Points

S The reference point between ISDN user terminal equipment (i.e., TE1 or TA) and the network termination equipment (NT1). This is a 4-wire interface that supports the BRI 2B+D protocol.

R The reference point representing a standardized non-ISDN interface such as EIA-232, EIA-422, V.24, V.35, etc. The combination of a TA and TE2 is equivalent to a TE1.

5.2.12.3.5 Requirements

All CPE devices covered by this section are required to meet the following requirements:

[Conditional] All CPE devices that support MLPP shall do so in accordance with the requirements as listed in UCR 2008, Section 5.2.2, Multilevel Precedence and Preemption, and shall not affect the DSN interface features and functions associated with line supervision and control.

[Required] All DSN CPE, as a minimum, must meet the requirements of Part 15 and Part 68 of the FCC Rules and Regulations, and the Administrative Council for Terminal Attachments (ACTA).

[Conditional] Device(s) that support auto-answer shall have a “Auto-Answer” mode settable have the feature to set the auto-answer mode to a “time” more than the equivalency of four (4) ROUTINE precedence ring intervals in accordance with UCR 2008, Section 5.2.2.3, Precedence Call Diversion, before “answer” supervision is provided. Handling of the precedence calls will be in accordance with UCR 2008, Section 5.2.2.2.4.2, Precedence Calls to Non-MLPP Networks.

[Conditional] Devices that are required to support precedence calls above ROUTINE precedence, shall respond properly to an incoming alerting (ringing) precedence call cadence as described in UCR 2008, Section 5.2.4.5.1, Ringing.

[Conditional] Device(s) that can "out-dial" DTMF and/or DP digits (automatic and/or manual) shall comply to the requirements as stated in UCR 2008, Section 5.2.4.4.1, Dial-Pulse Signals, and Section 5.2.4.4.2, DTMF Signaling, respectively, for its address digit generating capabilities and shall be capable of outpulsing DTMF digits specified in Telcordia Technologies GR-506-CORE, *Signaling for Analog Interfaces*, Issue 1 with Revision 1, June 1996.

[Conditional] Modems and facsimile machines shall be compatible with ITU and Telcordia standards, as applicable.

[Conditional] Facsimile devices, as a minimum, shall meet the requirements in accordance with applicable DISR standards

[Conditional] If Configuration Management and/or Fault Management is provided by the CPE device so that it can be managed by the ADIMSS or other management systems, then the management information shall be provided by one or more of the below listed serial or Ethernet interfaces.

1. Serial interfaces shall be in accordance with one of the following standards:

    a. ITU-T Recommendation V.35
    b. TIA-232-F
    c. EIA-449-1
    d. TIA-530-A

2. Ethernet interfaces shall be in accordance with IEEE Std. 802.3-2002, "Carrier sense multiple access with collision detection (CSMA/CD) access method and physical layer specifications."

[Conditional] As a minimum, the 911 and the E911 (tandem) Emergency Service shall have the capability to "hold" the originating subscriber/caller from releasing the call via the switch supervision interaction for line and trunk control by the "called-party" feature, in accordance with Telcordia Technologies GR-529-CORE.

5.2.12.3.5.1 2-Wire Analog Instruments/Devices

CPE(s) that connect to the DSN using a 2-wire analog interface (analog single line instrument/fax/modem/answering machine/voice mail/automated call distributor) shall meet the following requirements.

[Required] All 2-wire analog devices shall conform to the requirements of TIA/EIA-470-B.

5.2.12.3.5.2 2-Wire Digital Instruments/Devices

CPE(s) that connect to the DSN using a 2 wire digital interface (digital single/multiline proprietary instrument/fax/modem/ISDN BRI devices including 911 emergency service).

[Conditional] CPE(s)s that use loop signaling shall conform to the requirements of TIA/EIA-470-B.

[Conditional] CPE(s) that connect at the ISDN BRI "U" interface shall conform to ANSI T1.601-1999.

5.2.12.3.5.3 4-Wire Digital Instruments/Devices

[Conditional] CPE(s) that connect at the ISDN BRI "S" or "T" interface shall conform to ANSI T1.605-1991 (R1999).

5.2.12.3.5.4 ISDN Terminal Adapter

The general function of a TA is to adapt terminals with non-ISDN standard interfaces (e.g., X-series and V-series interfaces) to ISDN standard user-network interfaces. The TA shall adapt to, connect to, and/or be part of a data-type terminal. The TA connects terminal equipment (TE2), such as a computer, fax machine, LAN, and telephone set, to one or more B channels and passes along digital signals to the ISDN external line. A terminal adapter need not be a separate unit but could be contained within the TE or integrated with the NT1 into a single box. Terminal Adapter(s) shall meet the following requirements:

1. **[Required]** The TA shall be able to connect a non-ISDN terminal (TE2) to one or both of the B channels of an ISDN connection and establish a viable ISDN connection with a terminal at the distant end.

2. **[Required]** The TA shall meet its necessary requirements regardless if it is implemented as a stand-alone device or as a device integrated with either the TE2 it supports or the NT1 which connects it to the network.

3. **[Required]** The TA shall be compatible with National ISDN NI-1/2 as defined by UCR 2008, Section 5.2.1.3.3, National ISDN 1/2 Basic Access.

4. **[Conditional]** The TA shall provide loop back capability in accordance with ITU Recommendation V.54.

5. **[Conditional]** The TA shall support inverse multiplexing in accordance with ITU Recommendation H.244, and conform to Federal Telecommunications Recommendation (FTR) 1080B-2002, when connected to TE2 equipment.

6. **[Required]** The TA shall provide one or more of the below interfaces:

   a. EIA-366-A
   b. EIA-449-1
   c. TIA-530-A
   d. ITU-T Recommendation V.35

5.2.12.3.5.5 Automated Receiving Devices

Automated Receiving Devices (ARDs) are a family of automated devices, which are CPE or network elements, that attaches to the receiving end of a telephone call. Typical ARDs will have an automatic call distribution front-end which could be as simple as a queue that handles incoming calls on a first come first serve basis. More complex ARDs can be full function Automatic Call Distributors (ACDs) that also include pre-determined scheme and routes calls based on routing criteria and, quite often, database handling instructions. Once in queue, if the call is not answered in a specified amount of time, and if the caller had not terminated the call, ARD can also terminate the call, or send the call to another location. Usually the ARD invokes a network carrier based "take back and transfer" to the alternative location. Generally, ARDs do not originate calls to the network.

Automated Receiving Devices can have different names. The following are some typical devices included in this family:

- Automatic call distributor
- Voice messaging system
- Automatic announcer
- Event notification system
- Automated attendant
- Morale, Welfare, and Recreation (MWR) call systems
- Call center system

Automated Receiving Devices shall meet the following minimum requirements:

1. **[Required]** Automated Receiving Devices interfacing to the DSN shall provide at least one of the following interface types:

    a. 2-wire interface as specified in UCR 2008, Section 5.2.12.3.5.1, 2-Wire Analog Instruments/Devices, and/or Section 5.2.12.3.5.2, 2-Wire Digital Instruments/ Devices.

    b. 4-wire interface as specified in UCR 2008, Section 5.2.12.3.5.3, 2-Wire Digital Instruments/Devices.

    c. PCM-24 as specified in UCR 2008, Section 5.2.6.1, PCM-24 Digital Trunk Interface.

    d. PCM-30 as specified in UCR 2008, Section 5.2.6.2, PCM-30 Digital Trunk Interface.

5.2.12.3.5.6 Remote Access

This requirement is for calls attempting to access/leave the DSN via an ARD.

[Required] The Remote Access feature shall meet the overall requirements of ARD (UCR 2008, Section 5.2.12.3.5.5, Automated Receiving Devices).

[Required] The ARD shall receive calls, provide an alerting message or tone to alert the caller to dial additional digits and screen those digits in order to permit/restrict extending the call (Telcordia Technologies SR-504, Section 02-01-0150).

[Required] The ARD shall use a caller provided Personal Identification Number (PIN) and/ or Authorization (Auth) code (minimum of five digits for either with a failure of three attempts will result in a disconnect) and/or a system provided ANI. Any combination of screening features may be used to screen incoming callers for access permission and call extension control. This feature can be either enabled or disabled by an administrator.

[Required] The ARD shall verify that the ANI and/or PIN or Auth Code is not already in use on another call, thus preventing unauthorized use of the ANI/PIN/Auth code. This feature can be either enabled or disabled by an administrator.

5.2.12.4 Video Teleconferencing Requirements

5.2.12.4.1 Background

This section describes the requirements that must be met by all VTC systems and end points for them to be certified and used in the DSN.

5.2.12.4.2 Purpose

The purpose of this UCR 2008 section is to specify the video teleconferencing system operational interface requirements to DSN switches necessary to ensure proper MLPP and other MUF feature operations in accordance with the DoD directive for DSN services.

VTC systems connected to the DSN shall, as a minimum, comply with UCR 2008 and with the required capabilities identified in this section so that the VTC system has features and capabilities considered necessary for interfacing to a particular DSN serving switch type to support warfighter missions in DoD. These VTC features and capabilities will require JITC certification and DISA IA accreditation prior to connection to the DSN.

Conditional requirements are features and capabilities that are not considered critical for DoD mission support based on DoD policies. It is however, recognized that such features do have utility for some users or for specific operations. To ensure interoperability and consistency of the MUF functionalities across all platforms, these features and capabilities are specified with set parameters. If these features and capabilities are provided, the device shall perform and meet the requirements as identified in this UCR 2008 section.

5.2.12.4.3 Applicability

This section applies to all video teleconferencing systems/end points procured or leased for installation in the DSN. DSN assets, services, features, and functions (both unique military and standard commercial) shall not be adversely affected by the implementation of such VTC systems/end points. DSN assets include switches, trunks, lines, CPE, and ancillary equipment. This section also applies to upgrades and new software loads for existing VTC systems/ end points and equipment.

The UCR 2008 is the governing requirements document that takes precedence over the explicit or implicit requirements of subsidiary or reference documents, standards, and specifications. In the event of conflict, the explicit requirements of the UCR take precedence over the explicit or implicit requirements of the LSSGR and Generic Requirements.

5.2.12.4.4 General

The DSN provides an implementation of non-MLPP and MLPP ISDN that can be used for end-to-end digital VTC systems in secure or non-secure modes at any level of precedence. The DSN uses an intelligent signaling network and a limited set of user-network interfaces. The DSN implementation of ISDN will allow for the integration of voice, data, video, text, and graphics communications. The DSN is capable of two ISDN standard interfaces identified as:

- Basic Rate Interface (BRI)
- Primary Rate Interface (PRI)

Video teleconferencing systems and endpoints connected to the DSN may incorporate the following:

- Camera, monitor, microphone, and speakers
- Codec
- MCU
- H.323 to H.320 Gateway
- Cryptographic device/cryptographic device bypass unit
- Other similar equipment.

H.323 assured service has not yet been defined, thus the H.323 interface has no assured service capabilities. This interface can only serve DoD, non-DoD, non-governmental, and foreign government users having no missions or communications requirement to ever originate or receive C2 VTC communications under existing military scenarios. These users are provided access to the DSN for the economic or policy benefits of the DoD, when it is not in conflict with local PTT ordinances. Since H.323 does not provide assured services during a crisis or contingency, users' access to the DSN will be on a best effort basis. Therefore, C2 VTC users and special C2 VTC users are not authorized to be served by an H.323 interface.

These devices may be implemented as individual components or be integrated with one or more other components as a system. The terms VTC, VTC system(s), and VTC end point(s) are used synonymously.

VTC systems/end points are typically connected to the DSN via an IAS (see UCR 2008, Section 5.2.12.7, Integrated Access Switch/System Requirements, for DSN IAS requirements) or a Terminal Adapter (see UCR 2008, Section 5.2.12.3, Customer Premises Equipment Requirements, for DSN TA requirements). This requirement also addresses VTC systems/end points that have an integral IAS or TA for connection to the DSN. In addition to the requirements specified in this UCR 2008 section, VTC systems/devices that have integral

IAS/TA functions shall conform to the stated requirements identified in Section 5.2.12.7 and Section 5.2.12.3, as applicable.

Figure 5.2.12-4, Typical VTC System connections to the DSN, shows typical connections between VTC systems/endpoints and the DSN. Other connection configurations may be possible.

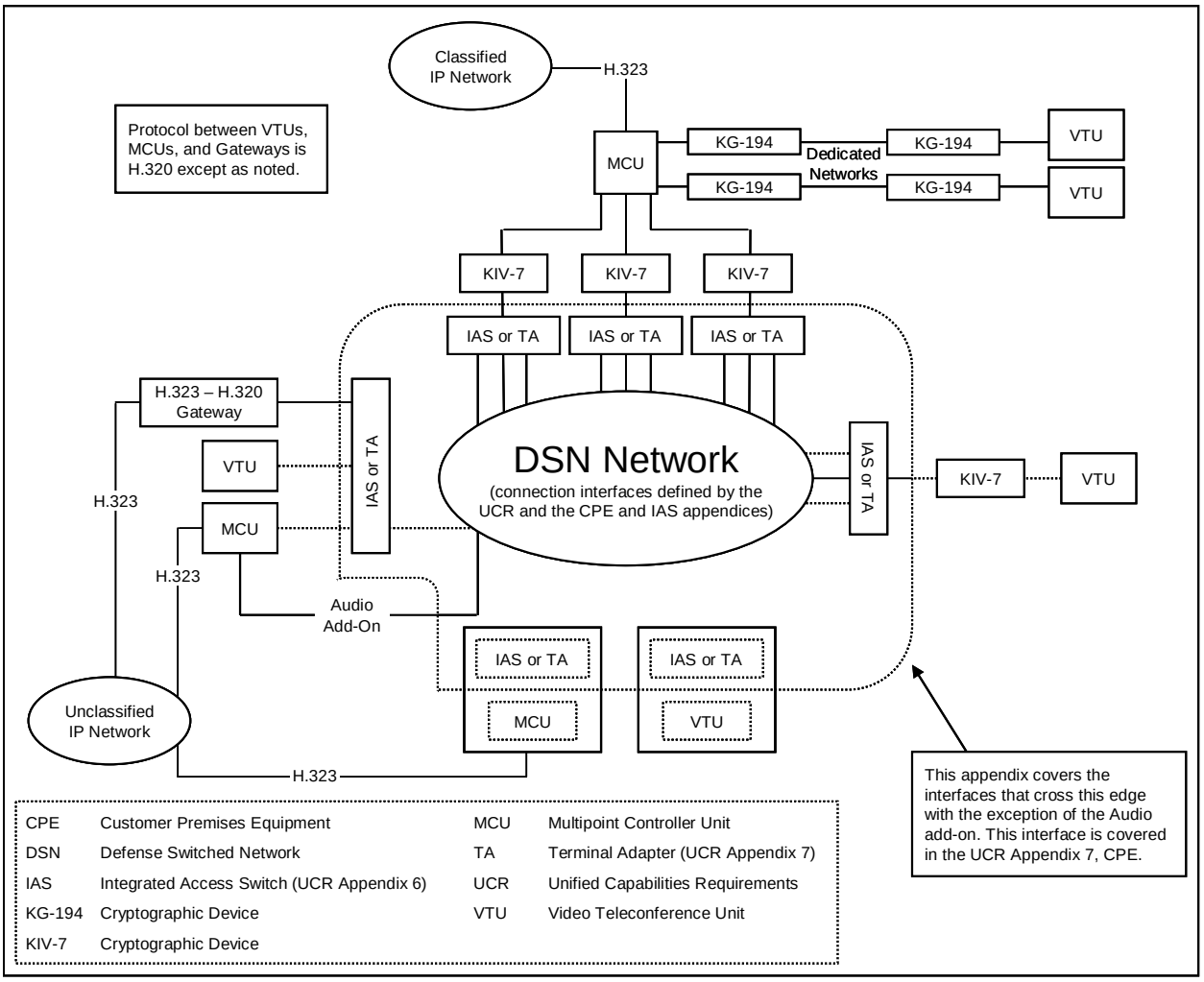


Figure 5.2.12-4. Typical VTC System connections to the DSN

5.2.12.4.5 Video Teleconferencing Requirements

This section provides the requirements for VTC systems/end points in the DSN. All VTC systems/end points, when interfaced to the DSN, are required to meet the following requirements:

1. **[Required]** The VTC system/endpoints shall meet the requirements of FTR 1080B-2002.

2. **[Conditional]** VTC features and functions used in conjunction with IP network services shall meet the requirements of H.323 in accordance with FTR 1080B-2002. Additionally, H323 Video EIs must meet the tagging requirements as specified in UCR 2008, Section 5.2.12.8.2.9, VoIP System Service Class Tagging Requirements.

3. **[Required]** A loss of any conferee on a multipoint videoconference shall not terminate or degrade the DSN service supporting VTC connections of any of the other conferees on the videoconference.

4. **[Conditional]** An Audio add-on interface, implemented independently of an IAS, shall be in accordance with UCR 2008 and in particular, UCR 2008, Section 5.2.12.3, Customer Premise Equipment Requirements.

5. **[Conditional]** A VTC system/end point that uses an integrated BRI interface to connect to the DSN shall be in conformance with the requirements associated with a TA as described in UCR 2008, Section 5.2.12.3, Customer Premise Equipment Requirements.

6. **[Conditional]** A VTC system/end point that uses an integrated PRI interface to connect to the DSN shall be in conformance with the requirements associated with an IAS as described in UCR 2008, Section 5.2.12.7, Integrated Access Switch/System Requirements.

7. **[Conditional]** A VTC system/end point that uses a serial interface(s) to another device, such as a cryptographic device, IAS, or TA, for eventual connection to the DSN, shall be in conformance with the requirements for that serial interface(s) as described in FTR 1080B-2002.

8. **[Required]** Physical, electrical, and software characteristics of VTU system(s)/end point(s) that are used in the DSN network shall not degrade, or impair, the serving DSN switch and its associated network operations.

5.2.12.4.6 Definitions

Definitions of terms can be found in UCR 2008, Appendix A, Section A2, Glossary and Terminology Description.

5.2.12.5 DSN Strategic Network Element Generic Requirements

5.2.12.5.1 Background

This section describes the requirements that must be met by DSN Strategic Network Element (S-NE) devices. The S-NE may be referred to as network element(s) in the remainder of the document.

A Network Element is any component of a network through which the DSN bearer and/or signaling traffic transits. For IP transport, the IP connection may transit a LAN, MAN, CAN, or WAN dependent on its deployment. Network elements may include multiplexers, routers, CSU/DSUs, compression devices, circuit emulation, channel banks and/or any network device that could have an effect on the performance of the associated network traffic. The network diagram Figure 5.2.12-5, Network Element Diagram, shows the typical network element as a stand-alone device or integrated into the transmission interfaces of switches or other network devices. The use of NEs shall not provide the means to bypass the DSN as the first choice for all switched voice and dial-up video telecommunications between DOD user locations.

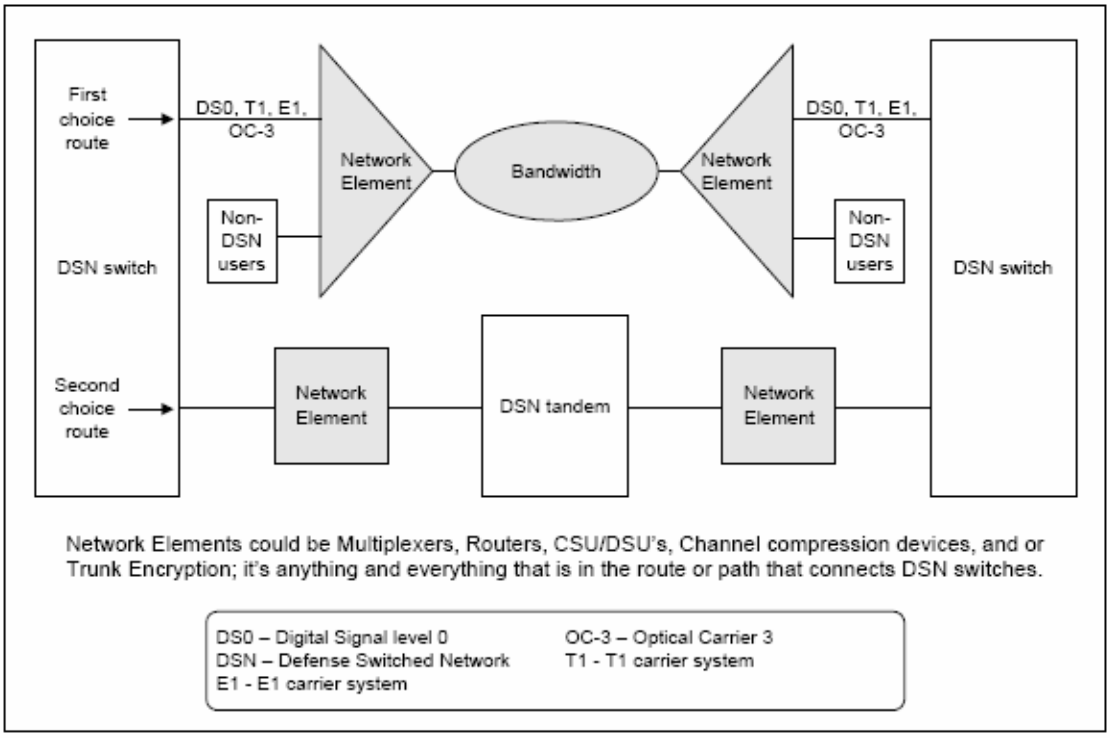


Figure 5.2.12-5. Network Element Diagram

5.2.12.5.2 Purpose

The purpose for developing this UCR 2008 section is to specify the NE requirements so they can be certified for use in the DSN.

5.2.12.5.3 Applicability

This requirement applies to all NEs procured or leased for installation in the DSN. All services, features, and functions (both unique military and standard commercial) identified in this UCR 2008 section are to be implemented in DSN assets including switches, trunks, and ancillary equipment. This requirement also applies to upgrades and new software loads for existing equipment. This section is not applicable to those network elements that are covered explicitly in the UCR or by other sections.

5.2.12.5.4 Definitions

Definitions of terms can be found in UCR 2008, Appendix A, Section A2, Glossary and Terminology Description.

5.2.12.5.5 Requirements

As a minimum, requirements below include the following features and capabilities considered necessary for a particular switch type to support warfighter missions in DoD. In addition to the compliance requirements of the main body of this UCR, all network elements are to be compliant with the following requirements and conditions.

5.2.12.5.5.1 Overall Requirements

5.2.12.5.5.1.1 General Requirements

[Required] All network trunk elements shall meet the following general requirements and conditions:

1. The introduction of an NE(s) shall not cause the end-to-end average MOS to fall below 4.0 as measured over any 5-minute time interval.

2. The introduction of an NE shall not cause to exceed more then .03 percent of the end-to-end digital bit error rate requirement of less than 1 error in $1x10^9$ (averaged over a 9-hour period).

3. The introduction of an NE(s) shall not degrade secure transmission for secure end devices as defined by UCR 2008, Section 5.2.12.6, DoD Secure Communications Devices.

4. The NE(s) shall support a minimum modem transmission speed of 9.6 kbps across the associated NE(s).

5. The NE(s) shall support a minimum facsimile transmission speed of 9.6 kbps across the associated NE(s).

6. The NE shall transport all call control signals transparently on an end-to-end basis.

7. The addition of S-NEs shall not cause the one-way delay measured from ingress to egress to increase by more than 5 milliseconds (ms) for each S-NE used, averaged over any 5-minute period.

5.2.12.5.5.1.1.1 Alarms

[Required] The NE shall be able to propagate CGAs in accordance with UCR 2008, Section 5.2.1.5.7, Carrier Group Alarm, upon physical loss of the TDM interface. Voice switching systems shall receive the proper CGAs from the NE upon loss of the transport link between NEs, regardless of whether it is TDM or IP.

5.2.12.5.5.1.1.2 Congestion Control

The network element shall assure that congestion between network elements does not impact DSN calls in progress or subsequent calls. Call congestion handling shall be met in one or more of the following ways.

5.2.12.5.5.1.1.2.1 For TDM Transport

[Conditional] The S-NE shall implement TDM congestion control via one of the following methods:

1. A dynamic load control signal (e.g., contact closure) shall be provided to the DSN switch in accordance with UCR 2008.

2. Congestion is not possible in the network element by nature of its functioning (e.g. a TDM multiplexer or transcoder).

A software capability in limiting the provisioning the input and/or output interfaces such that makes congestion impossible even under the worst congestion scenario. This can be done by limiting the bearer or aggregate provisioning

5.2.12.5.5.1.1.2.2 For IP Transport

[Conditional] The NE shall implement IP congestion control. Congestion may be controlled by using Differentiated Services which shall be capable of providing preferential treatment for call congestion over other media types in accordance with UCR 2008, Section 5.3.3, Network Infrastructure End-toEnd Requirements, and a capability to limit the provisioning of input and output interfaces such that congestion is impossible under the worst transport congestion scenario.

5.2.12.5.5.1.1.3 Compression

[Conditional] The network element used for voice compression shall support at least one of the following standards:

- ITU-T Recommendation G.726
- ITU-T Recommendation G.728
- ITU-T Recommendation G.729

5.2.12.5.5.1.2 Interface Requirements

5.2.12.5.5.1.2.1 Analog

[Conditional] The network element for an analog 2-wire or 4-wire trunk interface shall be in accordance with UCR 2008, Section 5.2.6.4, Analog Trunk Interface.

5.2.12.5.5.1.2.2 Serial

[Conditional] The network element used for serial interface connections shall be in accordance with one of the following standards:

- ITU-T Recommendation V.35
- TIA-232-F
- EIA-449-1
- TIA-530-A

5.2.12.5.5.1.2.3 BRI ISDN

[Conditional] ISDN Basic Rate Interface (BRI) interface shall meet the requirements and conditions in accordance with UCR 2008, Section 5.2.1.3.3, National ISDN 1/2 Basic Access.

5.2.12.5.5.1.2.4 DS1 Interface Requirements

[Conditional] T1 interface shall meet the requirements and conditions in accordance with UCR 2008, Section 5.2.6.1, PCM-24 Digital Trunk Interface.

5.2.12.5.5.1.2.5 E1 Interface Requirements

[Conditional] E1 interface shall meet the requirements and conditions in accordance with UCR 2008, Section 5.2.6.2, PCM-30 Digital Trunk Interface.

5.2.12.5.5.1.2.6 DS3 Interface Requirements

[Conditional] DS3 interface shall meet the following requirements and conditions.

5.2.12.5.5.1.2.6.1 Framing

[Required] Frame structure shall include M13 framing in accordance with ANSI T1.107-2002.

[Conditional] Frame structure may include C-bit parity application in accordance with ANSI T1.107-2002.

5.2.12.5.5.1.2.6.2 Line Coding

[Required] The line coding shall be bipolar 3 zero substitution (B3ZS) in accordance with ANSI T1.102-1993.

5.2.12.5.5.1.2.7 Timing

[Required] The network element shall be able to derive timing signal from an internal source, an incoming digital signal, or an external source in accordance with UCR 2008, Section 5.2.10.1, Timing Modes.

5.2.12.5.5.1.2.8 OC-X Interface Requirements

[Conditional] OC-X interface shall be in accordance with UCR 2008, Section 5.2.12.2, DSN Switch SONET Digital Trunk Interface, and/or appropriate SONET commercial standards. (NOTE: X stands for the capacity (e.g. 3, 48, 192 and higher).

5.2.12.5.5.1.2.9 IP Interface

[Conditional] S-NEs using IP shall meet all of the following parameters:

1. Delay. The addition of S-NEs shall not cause the one-way packet delay measured from ingress to egress to increase by more than 5 milliseconds (ms) for each S-NE used, averaged over any 5-minute period.

2. Jitter. The addition of an S-NE shall not cause jitter measured from ingress to egress to increase by more than 5 ms averaged over any 5-minute period:

3. Packet Loss. The addition of an S-NE shall not cause packet loss measured from ingress to egress to increase by more than 0.05% averaged over any 5-minute period.

[Conditional] IP interface shall meet the IP requirements detailed in the DoD Information Technology Standards Registry (DISR) and Section 5.3, IP-Based Capabilities and Features, inclusive.

5.2.12.5.5.2 Device Management

5.2.12.5.5.2.1 Management Options

[Required] Network element devices are to be managed by at least one of the following:

1. **[Conditional]** A front or back panel and/or external console control capability shall be provided for local management.

2. **[Conditional] Remote monitoring and management** by the ADIMSS as described in the UCR 2008, Section 5.2.8, Network Management, Section 5.2.8.3, Fault Management, and Section 5.2.8.4, Configuration Management.

5.2.12.5.5.2.2 Fault Management

[Conditional] Shall report any failure of self-test diagnostic function on non-active and active channels on a noninterference basis to the assigned NM system.

5.2.12.5.5.2.3 Loop Back Capability

[Conditional] The network element shall provide loop back capability on each of the trunk side interfaces in accordance with ITU-T Recommendation V.54.

5.2.12.5.5.3 Operational Configuration Restoral

[Required] Loss of power should not remove configuration settings. Unit should be restored to the last customer configured state prior to the power loss, without intervention when power is restored.

5.2.12.6 DoD Secure Communications Devices

5.2.12.6.1 Background

This section describes the requirements that will be used to certify DoD Secure Communications Devices (DSCDs) when directly connected to or otherwise traversing the DSN, the PSTN, or the DRSN Gateway to/from the DSN.

5.2.12.6.2 Definitions

Definitions of terms can be found in UCR 2008, Appendix A, Section A2, Glossary and Terminology Description.

5.2.12.6.3 Scope

This section applies to the secure mode operation of any DSCD that either directly connects to the DSN, the PSTN, or the DRSN Gateway, or traverses these networks in the course of conducting a secure communications session, regardless of where the telephone call originates or terminates. The certification test environment for DSCDs shall include configurations that realistically simulate strategic networks (DSN, DRSN via the DSN Gateway, PSTN), as well as tactical networks, such as DVX Systems and other configurations as defined by the Executive Agent for Theater Joint Tactical Networks, or any combination thereof.

5.2.12.6.4 Purpose

The purpose of this section is to specify the minimum requirements that a DSCD must meet in order to be certified.

5.2.12.6.5 Applicability

This section applies to all DSN DSCDs that are procured or leased for installation in the DSN. All services, features and functions (both unique military and standard commercial) that are implemented in DSN DSCDs shall meet the requirements identified in this UCR and associated UCR 2008 sections. This requirement also applies to upgrades and new software loads for existing equipment. This section applies to all past, current, and future DSCDs, including DSCD hardware and/or software upgrades and patches to DSCDs when used on the DSN or other connected networks.

5.2.12.6.6 Requirements

The JITC will validate all of the features and capabilities of a DSCD device, to include voice, data, and facsimile transmission.

[Required: STE Enabled DSCD, FNBDT/SCIP Enabled DSCD] The enabled DSCD shall be only those that are Type Approved by NSA and are listed on the NSA Secure Product Web site. Each DSCD must support at least one NSA approved secure protocol. If the DSCD supports more than one secure protocol, it must meet all the requirements for at least one of the secure protocols, and must minimally support the other protocols that are provided on the DSCD.

[Required: STE Enabled DSCD, FNBDT/SCIP Enabled DSCD] DSCD devices that use a 2-wire analog or BRI interface shall meet the EI requirements as specified in Section 5.2.12.3, Customer Premises Equipment Requirements. DSCD devices that use an IP interface shall meet the end instrument requirements as specified in Section 5.3.2, Assured Services Requirements.

[Required: STE Enabled DSCD, FNBDT/SCIP Enabled DSCD] A DSCD device that supports one of the required signaling modes shall interoperate with and establish secure sessions with other compatible devices with at least an 85% secure call completion rate.

[Required: STE Enabled DSCD, FNBDT/SCIP Enabled DSCD] The DSCD shall be capable of using the protocol(s) provided to establish a secure session within 60 seconds and must maintain secure communications for the duration of the secure portion of the call.

[Required: STE Enabled DSCD, FNBDT/SCIP Enabled DSCD] The DSCD shall operate in a network that has an end-to-end latency of up to 600 milliseconds.

[Required: STE Enabled DSCD, FNBDT/SCIP Enabled DSCD] The DSCD shall achieve and maintain a secure voice connection with a minimum MOS of 3.0.

[Required: STE Enabled DSCD, FNBDT/SCIP Enabled DSCD] Once connected to the re-key center, the DSCD shall obtain a new key and properly process that new key with a 95% rekey completion rate.

[Conditional: STE Enabled DSCD, FNBDT/SCIP Enabled DSCD] DSCDs that establish secure sessions on a Continuously Variable Slope Delta (CVSD) switch and terminate on a CVSD switch, without ever traversing or otherwise interacting with the DSN, DRSN, or PSTN must do so with a 50% completion rate.

[Conditional: FNBDT/SCIP enabled DSCD] DSCDs that establish secure sessions on IP networks using FNBDT/SCIP shall satisfy all of the end point requirements described SCIP-215 and SCIP-216.

[Conditional: STE and FNBDT/SCIP Enabled DSCD] DSCD devices shall support a minimum data rate and facsimile transmission rate of 9.6 kbps.

5.2.12.7 Integrated Access Switch/System Requirements

5.2.12.7.1 Background

This section describes the requirements that must be met by all Integrated Access Switch/System (IAS) CPE devices for them to be certified and used in the DSN. An IAS is an ISDN device with one or more PRI interfaces to a DSN switch. It will only be used to support video and data services.

5.2.12.7.2 Purpose

The purpose of this UCR 2008 section is to specify the IAS CPE requirements so it can be certified for use in the DSN.

5.2.12.7.3 Applicability

This UCR 2008 section applies to all DSN IAS CPE devices/systems procured or leased for installation in the DSN. All services, features, and functions (both unique military and standard commercial) identified in this UCR and associated sectiones are to be implemented in DSN assets including switches, trunks, lines, CPE, and ancillary equipment. This requirement also applies to upgrades and new software loads for existing equipment.

The UCR 2008 is the governing requirements document that takes precedence over the explicit or implicit requirements of subsidiary or reference documents, standards, and specifications. In the event of conflict, the explicit requirements of the UCR 2008 take precedence over the explicit or implicit requirements of the LSSGR and Generic Requirements.

5.2.12.7.3.1 Definitions

Definitions of terms can be found in UCR 2008, Appendix A, Section A2, Glossary and Terminology Description.

5.2.12.7.4 Integrated Access Switch Requirements

The IAS is CPE system that interconnects a DSN switch and Terminal Equipment (TE) such as Inverse Multiplexers (IMUXs), routers, VTC (Video Teleconference) Codecs, VTC Monitors, and Multipoint Control Units (see Figure 5.2.12-6, Typical Connections for an IAS). The IAS is able to originate multiple data and/or video calls in accordance with the worldwide numbering and dialing plan (WWNDP) as described in Section 5.2.3.5.1, DSN Worldwide Numbering and Dialing Plan. Depending on the local implementation, PRI to PRI, PRI to BRI or BRI to PRI, interconnection is accomplished by the IAS. The IAS does not possess any functions of MLPP, but shall be able to originate calls that can be interpreted by the DSN switch as precedence calls and may be preempted on the DSN switching platforms and network trunks (see Figure 5.2.12-7, MLPP Implementation and the IAS). The IAS shall be provisioned so that the number of provisioned TE interface bearer channels shall not exceed the number of provisioned DSN or commercial interface bearer channels. This is to reduce the possibility of a call destined for a TE from being blocked by the DSN or commercial interfaces on the IAS not having available bearer channels for this call. It should also be noted that VTC call inherently has a ROUTINE precedence level. A typical layout of the IAS is illustrated in Figure 5.2.12-6.

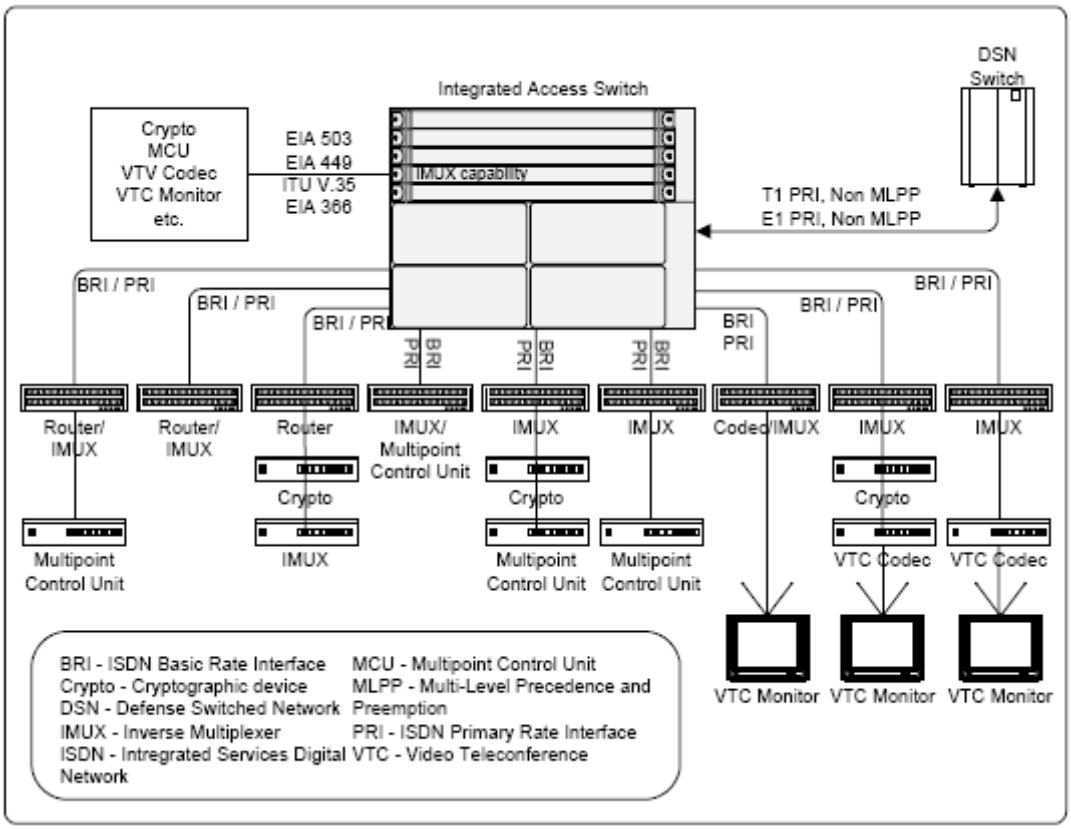


Figure 5.2.12-6. Typical Connections for an IAS

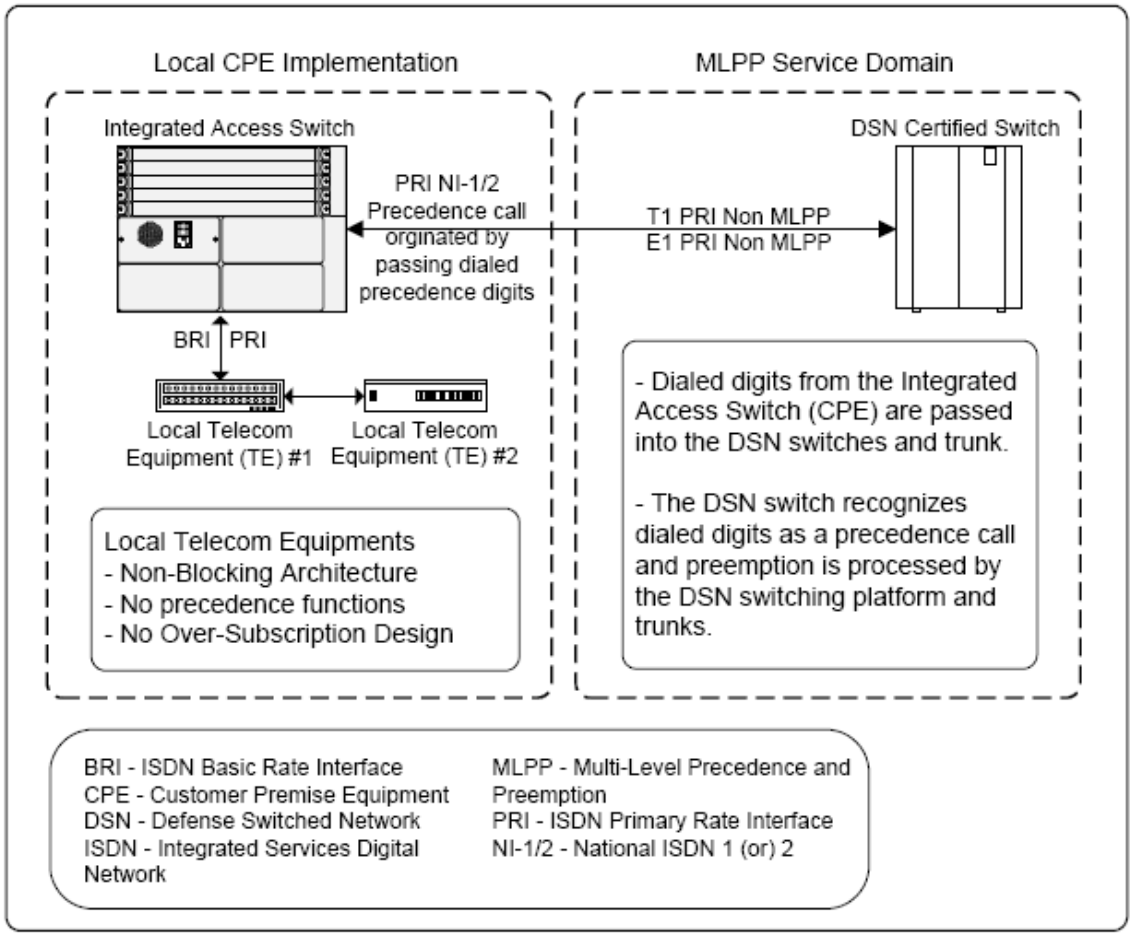


Figure 5.2.12-7. MLPP Implementation and the IAS

Figure 5.2.12-8, Applications for the IAS, shows the applications for the IAS.

All IASs are required to meet the following requirements.

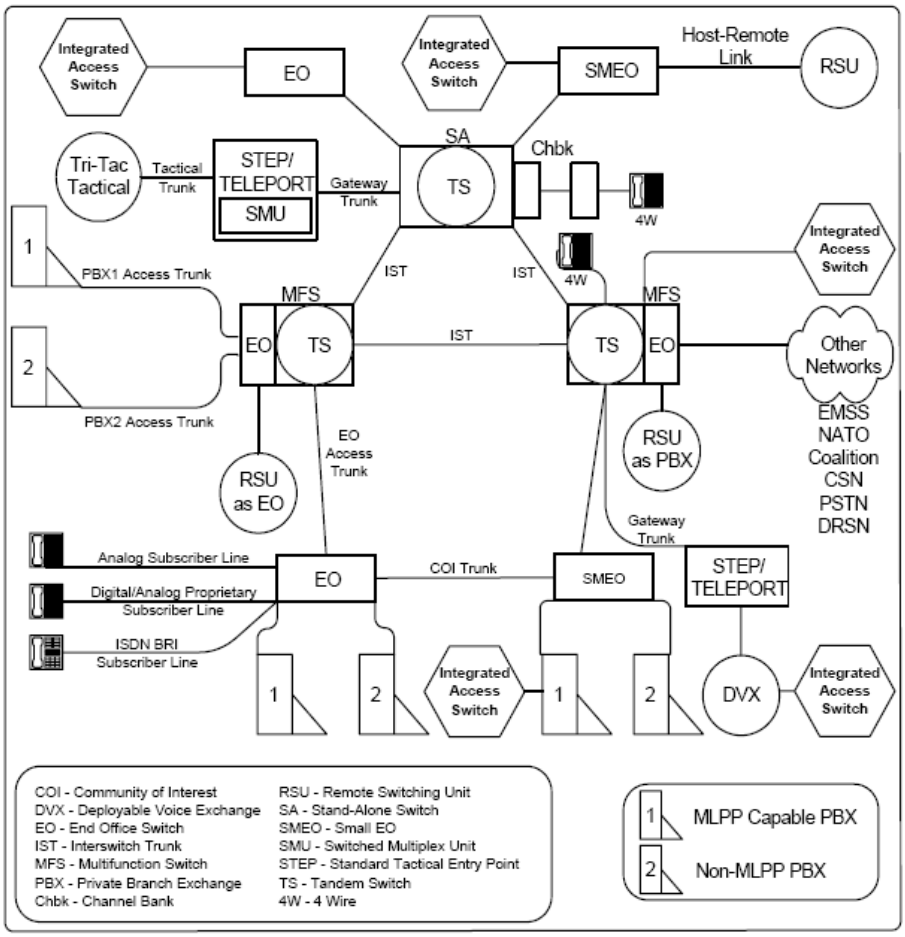


Figure 5.2.12-8. Applications for the IAS

5.2.12.7.4.1 Interfaces

DSN interfaces:

[Required] T1 ISDN PRI NI 1/2

1. The IAS shall conform to Section 5.2.1.3.4, ISDN Primary Access, and Section 5.2.4.7, ISDN Digital Subscriber Signaling System No. 1 Signaling, inclusive and shall provide the ISDN PRI capabilities shown in Table 5.2.9-5, PRI Features.

2. The IAS shall conform to Telcordia Technologies, SR-2275, Table 14-4, which provides the specific requirements for features and capabilities listed in Table 5.2.12-1, T1 PRI Access, Call Control, and Signaling.

The IAS shall support line timing mode in accordance with UCR 2008, Section 5.2.10.1, Timing Modes.

Table 5.2.12-1. T1 PRI Access, Call Control, and Signaling

FEATURE OR CAPABILITY	REQUIREMENT
PRI Layer 1	Required
PRI Layer 2 (Circuit)	Required
PRI Call Control and Signaling Basic Call Control for Circuit-Mode Calls Multiple DS1 Facilities Controlled by a Single D-Channel D Channel Backup Access to Selected Primary Rate Services on a Per-Call Basis PRI Interworking with SS7	 Required Conditional Conditional Conditional Conditional
Uniform Cause Values and Location Indicators – Subset	Conditional
RESTART Procedures Support of Single Interface Initiated by the CPE Support of Restart of All DS1s Controlled by a D channel, Initiated by the SPCS Support of Restart Collision Procedures	 Conditional Conditional Conditional
SWF-DS1	Required
PRI Packet-Mode Call Control	Conditional

[Conditional] E1 ISDN PRI

If provided, the IAS shall conform to Section 5.2.1.3.4, ISDN Primary Access, and Section 5.2.4.7, ISDN Digital Subscriber Signaling System No. 1 Signaling, inclusive.

TE Interfaces:

[Required] One of the following interfaces is required.

1. **[Conditional]** T1 ISDN PRI NI 1/2

    a. The IAS shall conform to Section 5.2.1.3.4, ISDN Primary Access, and Section 5.2.7, Tandem Switching, inclusive and provide the ISDN PRI capabilities shown in Table 5.2.12-2, T1 PRI Access, Call Control, and Signaling.

    b. The IAS shall conform to Table 14-4 of Telcordia Technologies, SR-2275, Telcordia Notes on the Networks, Issue 4, October 2000, which provides the specific requirements for features and capabilities listed in Table 5.2.12-2.

Table 5.2.12-2. T1 PRI Access, Call Control, and Signaling

FEATURE OR CAPABILITY	REQUIREMENT
PRI Layer 1	Required
PRI Layer 2 (Circuit)	Required
PRI Call Control and Signaling Basic Call Control for Circuit-Mode Calls Multiple DS1 Facilities Controlled by a Single D-Channel D-Channel Backup Access to Selected Primary Rate Services on a Per-Call Basis PRI Interworking with SS7	 Required Conditional Conditional Conditional Conditional
Uniform Cause Values and Location Indicators - Subset	Conditional
RESTART Procedures Support of Single Interface Initiated by the CPE Support of Restart of All DS1's Controlled by a D-channel, Initiated by the SPCS Support of Restart Collision Procedures	 Conditional Conditional Conditional
SWF-DS1	Required
PRI Packet-Mode Call Control	Conditional

2. **[Conditional]** E1 ISDN PRI NI 1/2

The IAS shall conform to Section 5.2.4.7, ISDN Digital Subscriber Signaling System No. 1 Signaling, inclusive.

3. **[Conditional]** ISDN BRI NI 1/2

   a. The IAS shall conform to the requirements in Section 5.2.1.3.3, National ISDN 1/2 Basic Access, and Section 5.2.9, Integrated Services digital Network, inclusive, with the exception that the IAS may include either the S/T or U interface, and provide the ISDN BRI capabilities shown in Table 5.2.12-3, BRI Access, Call Control, and Signaling.

   b. The IAS shall conform to Tables 14-1 through 14-3 of Telcordia Technologies, SR-2275, *Telcordia Notes on the Networks*, Issue 4, October 2000, which provides the specific requirements for features and capabilities listed in Table 5.2.12-3.

5.2.12.7.4.2 Security

[Required] The IAS shall conform to the requirements outlined in DoDI 8510.bb and the applicable DSN STIGs.

Table 5.2.12-3. BRI Access, Call Control, and Signaling

FEATURE OR CAPABILITY	REQUIREMENT
ISDN BRI Layer 1	Required
4:1 TDM Method for ISDN Basic Access	Conditional
ISDN BRI Layer 2	Required
BRI Circuit-Mode Call Control Basic Call Control	Required Required
Uniform Cause Values and Location Identifiers – Subset	Conditional
BRI Terminal Initialization	Required
Service Profile Identifier	Required
Parameter Downloading Parameter Downloading – Version 2 (Extensions for Virtual Key Service) Download Additional Data for Softkey Operations – Parameter Downloading – Version 2.1	 Conditional Conditional Conditional
Automatic SPID	Conditional
Default Services for Terminals	Conditional
BRI Interworking with SS7	Conditional
ISDN BRI Packet-Mode Call Control User Originated, On-Demand B Channel Packet Conditional Notification	Conditional Conditional Conditional

5.2.12.7.4.3 Numbering Plan

[Required] The IAS shall provide the capability to integrate its numbering plan with the 10-digit format of the NANP and conform to the Section 5.2.3.5.1, DSN Worldwide Numbering and Dialing Plan, inclusive, which defines the DSN World Wide Numbering and Dialing Plan (WWNDP).

[Required] IAS line number assignments shall be within existing geographic DSN WWNDP office codes and shall support the same format that the local PSTN/POTS numbers are assigned (NPA-NXX-XXXX).

[Required] IAS numbering shall conform to ITU-T Recommendation E.164. It shall be able to send all digits defined in UCR 2008, Table 5.2.3-6, DSN User Dialing Format. The IAS shall be able to receive dialed digits and manipulate them as necessary to support the above requirement.

5.2.12.7.4.4 Provisioning

[Conditional] The IAS shall provide software capability to ensure that the number of provisioned TE interface bearer channels do not exceed the number of provisioned DSN or commercial interface bearer channels. This is to reduce the possibility of a call destined for a TE to be blocked by the DSN or commercial interfaces not having available bearer channels for this call.

[Required] The IAS shall provide the capability to allocate a specific amount of bandwidth to each of the TE interfaces at the DS0 level. Calls originating from the TE interfaces shall be prevented from exceeding this bandwidth.

5.2.12.7.4.5 Reliability

[Required] The IAS equipment reliability and availability shall conform to Telcordia Technologies GR-512-CORE, Section 5, as specified for individual devices. The vendor shall provide a reliability model for the system, showing all calculations and showing how the overall availability will be met, if requested.

5.2.12.7.4.6 Loop Back Capability

[Conditional] The IAS shall provide loop back capability on each of the TE interfaces in accordance with ITU-T Recommendation V.54.

5.2.12.7.4.7 Inverse Multiplexer Capability

[Conditional] The IAS Inverse Multiplexer (IMUX) capability shall meet the ITU-T Recommendation H.244 requirements and shall conform to FTR 1080B-2002 when connected to TE equipment. Additionally, the IAS IMUX shall provide one or more of the following interfaces:

- EIA-366-A
- EIA-449-1
- TIA/EIA-530-A
- ITU-T Recommendation V.35

5.2.12.8 DSN Line Side Voice over Internet Protocol Requirement

5.2.12.8.1 Background

This UCR 2008 section describes the requirements that will be used to certify Voice over Internet Protocol (VoIP) services provided on the line side of a TDM switch. A TDM switch providing DSN line side VoIP is also referred to as an IP-enabled switch. This requirement only applies to DSN TS, MFS, EO, SMEO, PBX1 and PBX2 switch types which connect to the DSN network via TDM trunks and which may contain TDM and VoIP line side end instruments. Requirements for LANs appear in UCR 2008, Section 5.3.1, ASLAN Infrastructure Product Requirements.

5.2.12.8.1.1 Definitions

Definitions of terms can be found in UCR 2008, Appendix A, Section A2, Glossary and Terminology Description.

5.2.12.8.1.2 Approach

The requirements contained within this section address VoIP-unique requirements for TDM systems having line side VoIP (IP Enabled System). The system will be required to meet the pertinent UCR requirements defined for each TDM-based switch type. For systems that wish to be certified to provide Line Side VoIP functions, in addition to the UCR 2008 switching system requirements, the VoIP system requirements and appropriate IP LAN (i.e., ASLAN or non-ASLAN) requirements contained in UCR 2008, Section 5.3.1, ASLAN Infrastructure Product Requirements, apply also.

5.2.12.8.1.3 Certification

The Line Side IP solutions will be certified in accordance with the UCR and this section. To be certified, switching platforms shall meet the physical interface and feature/capability requirements. The ASLAN and non-ASLAN requirements are summarized in UCR 2008, Section 5.3.1, ASLAN Infrastructure Product Requirements.

UCR 2008, Section 5.3.2, Assured Services Requirements, defines requirements for AS-SIP signaling which will provide IP network-level MLPP. UCR 2008 currently does not require AS-SIP signaling between a switching system (or LSC) and its end instruments, therefore vendors may provide proprietary solutions on the line side in order to meet the MLPP functionality. The ability of the equipment in the LAN to provide voice services in accordance with DoD requirements will be tested using JITC's Generic Switch Test Plan (GSTP) in conjunction with the circuit switch portion of the solution. Upon meeting the requirements, JITC will issue an appropriate letter of certification (e.g., MFS, EO, SMEO, PBX1, or PBX2) for the combined TDM and IP equipment.

5.2.12.8.1.3.1 End Instrument Use in Non-DoD Controlled Networks

If an APL certified IP EI is used to provide DSN voice service where the end-to-end transmission path is not entirely on a DoD controlled network, such as the Internet, performance and reliability cannot be guaranteed. The IP EI connection must be approved through following the DIACAP and local accreditation rules.

5.2.12.8.2 VoIP System Requirements

5.2.12.8.2.1 VoIP System Voice Quality

[Required: TS, EOS, MFS, SMEO, PBX1, PBX2] VoIP systems shall meet the voice quality requirements specified in UCR 2008, Section 5.3.3.14, Voice Service Quality.

5.2.12.8.2.2 VoIP System Codec

[Required: TS, EOS, MFS, SMEO, PBX1, PBX2] IP enabled systems shall use the ITU-T Recommendation G.711 PCM 64 kbps codec. The codec shall use a 20 ms sample size. IP enabled systems shall not use any other codec unless specified in UCR 2008, Section 5.3, IP-Based Capabilities and Features, and Section 6.1, Unique Capabilities and Requirements, of this document.

5.2.12.8.2.3 VoIP System Multilevel Precedence and Preemption

[Required: TS, EOS, MFS, SMEO, PBX1 – Conditional: PBX2] VoIP system shall meet all MLPP requirements identified in UCR 2008, Section 5.2.2, Multilevel Precedence and Preemption. Standards for IP line side MLPP signaling have not been specified in UCR 2008, therefore vendors may initially implement proprietary protocols in their line side VoIP systems to ensure complete MLPP functionality is provided to the DSN IP telephony subscriber, as detailed in Section 5.2.2.. LANs requirements for VoIP systems are provided in UCR 2008 Section 5.3.1, ASLAN Infrastructure Product Requirements.

5.2.12.8.2.4 VoIP System Security

[Required: TS, EOS, MFS, SMEO, PBX1, PBX2] The VoIP implementations within DoD for the provisioning of voice services shall meet the same stringent security procedures as circuit switches. The VoIP systems, either IP Enabled or IP Centric, shall adhere to the GR-815-CORE security measures already outlined in UCR 2008, Section 5.4, Information Assurance Requirements, to provide the features and functionality needed to implement the requirements of the DSN STIG. Additionally, the VoIP system shall provide the features and functionality needed to implement the requirements of the VoIP STIG. Any VoIP subcomponents that utilize operating system, data client, Internet, and/or network technologies (e.g., Windows XP®, UNIX®; Database Management System (DBMS)/Structured Query Language (SQL) Databases, Oracle®, and/or Web Service) for which DISA Field Security Office (FSO) STIGs are enforced, the VoIP subcomponents shall provide the features and functionality needed to implement the requirements of the appropriate DISA FSO STIG requirements..

The following security requirements shall apply for equipment employing VoIP. All VoIP systems shall follow the DSN Switch Certification and Accreditation Processes as defined in Section 6, Procedures, of the ASD(NII)/DoD CIO DoDI 8100.3, dated 16 January 2004.

As applicable, all VoIP systems shall under go:

- STIG testing
- Telcordia Technologies GR-815-CORE testing
- IP vulnerability testing
- TDM vulnerability testing

5.2.12.8.2.5 VoIP System Network Management

[Required: TS, EOS, MFS, SMEO – Conditional: PBX1, PBX2] VoIP systems shall meet the network management functions described in Section 5.2.8, Network Management, as applicable to switch type. The LAN manageability functions specific to the LAN are described in UCR 2008, Section 5.3.1.5, LAN Network Management. The NM requirements specific for the LAN shall be provided via an additional interface beyond those NM interfaces required in UCR 2008, Section 5.2.8, Network Management.

5.2.12.8.2.6 VoIP System Timing

[Required: TS, EOS, SMEO, MFS, PBX1, PBX2] The VoIP system shall support timing as defined in UCR 2008, Section 5.2.10, Synchronization, as appropriate per switch type.

5.2.12.8.2.7 VoIP System Latency

[Required: TS, EOS, MFS, SMEO, PBX1, PBX2] The VoIP one-way system latency shall not be greater than 60 ms averaged over any 5-minute period. The latency is to be measured from IP handset to egress from the VoIP system via a DSN trunk.

5.2.12.8.2.8 VoIP System Internet Protocol Version 6 Requirements

[Required: TS, EOS, MFS, SMEO, PBX1, PBX2] The VoIP systems (a combination of call control and End Instruments) must meet Internet Protocol Version 6 (IPv6) capability requirements as defined in UCR 2008, Section 5.3.5, IPv6 Requirements.

5.2.12.8.2.9 VoIP System Service Class Tagging Requirements

VoIP system shall meet the service class tagging requirements as provided in UCR 2008, Section 5.3.1, ASLAN Infrastructure Product Requirements.

5.2.12.8.2.10 Wireless Instrument Interaction

[Required: TS, EOS, MFS, SMEO, PBX1, PBX2] WEIs shall be in accordance with Section 5.3.1.6.2, Wireless Requirements.

5.2.12.8.3 Softphones

5.2.12.8.3.1 Softphone Interface

[Required : Softphone] The softphone application shall support the following interface capabilities provided by the general-purpose computer hosting the softphone:

- Microphone and speaker or headphone, or any other audio input/output device
- Ethernet interface(s)
- Mouse (Point and click) interaction

5.2.12.8.3.2 Softphone Alerting Signals and Tones

[Required] Softphone shall provide audible and visual alerting to the end user of an incoming call, even if the application is running in the background.

5.2.12.8.3.3 Softphone Reliability

[Conditional] The softphone application shall be exempt from reliability requirements specified elsewhere in this document.

5.2.12.8.3.4 Softphone Security

[Required] Softphone security and all IA requirements are provided in UCR 2008, Section 5.4, Information Assurance Requirements.

5.2.12.8.4 V.150.1 Gateway Capability

[Conditional: TS, EOS, MFS, SMEO, PBX1, PBX2] VoIP systems that establishes IP sessions between V.150.1-based endpoints, such as IP-based DSCDs and the switch TDM gateway, shall comply with the requirements put forth in the NSA specification SCIP-216, or the most current version as listed in the DISR. The DSCDs operating in secure mode as an IP-based V.150.1 end point shall support FNBDT/SCIP compression modes.

THIS PAGE INTENTIONALLY LEFT BLANK

TABLE OF CONTENTS

SECTION **PAGE**

SECTION 5.3 – IP-BASED CAPABILITIES AND FEATURES 351
5.3.1 Assured Services Local Area Network Infrastructure 355
5.3.1.1 Introduction.....355
5.3.1.1.1 IP Network Segments and LAN Nomenclature 355
5.3.1.2 Overview of LAN General Design and Requirements 357
5.3.1.2.1. LAN Types and Mission Support Summary 359
5.3.1.3 General Performance Parameters.....359
5.3.1.3.1 Port Interface Rates.....360
5.3.1.3.2 Port Parameter Requirements 361
5.3.1.3.3 Class of Service Markings 361
5.3.1.3.4 Virtual LAN Capabilities.....363
5.3.1.3.5 Protocols 364
5.3.1.3.6 Quality of Service Features.....365
5.3.1.3.7 Network Monitoring 367
5.3.1.3.8 Security 367
5.3.1.3.9 Product Requirements Summary 367
5.3.1.4 End-to-End Performance Requirements 369
5.3.1.4.1 Voice Services 369
5.3.1.4.2 Video Services 370
5.3.1.4.3 Data Services 370
5.3.1.5 Information Assurance Requirements 371
5.3.1.6 LAN Network Management Requirements 371
5.3.1.6.1 Configuration Control.....372
5.3.1.6.2 Operational Changes.....372
5.3.1.6.3 Performance Monitoring.....372
5.3.1.6.4 Alarms.....372
5.3.1.6.5 Reporting.....373
5.3.1.7 Engineering Requirements.....373
5.3.1.7.1 Physical Media.....373
5.3.1.7.2 Wireless.....373
5.3.1.7.3 Traffic Engineering.....384
5.3.1.7.4 VLAN Design and Configuration.....388
5.3.1.7.5 Power Backup 390
5.3.1.7.6 Availability 391
5.3.1.7.7 Redundancy.....392

5.3.1.7.8 Maintainability 394
5.3.1.7.9 Survivability 395
5.3.1.7.10 Summary of LAN Requirements by Subscriber Mission .. 395

SECTION 5.3
IP-BASED CAPABILITIES AND FEATURES

Section 5.3 and its subsections describe requirements for IP-based UC products to be certified for use in the DISN in support of UC. As illustrated in Figure 5.3-1, requirements for IP-based products are spread across several subsections of UCR 2008. As an example, requirements for a LSC are specified in Sections 5.3.2, 5.3.4, 5.3.5, and 5.4.

Section 5.3.1 defines basic requirement for LAN products, and design guidance for an ASLAN; while IA requirements applicable to LAN products are found in UCR 2008, Section 5.4, IA Requirements.

Section 5.3.2 defines requirements for Assured Services. Assured Services are provided by replacing the current TDM-based Multilevel Precedence and Preemption (MLPP) functionality with IP-based ASLANs, ASAC, and AS-SIP signaling. The Assured Services requirements which must be met by the LSC, MFSS, Edge Boundary Controller (EBC), Customer Edge Router (CE), together with ASLAN and the end-to-end Network Infrastructure make up the total system required to initiate, supervise, and terminate voice and video sessions with precedence and preemption on an End Instrument (EI) to EI basis, while functioning within a converged total DoD Global Information Grid (GIG) network.

Section 5.3.3 defines end-to-end performance requirements for the GIG network infrastructure. The GIG end-to-end is defined in terms of three network segments referred to as CE, Network Edge, and Network Core Segments. The Core Segment DISN WAN consists of hundreds of worldwide Service Delivery Nodes (SDNs) interconnected by a highly robust, bandwidth rich optical fiber cross-connected core with gigabit routers (i.e., the DISN Core).

Section 5.3.4 defines requirements for the AS-SIP. The AS-SIP protocol is critical to provide assured services from EI to EI across the IP-based infrastructure.

The following sections use terms such as “appliance functions” and UC Products to be tested for APL certification. The term “appliance function” is introduced because IP-based APL products will often consist of software functions and features (e.g. appliances) that are distributed over several hardware components connected over a network infrastructure (e.g., LAN), while a Time Division Multiplexing (TDM)-based APL product such as an End Office (EO) consists of a single unit containing all required functions. Appliances operate at the signaling, bearer, and network management planes. Appliance functions are described or referred to throughout the UCR 2008, but are not considered products for APL certification, but rather functions and features that form parts of the UC APL products requirements defined in UCR 2008.

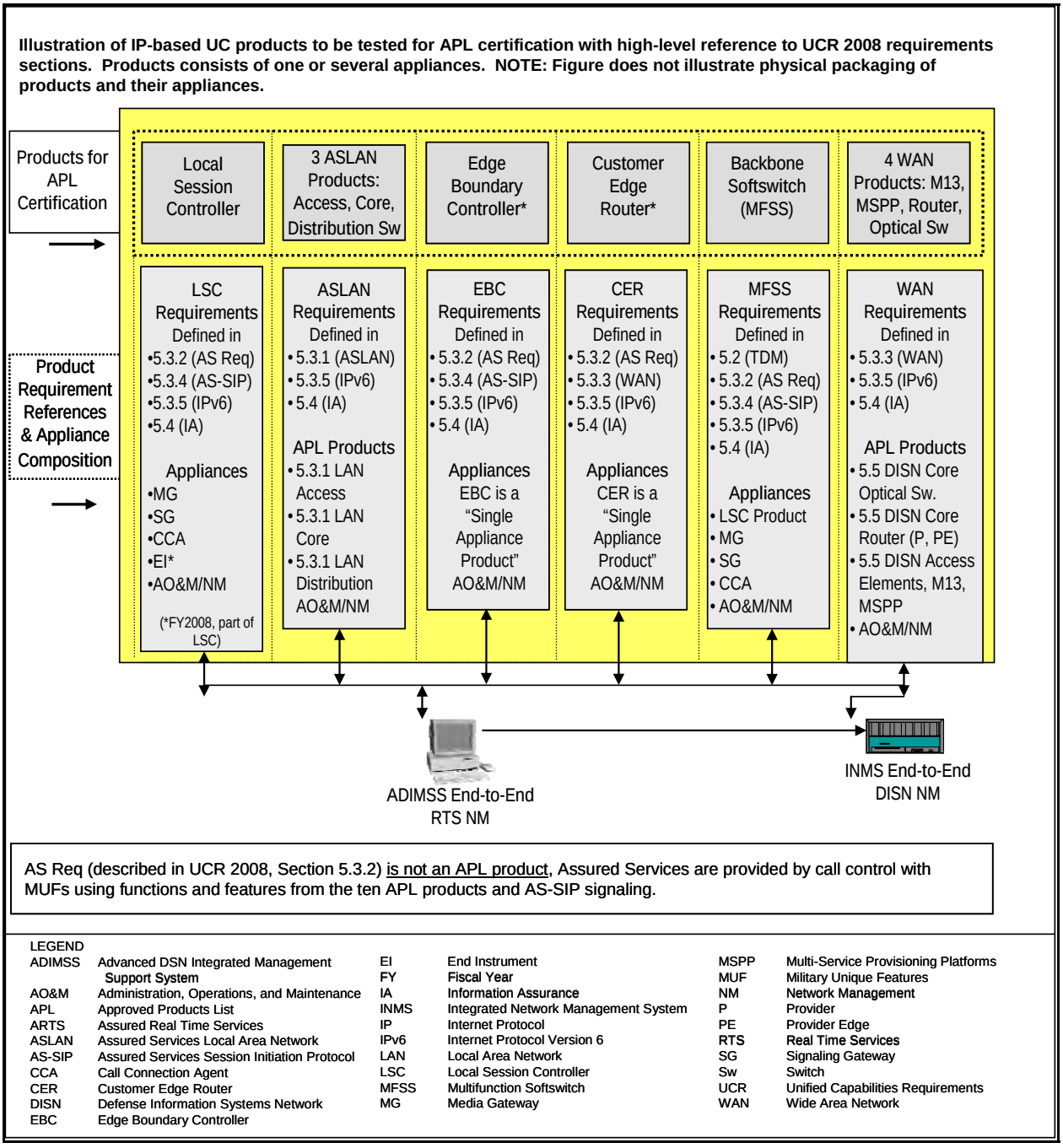


Figure 5.3-1. Illustration of How Requirements for IP-Based APL Products are Defined Across Multiple UCR 2008 Sections

Table 5.3-1 provides a partial listing of appliance functions and UC APL Products.

Table 5.3-1. Listing of Appliances and UC APL Products

ITEM	ITEM CATEGORY	ROLE AND FUNCTIONS
End Instrument	Appliance	Appliance part of LSC
Media Gateway	Appliance	Appliance function performing media conversion as part of the LSC and MFSS, and also in-band signaling conversion.
Signaling Gateway	Appliance	Appliance function performing signaling conversion between CCS7 and AS-SIP as part of the LSC and MFSS.
AS-SIP Signaling Appliance	Appliance	Appliance Function within an LSC and MFSS that provides AS-SIP signaling capabilities.
Call Connection Agent	Appliance	Appliance function within an LSC and MFSS that performs parts of session control and signaling functions.
Registrar	Appliance	Appliance function that stores the location of a registrant and its profile.
Registrant	Appliance	An appliance that is used to register with the network to seek and gain authority to invoke services or resources from the network.
LAN Switch/Routers: Access, Distribution, and Core Devices	APL Products	Three APL products used in ASLANs.
Secure End Instrument	APL Product	APL product providing secure RTS bearer service.
Local Session Controller	APL Product	APL product providing many local voice and video session control functions and features.
Multifunction Softswitch	APL Product	Large, complex APL product providing many local and WAN-related session controls and signaling functions.
Edge Boundary Controller	APL Product	APL product providing firewall functions.
Customer Edge Router	APL Product	APL product providing routing functions at the customer enclave boundary.
DISN WAN Access Device M13 Multiplexer	APL Product	APL product performing multiplexing of T1 carriers to T3 carriers.
DISN WAN Access Device Multi-Service Provisioning Platform	APL Product	APL Product providing the interface point to the DISN WAN for all customer legacy point-to-point services.
DISN WAN Router (Aggregation, Provider, Provider Edge Router)	APL product	APL Products performing routing of IP packets in the DISN WAN.
DISN Optical Switch	APL product	APL product serving as an optical transport node.

THIS PAGE INTENTIONALLY LEFT BLANK

5.3.1 Assured Services Local Area Network Infrastructure

5.3.1.1 Introduction

The UCR 2008, Assured Services Local Area Network Infrastructure (ASLAN), section establishes the requirements for the products used in LANs to support C2 and non-C2 IP-based communication services. The requirements, which are based on commercial standards, were developed to ensure availability of assured services capabilities to C2 users.

This section has two main purposes:

1. Define Product Requirements. Specifies the required and optional capabilities for network products that can be used in a LAN. This section is intended to support equipment certification.

2. Design Guidance. Provides design guidance for an ASLAN to meet its mission needs; provides introductory guidance on issues such as traffic engineering for performance (to ensure that an ASLAN can support the planned traffic and surges), availability (i.e., through high-reliability components and redundant components with automatic component failover), E2E performance requirements, and system administration and management.

5.3.1.1.1 IP Network Segments and LAN Nomenclature

The UCR 2008, Section 5.3.3, Network Infrastructure End-to-End Performance Requirements, describes the end-to-end network infrastructure as consisting of three network segments. The network segments are the Customer Edge, Network Edge, and Network Core. Figure 5.3.1-1, GIG End-to-End IP Network Infrastructure Segments, provides a high-level overview of the three-segment network infrastructure.

The Customer Edge Segment may consist of a single LAN or a Campus Area Network (CAN), or it may be implemented as a Metropolitan Area Network (MAN) in certain locations. The boundary for the Customer Edge Segment is the Customer Edge Router (CE Router), which is owned and maintained by the B/P/C/S. The Customer Edge Segment is connected to the Network Core Segment by the Network Edge Segment, which is a traffic-engineered bandwidth (IP connection) that connects the CE Router to an SDN. Detailed descriptions of the network segments and connection arrangements at an SDN are provided in UCR 2008, Section 5.3.3.1, End-to-End Network Infrastructure Description.

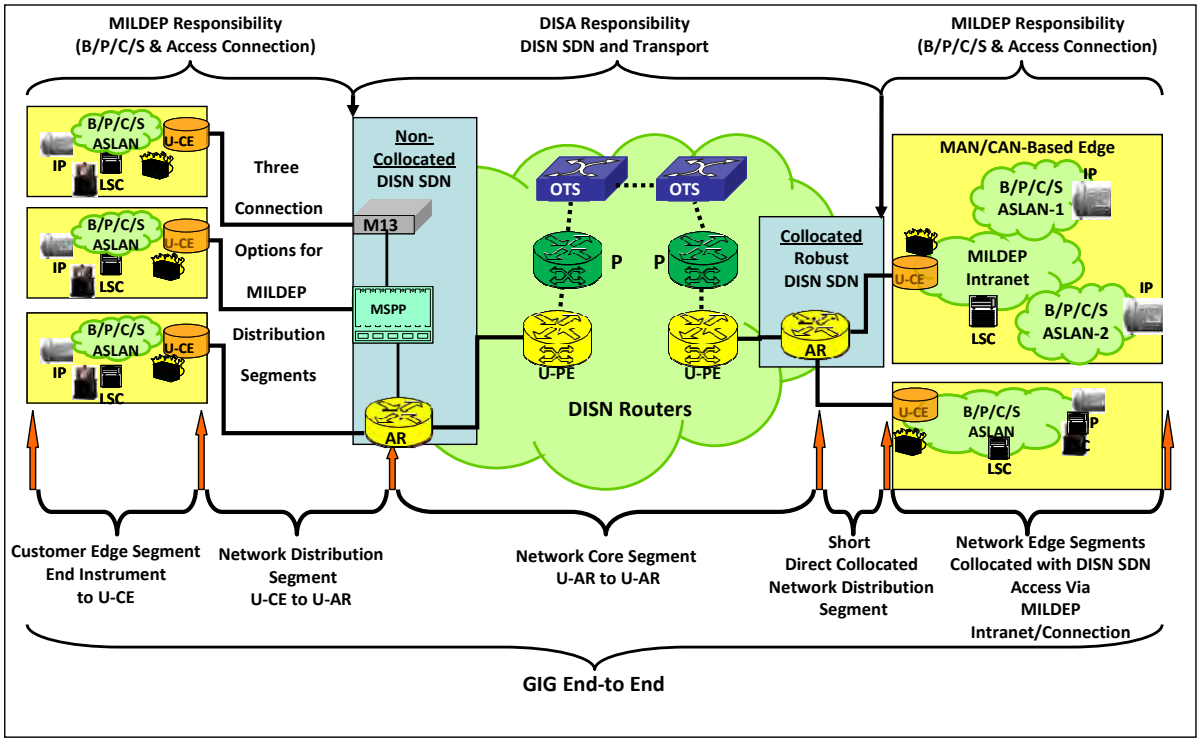


Figure 5.3.1-1. GIG End-to-End IP Network Infrastructure Segments

The LAN consists of the Core, Distribution, and Access Layers, which all reside in the Customer Edge Segment of the end-to-end GIG network reference. A high-level illustration of the three LAN Layers is provided in Figure 5.3.1-2, B/P/C/S LAN Layers and Relationship to Customer Edge Segment.

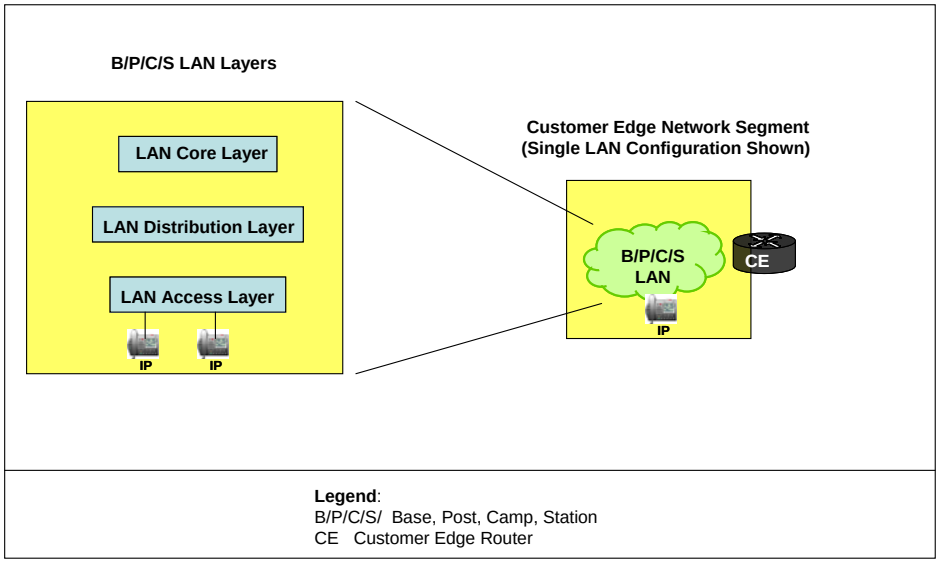


Figure 5.3.1-2. B/P/C/S LAN Layers and Relationship to Customer Edge Network Segment

5.3.1.2 Overview of LAN General Design and Requirements

To provide cost-effective LAN solutions that meet mission requirements for all users served by a LAN, two types of LANs are defined; they are ASLANs and non-ASLANs. The LANs will be designed to meet traffic engineering and redundancy requirements, as required by applicable mission needs. ASLANs and non-ASLANs may be designed to use any combination of the layers and functional capabilities, shown in Figure 5.3.1-3, LAN Layers. Multiple layers may be combined in a single switch or router (i.e., router acts as Distribution and Access Layers).

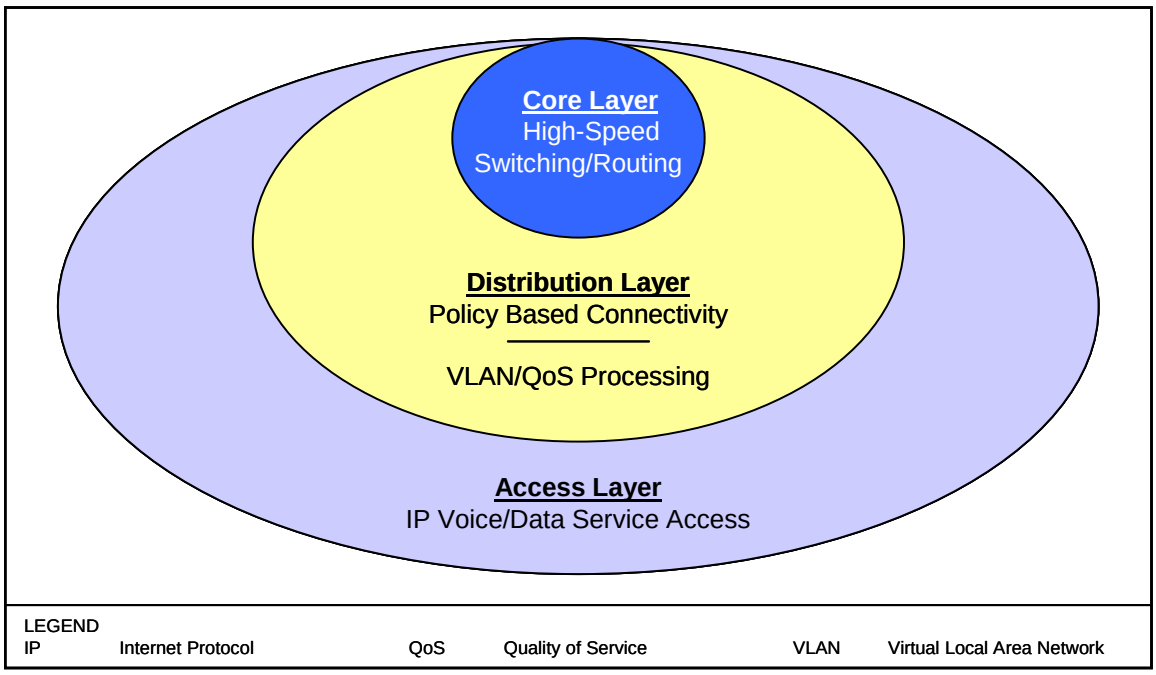


Figure 5.3.1-3. LAN Layers

The three LAN layers are as follows:

1. Access Layer. The Access Layer is the point at which local end users are allowed into the network. This layer may use access lists or filters to optimize further the needs of a particular set of users.

2. Distribution Layer. The Distribution Layer of the network is the demarcation point between the Access and Core Layers and helps to define and differentiate the Core. The purpose of this layer is to provide boundary definition and is the place at which packet manipulation can take place.

3. Core Layer. The Core Layer is a high-speed switching backbone and is designed to switch packets as fast as possible.

Figure 5.3.1-4, Representative B/P/C/S Design and Terminology, illustrates a typical B/P/C/S LAN design. The LAN design and requirements refer to LAN products in terms of the Core, Distribution, and Access Layer products. These products are often known by other names such as Main Communication Node (MCN), Area Distribution Node (ADN), and End User Building (EUB) switch.

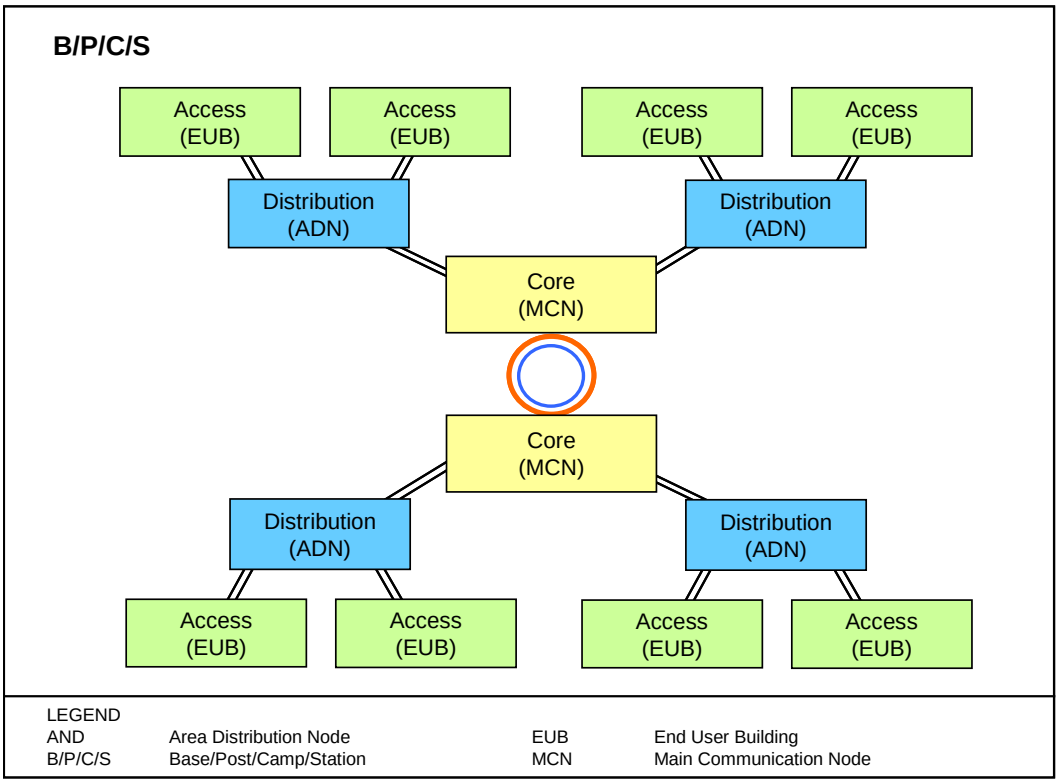


Figure 5.3.1-4. Representative B/P/C/S Design and Terminology

Within the LAN, the terminology used to reference traffic at each specific Open Systems Interconnect (OSI) layer is shown in Table 5.3.1-1, OSI Layer Control Information Name.

Table 5.3.1-1. OSI Layer Control Information Name

OSI LAYER	CONTROL INFORMATION NAME
Application Presentation Session	Data
Transport	Segment
Network	Packet
Data Link	Frame
Physical	Bit
LEGEND OSI Open Systems Interconnect	

5.3.1.2.1 LAN Types and Mission Support Summary

The LAN requirements are driven primarily by the types of users they support. To provide cost-effective LAN solutions that meet mission requirements, two types of LANs have been defined: the ASLAN and the non-ASLAN. Within the ASLAN type, there are two categories: high availability ASLANs and medium availability ASLANs. Table 5.3.1-2 outlines the types of LANs that may support voice and video traffic by subscriber mission categories.

Table 5.3.1-2. Summary of LAN Types by Subscriber Mission

REQUIREMENT ITEM	SUBSCRIBER MISSION CATEGORY			
	SPECIAL C2	C2	C2(R)	NON-C2
ASLAN high	R	P	P	P
ASLAN medium	NP	P	P	P
Non-ASLAN	NP	NP	P	P
MLPP	R	R	R	NR
Diversity	R	R	NR	NR
Redundancy	R	R	NR	NR
Battery Backup	8 hours	2 hours	NR	NR
Single Point of Failure user > 96 allowed	No	No	Yes	Yes
LAN GOS p=	0.0	0.0	0.0	N/A
Availability	99.999	99.997	99.9	99.9

LEGEND

ASLAN	Assured Services LAN	NP	Not Permitted
C2	Command and Control	NR	Not Required
C2(R)	C2 Routine	p	Probability of Blocking
GOS	Grade of Service	P	Permitted
LAN	Local Area Network	R	Required
MLPP	Multilevel Precedence and Preemption		

5.3.1.3 General Performance Parameters

[Required: Core, Distribution, and Access Products] The Core, Distribution, and Access products shall be capable of meeting the following parameters:

1. Non-Blocking. All Core, Distribution, and Access products shall be non-blocking for a minimum of 50 percent (maximum voice and video traffic) of its maximum rated output capacity. Non-blocking is defined as the capability to send and receive 64 to 1518 byte packets at full duplex rates from ingress ports to egress ports without losing any packets.

2. Latency. All Core, Distribution, and Access products shall have the capability to transport prioritized voice and video packets (media and signaling), with no more than 2 milliseconds (ms) latency for Core and Distribution products, and 1 ms latency for Access

products. The latency shall be achievable over any 5-minute period measured from ingress ports to egress ports under congested conditions.

3. Jitter. All Core, Distribution, and Access products shall have the capability to transport prioritized voice and video packets (media and signaling) with no more than 1 ms jitter across Core and Distribution products, and 1 ms across Access products. The jitter shall be achievable over any 5-minute period measured from ingress ports to egress ports under congested conditions.

4. Packet Loss. All Core, Distribution, and Access products shall have the capability to transport prioritized voice and video packets (media and signaling) with no more than 0.02 percent packet loss for Core and Distribution products. Access products shall have the capability to transport prioritized voice and video packets with no more than 0.01 percent packet loss. The packet loss shall be achievable over any 5-minute period measured from ingress ports to egress ports under congested conditions.

5. Bit Error Rate (BER). All Core, Distribution, and Access products shall have the capability to transport prioritized voice and video packets (media and signaling) with a BER of no more than 1 bit error in 10^6 bits. The BER shall be achievable over any 5-minute period measured from ingress ports to egress ports under congested conditions.

5.3.1.3.1 Port Interface Rates

[Required: Core and Distribution Products] Minimally, Core and Distribution products shall support the following interface rates:

- 100 megabits per second (Mbps) IAW IEEE 802.3u
- 1 gigabit per second (Gbps) IAW IEEE 802.3z

[Required: Access Products] Minimally, Access products shall provide the following interface rates:

- 10 Mbps IAW IEEE 802.3i
- 100 Mbps IAW IEEE 802.3u

[Conditional: Core, Distribution, and Access Products] The Core, Distribution, and Access products may provide the following interface rate:

- 10 Gbps IAW IEEE 802.3ae

[Conditional: Core, Distribution, and Access Products] The Core, Distribution, and Access products may provide the following wireless LAN interface rates:

- 54 Mbps IAW IEEE 802.11a
- 11 Mbps IAW IEEE 802.11b
- 54 Mbps IAW IEEE 802.11g
- IEEE 802.16 – Broadband wireless communications standards for MANs

[Conditional] If any of the above wireless interfaces are provided, the interfaces must support the requirements of Section 5.3.1.7.2, Wireless.

5.3.1.3.2 Port Parameter Requirements

[Required: Core, Distribution, and Access Products] The Core, Distribution, and Access products shall provide the following parameters on a per port basis:

- Auto-negotiation IAW IEEE 802.3
- Force mode IAW IEEE 802.3
- Flow control IAW IEEE 802.3x
- Filtering IAW RFC 1812
- Link Aggregation IAW IEEE 802.3ad (output/egress ports only)
- Spanning Tree Protocol IAW IEEE 802.1D
- Multiple Spanning Tree IAW IEEE 802.1s
- Rapid Reconfiguration of Spanning Tree IAW IEEE 802.1w
- Port-Based Access Control IAW IEEE 802.1x

5.3.1.3.3 Class of Service Markings

[Required: Core, Distribution, and Access Products] The Core, Distribution, and Access products shall support Differentiated Services Code Points (DSCPs) IAW RFC 2474 as follows:

1. The Core, Distribution, and Access products shall be capable of accepting any packet tagged with a DSCP (0-63) on an ingress port and assign that packet to a QoS behavior listed in UCR 2008, Section 5.3.1.3.6, Quality of Service Features.

2. The Core, Distribution, and Access products shall be capable of accepting any packet tagged with a DSCP (0-63) on an ingress port and reassign that packet to any new DSCP value (0-63). Default DSCPs are provided in Table 5.3.1-3.

Table 5.3.1-3. Default DSCPs

NO.	AGGREGATE SERVICE CLASS	GRANULAR SERVICE CLASS	DEFAULT DSCPs		
			BASE 2	BASE 10	BASE 16[3]
1	Control	Network Control	110 000-111 000	48-56	0xC0 - 0xE0
2	Inelastic/ Real-Time	User Signaling[1]	101 000-101 111	40-47	0xA0 - 0xBC
		Circuit Emulation[1]			
		Short messages[1]			
		Voice[2]			
		Video/VTC	100 000-100 111	32-39	0x80 - 0x9C
		Streaming	011 000-011 111	24-31	0x60 - 0x7C
3	Preferred Elastic	Interactive Transactions	010 000-010 111	16-23	0x40 - 0x5C
		File Transfers	001 000-001 111	8-15	0x20 - 0x3C
4	Elastic	Default	000 000-000 111	0-7	0x0 - 0x1C

NOTES
1. All user signaling (voice and video) may be grouped into this granular service class. User signaling, circuit emulation, and short messages may use the same DSCP.
2. Voice traffic must be differentiated with a different DSCP from user signaling, circuit emulation, and short messages.
3. DSCP Hexadecimal (Base 16) values assume last two bits of the 8 bit field to be 00.

- Specific DSCPs for each precedence level are contained in UCR 2008, Section 5.3.3, Network Infrastructure End-to-End Performance Requirements.
- Definitions of granular service classes are provided in UCR 2008, Section 5.3.3, Network Infrastructure End-to-End Performance Requirements.

LEGEND
DSCP Differentiated Services Code Point
No. Number
UCR Unified Capabilities Requirements
VTC Video Teleconferencing

3. The Core, Distribution, and Access products must be able to support the prioritization of aggregate service classes described in Table 5.3.1-4, Traffic Prioritizations. Traffic Prioritizations Prioritized service classes shall be queued according to UCR 2008, Section 5.3.1.3.6, Quality of Service Features.

Table 5.3.1-4. Traffic Prioritizations

NO.	AGGREGATE SERVICE CLASS	GRANULAR SERVICE CLASS	PRIORITY
1	Control	Network Control	1
2	Inelastic/ Real-Time	User Signaling	2
		Circuit Emulation	2
		Short messages	2
		Voice	3
		Video/VTC	4
		Streaming	5
3	Preferred Elastic	Interactive Transactions and OA&M	6
		File Transfers and OA&M	7
4	Elastic	Default	Best Effort

LEGEND
No. Number
OA&M Operations, Administration and Management
VTC Video Teleconferencing

[Conditional: Core, Distribution, and Access Products] The Core, Distribution, and Access products may support the 3-bit user priority field of the IEEE 802.1Q 2-byte Tag Control Information (TCI) field (see Figure 5.3.1-5, IEEE 802.1Q Tagged Frame for Ethernet, and Table 5.3.1-7, TCI Field Description). Default values are provided in Table 5.3.1-5, 802.1Q Default Values.

If provided, the following CoS requirements apply:

1. The Core, Distribution, and Access products shall be capable of accepting any frame tagged with a user priority (0-7) on an ingress port and assign that frame to a QoS behavior listed in UCR 2008, Section 5.3.1.3.6, Quality of Service Features.

2. The Core, Distribution, and Access products shall be capable of accepting any frame tagged with a user priority (0-7) on an ingress port and reassign that frame to any new user priority value (0-7).

5.3.1.3.4 Virtual LAN Capabilities

[Required: Core, Distribution, and Access Products] The Core, Distribution, and Access products shall be capable of the following:

Table 5.3.1-5. 802.1Q Default Values

NO.	AGGREGATE SERVICE CLASS	GRANULAR SERVICE CLASS	DEFAULT 802.1Q COS TAG	
			BASE 2	BASE 10
1	Control	Network Control	111	7
2	Inelastic/ Real-Time	User Signaling[1]	110	6
		Circuit Emulation[1]	110	6
		Short messages[1]	110	6
		Voice[2]	101	5
		Video/VTC	100	4
		Streaming	011	3
3	Preferred Elastic	Interactive Transactions OA&M – SNMP	010	2
		File Transfers OA&M – Trap/SysLog	001	1
4	Elastic	Default	000	0

NOTES
1. All user signaling (voice and video) may be grouped into this granular service class. User signaling, circuit emulation, and short messages may use the same TCI tag.
2. Voice traffic must be differentiated with a different TCI tag from user signaling, circuit emulation, and short messages.

LEGEND

802.1Q	IEEE VLAN/User Priority Specification	SNMP	Simple Network Management Protocol
CoS	Class of Service	SysLog	System Log
OA&M	Operations, Administration, and Maintenance	TCI	Tag Control Information
		VTC	Video Teleconferencing

1. Accepting VLAN tagged frames according to IEEE 802.1Q (see Figure 5.3.1-5, IEEE 802.1Q Tagged Frame for Ethernet, and Figure 5.3.1-6, TCI Field Description).

2. Configuring VLAN IDs (VIDs). VIDs on an ingress port shall be configurable to any of the 4094 values (except 0 and 4095).

3. Supporting port-based VLANs, Media Access Control (MAC) address-based VLANs, and protocol-based VLANs.

5.3.1.3.5 Protocols

[Required: Core, Distribution, and Access Products] The Core, Distribution, and Access products shall meet the DoD Information Technology Standards Registry (DISR) protocol requirements for IPv4 and IPv6.

BYTES								
7	1	6	6	2	2	2	42-1496	4
Preamble	SFD	DA	SA	TPID	TCI	Type Length	Data	CRC

NOTE: The TCI field includes user priority, CFI, and VLAN ID.

LEGEND

CFI	Canonical Format Indicator	SFD	Start Delimiter Frame
CRC	Cyclic Redundancy Check	TCI	Tag Control Information
DA	Destination Address	TPID	Tag Protocol Identification
SA	Source Address	VLAN	Virtual Local Area Network

Figure 5.3.1-5. IEEE 802.1Q Tagged Frame for Ethernet

BITS		
3	1	12
User Priority	CFI	VID

NOTES
1. **User Priority**. Defines eight (23) user priority levels. Access devices must be capable of recognizing the user priorities (0-7) and assign them to the QoS mechanisms listed below.
2. **CFI**. Always set to zero for Ethernet switches. CFI is used for compatibility reasons between Ethernet type network and Token Ring type network. If a frame received at an Ethernet port has a CFI set to 1, then that frame should not be forwarded as it is to an untagged port.
3. **VID**. Has 12 bits and allows the identification of 4096 (212) VLANs. Of the 4096 possible VIDs, a VID of 0 is used to identify priority frames and value 4095 (FFF) is reserved, so the maximum possible VLAN configurations are 4094.

LEGEND

CFI	Canonical Format Indicator	VID	Virtual Identification
QoS	Quality of Service	VLAN	Virtual Local Area Network

Figure 5.3.1-6. TCI Field Description

5.3.1.3.6 Quality of Service Features

[Required: Core, Distribution, and Access Products] The Core, Distribution, and Access products shall be capable of the following QoS features:

1. Providing a minimum of four (4) queues (see Figure 5.3.1-7).

2. Assigning any “tagged” session to any of the queues.

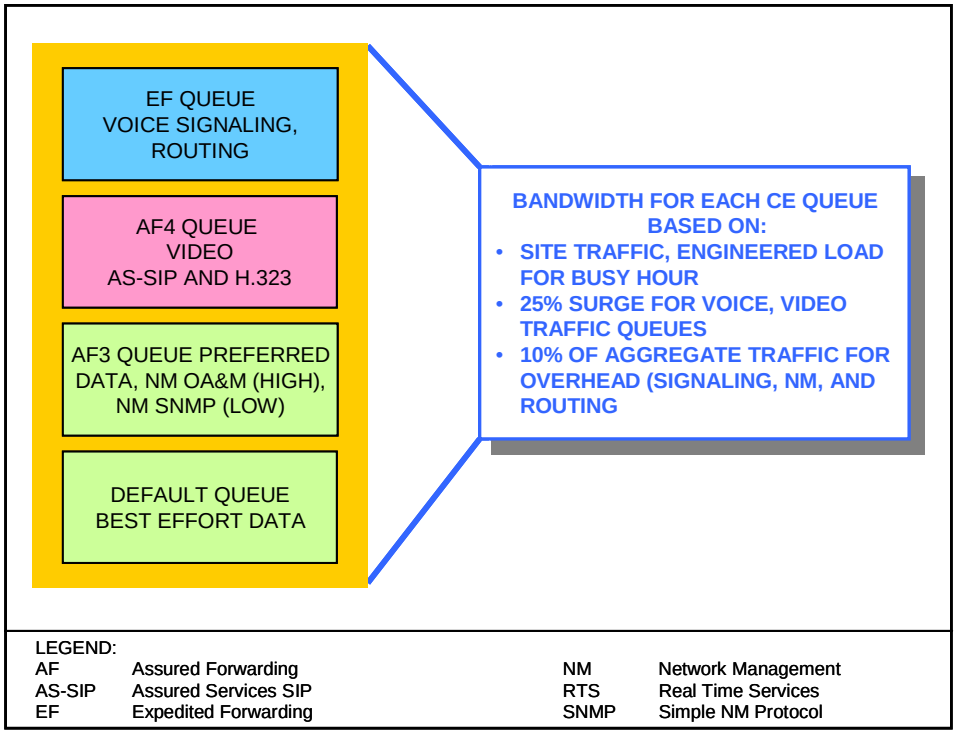


Figure 5.3.1-7. 4-Queue Design

3. Supporting Differentiated Services (DiffServ) per hop behaviors (PHBs) per RFCs 2474, 2494, 2597, 2598, and 3246.

    a. Expedited Forwarding (EF)
    b. Assured Forwarding (AF)
    c. Best Effort (BE)
    d. Class Selector (CS)

4. Supporting a minimum of one of the following:

    a. Weighted Fair Queuing (WFQ) IAW RFC 3662
    b. Priority Queuing (PQ) IAW RFC 1046
    c. Class-Based WFQ IAW RFC 3366

5. All queues shall be capable of having a bandwidth (BW) assigned (i.e., queue 1: 200 kbps, queue 2: 500 kbps, etc.) or percentage of traffic (queue 1: 25 percent, queue 2: -25 percent, etc.).

5.3.1.3.7 Network Monitoring

[Required: Core, Distribution, and Access Products] The Core, Distribution, and Access products shall support the following network monitoring features:

- Simple Network Management Protocol (SNMP) IAW RFCs 1157, 2206, 3410, 3411, 3412, 3413, and 3414
- SNMP Traps IAW RFC 1215
- Remote Monitoring (RMON) IAW RFC 2819
- Coexistence between Version 1, Version 2, and Version 3 of the Internet-standard Network Management Framework IAW RFC 3584
- The Advanced Encryption Standard (AES) Cipher Algorithm in the SNMP User-based Security Model IAW RFC 3826

5.3.1.3.8 Security

[Required: Core, Distribution, and Access Products] The Core, Distribution, and Access products shall meet the security protocol requirements listed in UCR 2008, Section 5.4, Information Assurance Requirements.

5.3.1.3.9 Product Requirements Summary

Table 5.3.1-6, Core, Distribution, and Access Product Requirements Summary, summarizes product requirements.

Table 5.3.1-6. Core, Distribution, and Access Product Requirements Summary

REQUIREMENTS	FEATURES	REFERENCES	APPLICABILITY		
			C	D	A
Physical Ports	Serial Port	EIA/TIA	R	R	R
	10BaseT UTP	IEEE 802.3i	C	C	R
	100BaseT UTP	IEEE 802.3u	R	R	R
	100Base-FX	IEEE 802.3u	R	R	R
	1000Base-T UTP	IEEE 802.3ab	C	C	C
	1000Base-X Fiber	IEEE 802.3z	R	R	C
	10GBase-X	IEEE 802.3ae	C	C	C
Port Parameters	Auto-negotiation	IEEE 802.3	R	R	R
	Force Mode	IEEE 802.3	R	R	R

REQUIREMENTS	FEATURES	REFERENCES	APPLICABILITY		
			C	D	A
	Flow Control	IEEE 802.3x	R	R	R
	Filtering	RFC 1812	R	R	R
	Link Aggregation	IEEE 802.3ad	R	R	R
	Spanning Tree Protocol	IEEE 802.1D	R	R	R
	Multiple Spanning Tree Protocol	IEEE 802.1s	R	R	R
	Rapid Reconfiguration of Spanning Tree	IEEE 802.1w	R	R	R
	Port Based Access Control	IEEE 802.1x [1]	R	R	R
Traffic Prioritization	CoS Traffic Classes	IEEE 802.1D/Q	C	C	C
	DSCP	RFC 2474	R	R	R
VLANs	Port based	IEEE 802.1Q	R	R	R
	MAC based	IEEE 802.1Q	R	R	R
	Protocol based	IEEE 802.1Q	R	R	R
IPv4 Protocols	IPv4 requirements are contained within the DISR on-line RTS profiles for Core, Distribution, and Access products.	DISR	R	R	R
IPv6 Protocols	See IPv6 profiles contained in the DISR	DISR	R	R	R
QoS	DiffServ PHBs	RFCs 3246, 2597	R	R	R
	Minimum 4 hardware queues	DoD CoS/QoS WG	R	R	R
	FIFO	RFC 3670	C	C	C
	WFQ	RFC 3662	C[2]	C[2]	C[2]
	CQ	RFC 3670	C[2]	C[2]	C[2]
	PQ	RFC 1046	C[2]	C[2]	C[2]
	CB-WFQ	RFC 3366	C[2]	C[2]	C[2]
Security	Security requirements are contained in the IA portion of the document.		R	R	R

NOTES
1 Only between end-user and product; not trunks.
2. One of these queuing mechanisms is required to implement EF PHB.

LEGEND

C	Conditional	MAC	Media Access Control
CB-WFQ	Class-Based Weighted Fair Queuing	PHB	Per Hop Behavior
CoS	Class of Service	PQ	Priority Queuing
CQ	Custom Queuing	R	Required
DiffServ	Differentiated Services	RFC	Request For Comment
DISR	DoD Information Technology Standards Registry	RMON	Remote Monitoring
EF	Expedited Forwarding	RTS	Real Time Services
EIA	Electronics Industries Alliance	TIA	Telecommunications Industry Association
FIFO	First-in First-out	UTP	Unshielded Twisted Pair
IEEE	Institute of Electrical and Electronic Engineers Inc.	VLAN	Virtual LAN
IPv4	IP version 4	WFQ	Weighted Fair Queuing
IPv6	IP version 6		

5.3.1.4 End-to-End Performance Requirements

End-to-end performance across a LAN is measured from the traffic ingress point (typically, the LAN Access product input port) to the traffic egress port (typically, the LAN Core product port connection to the CE Router).

5.3.1.4.1 Voice Services

5.3.1.4.1.1 Latency

[Required: ASLAN and Non-ASLAN] The LAN shall have the capability to transport voice IP packets, media and signaling, with no more than 5 ms latency end-to-end across the ASLAN as measured under congested conditions. Congested condition is defined as 100 percent of link capacities. The latency shall be achievable over any 5-minute measured period under congested conditions.

5.3.1.4.1.2 Jitter

[Required: ASLAN and Non-ASLAN] The LAN shall have the capability to transport voice IP packets end-to-end with no more than 3 ms of jitter. The jitter shall be achievable over any 5-minute measured period under congested conditions. Congested condition is defined as 100 percent of link capacities.

5.3.1.4.1.3 Packet Loss

[Required: ASLAN and Non-ASLAN] The LAN shall have the capability to transport voice IP packets end-to-end with packet loss not to exceed configured traffic engineered (queuing) parameters. The packet loss shall be achievable over any 5-minute measured period under congested conditions. Congested condition is defined as 100 percent of link capacities.

5.3.1.4.1.4 Bit Error Rate

[Required: ASLAN and Non-ASLAN] The LAN shall have the capability to transport voice IP packets end-to-end with a BER of no more than 3 bit errors in 10^6 bits. The BER shall be achievable over any 5-minute measured period under congested conditions. Congested condition is defined as 100 percent of link capacities.

5.3.1.4.2 Video Services

5.3.1.4.2.1 Latency

[Required: ASLAN and Non-ASLAN] The LAN shall have the capability to transport video IP packets with no more than 35 ms latency end-to-end across the LAN. Latency is increased over voice IP packets because of the increased size of the packets (230 bytes for voice packets and up to 1518 bytes for video). The latency shall be achievable over any 5-minute measured period under congested conditions. Congested condition is defined as 100 percent of link capacities.

5.3.1.4.2.2 Jitter

[Required: ASLAN and Non-ASLAN] The LAN shall have the capability to transport video IP packets end-to-end with no more than 30 ms of jitter. The jitter shall be achievable over any 5-minute measured period under congested conditions. Congested condition is defined as 100 percent of link capacities.

5.3.1.4.2.3 Packet Loss

[Required: ASLAN and Non-ASLAN] The LAN shall have the capability to transport video IP packets end-to-end with packet loss not to exceed configured traffic engineered (queuing) parameters. The packet loss shall be achievable over any 5-minute measured period under congested conditions. Congested condition is defined as 100 percent of link capacities.

5.3.1.4.2.4 Bit Error Rate

[Required: ASLAN and Non-ASLAN] The LAN shall have the capability to transport video IP packets end-to-end with a BER of no more than 3 bit errors in 10^6 bits. The error rate shall be achievable over any 5-minute measured period under congested conditions. Congested condition is defined as 100 percent of link capacities.

5.3.1.4.3 Data Services

5.3.1.4.3.1 Latency

[Required: ASLAN and Non-ASLAN] The LAN shall have the capability to transport prioritized data IP packets with no more than 50 ms latency end-to-end across the ASLAN. Latency is increased over voice IP packets because of the increased size of the packets (230 bytes for voice packets and up to 1518 bytes for data). The latency shall be achievable over any

5-minute measured period under congested conditions. Congested condition is defined as 100 percent of link capacities.

5.3.1.4.3.2 Jitter

There are no jitter requirements for data IP packets.

5.3.1.4.3.3 Packet Loss

[Required: ASLAN and Non-ASLAN] The LAN shall have the capability to transport prioritized data IP packets end-to-end with packet loss not to exceed configured traffic engineered (queuing) parameters. The packet loss shall be achievable over any 5-minute period measured under congested conditions. Congested condition is defined as 100 percent of link capacities.

5.3.1.4.3.4 Bit Error Rate

[Required: ASLAN and Non-ASLAN] The LAN shall have the capability to transport prioritized data IP packets end-to-end with a BER of no more than 3 bit error in 10^6 bits.

5.3.1.5 Information Assurance Requirements

[Required: ASLAN and Non-ASLAN] All LAN infrastructure components must be IA certified to be placed on the APL. The IA requirements are contained in UCR 2008, Section 5.4, Information Assurance Requirements.

5.3.1.6 LAN Network Management Requirements

[Required: ASLAN and Non-ASLAN] Network managers must be able to monitor, configure, and control all aspects of the network and observe changes in network status. The LAN infrastructure components shall have an NM capability that leverages existing and evolving technologies and has the ability to perform remote network product configuration/ reconfiguration of objects that have existing DoD GIG management capabilities. The LAN infrastructure components must be able to be centrally managed by an overall network management system (NMS). In addition, both NMS (RMON2) and (MIB II) shall be supported for SNMP. In addition, if other methods are used for interfacing between LAN products and the NMS they shall be implemented in a secure manner, such as with the following methods:

1. Secure Shell 2 (SSH2). The SSH2 protocol shall be used instead of Telnet due to its increased security. The LAN products shall support RFC 4251 through RFC 4254 inclusive.

2. HyperText Transfer Protocol, Secure (HTTPS). HTTPS shall be used instead of HTTP due to its increased security as described in RFC 2660. The LAN products shall support RFC 2818.

5.3.1.6.1 Configuration Control

[Required: ASLAN and Non-ASLAN] Configuration Control identifies, controls, accounts for, and audits all changes made to a site or information system during its design, development, and operational life cycle (DoD CIO Guidance IA6-8510 IA). LANs shall have an NM capability that leverages existing and evolving technologies and has the ability to perform remote network product configuration/reconfiguration of objects that have existing DoD GIG management capabilities. The NMS shall report configuration change events in near real time (NRT), whether or not the change was authorized. The system shall report the success or failure of authorized configuration change attempts in NRT. NRT is defined as within 5 seconds of detecting the event, excluding transport time.

5.3.1.6.2 Operational Changes

[Required: ASLAN and Non-ASLAN] LAN infrastructure components must provide metrics to the network management (NM) system to allow them to make decisions on managing the network. NMSs shall have an automated NM capability to obtain the status of networks and associated assets in NRT 99 percent of the time (with 99.9 percent as an Objective Requirement). NRT is defined as within 5 seconds of detecting the event, excluding transport time.

5.3.1.6.3 Performance Monitoring

[Required: ASLAN and Non-ASLAN] All LAN components shall be capable of providing status changes 99 percent of the time (with 99.9 percent as an Objective Requirement) by means of an automated capability in NRT. An NMS will have an automated NM capability to obtain the status of networks and associated assets 99 percent of the time (with 99.9 percent as an Objective Requirement) within 5 seconds of detecting the event, excluding transport. The NMS shall collect statistics and monitor bandwidth utilization, delay, jitter, and packet loss.

5.3.1.6.4 Alarms

[Required: ASLAN and Non-ASLAN] All LAN components shall be capable of providing SNMP alarm indications to an NMS. Network Management Systems will have the NM capability to perform automated fault management of the network, to include problem detection, fault correction, fault isolation and diagnosis, problem tracking until corrective actions are completed, and historical archiving. This capability allows network managers to monitor and maintain the situational awareness of the network's manageable products automatically, and to

become aware of network problems as they occur based on the trouble tickets generated automatically by the affected object or network. Alarms will be correlated to eliminate those that are duplicate or false, initiate test, and perform diagnostics to isolate faults to a replaceable component. Alarms shall be reported as TRAPs via SNMP in NRT. More than 99.95 percent of alarms shall be reported in NRT. NRT is defined as within 5 seconds of detecting the event, excluding transport time.

5.3.1.6.5 Reporting

[Required: ASLAN and Non-ASLAN] To accomplish GIG end-to-end situational awareness, an NMS will have the NM capability of automatically generating and providing an integrated/ correlated presentation of network and all associated networks.

5.3.1.7 Engineering Requirements

5.3.1.7.1 Physical Media

[Required: ASLAN and Non-ASLAN] Wires used for the LAN shall not be lower than a CAT-5 performance (see Table 5.3.1-7, Cable Grade Capabilities). The CAT-5 cable specification is rated up to 100 megahertz (MHz) and meets the requirement for high-speed LAN technologies, such as Fast Ethernet and Gigabit Ethernet. The Electronics Industry Association/Telecommunications Industry Association (EIA/TIA) formed this cable standard that describes performance the LAN manager can expect from a strand of twisted pair copper cable. Along with this specification, the committee formed the EIA/TIA-568-B standard named the "Commercial Building Telecommunications Cabling Standard" to help network managers install a cabling system that would operate using common LAN types, like Fast Ethernet. The specification defines Near End Crosstalk (NEXT) and attenuation limits between connectors in a wall plate to the equipment in the closet.

5.3.1.7.2 Wireless

[Conditional: ASLANs or Non-ASLANs]

Wireless LAN implementations are considered as extensions of the physical layer. This section outlines the requirements when using wireless Ethernet technologies in a LAN to provide VoIP service to subscribers. In particular, this section defines four wireless areas that may apply to VoIP subscribers: Wireless End Instruments (WEIs), Wireless LAN Access System (WLAS), Wireless Access Bridges (WABs), and general requirements for wireless LANs (WLANs). For LANs supporting VoIP subscribers, wireless transport may only be used:

Table 5.3.1-7. Cable Grade Capabilities

CABLE NAME	MAKEUP	FREQUENCY SUPPORT	DATA RATE	NETWORK COMPATIBILITY
CAT-5	4 twisted pairs of copper wire -- terminated by RJ45 connectors	100 MHz	Up to 1000 Mbps	ATM, Token Ring, 1000Base-T, 100Base-TX, 10Base-T
CAT-5e	4 twisted pairs of copper wire -- terminated by RJ45 connectors	100 MHz	Up to 1000 Mbps	10Base-T, 100Base-TX, 1000Base-T
CAT-6	4 twisted pairs of copper wire -- terminated by RJ45 connectors	250 MHz	1000 Mbps	10Base-T, 100Base-TX, 1000Base-T

LEGEND

ATM	Asynchronous Transfer Mode	MHz	Megahertz
Base	Baseband	RJ	Registered Jack
CAT	Category	T	Ethernet half-duplex
Mbps	Megabits per second	TX	Ethernet full-duplex

- Between EIs and a WLAN to provide Access layer functionality (i.e., wired Distribution and Core layers)

- Between two or more LANs as a “bridge” technology

The components of a wireless network are certified along with an ASLAN, while wireless VoIP devices are certified with the VoIP solution.

The requirements for each of the wireless technologies (i.e., WEIs, WLAS, WABs, and WLANs) are contained in the following sections.

5.3.1.7.2.1 General Wireless Product Requirements

[Required: WLANs] The following general wireless requirements must be met by WLANs and WLAN components:

1. If an IP interface is provided in any of the wireless components, then it shall meet the IP requirements detailed in the DISR UCR 2008 IPv6 Requirements.

2. 802.11 wireless products must be WiFi Alliance Certified.

3. Wireless networks may support C2, C2(R), and Non-C2 users, but shall not be used to support special C2 users.

4. For wireless products that provide transport to more than 96 telephony users, the wireless products shall provide redundancy and WLAS and/or associated WLAN

controller/switches that provide and/or control voice services to more than 96 WEIs shall provide redundancy through either:

a. Single Product Redundancy. Shall have the following as a minimum: Dual power supplies/processors /radio systems/Ethernet ports; redundancy protocol; and no single point of failure for more than 96 subscribers.

b. Dual Product Redundancy. Shall be collocated or coadjacent and shall have the following as a minimum: Traffic engineering to support all users on a single product upon failure of the other product. Secondary product may be on full standby or traffic sharing, supporting 50 percent of the traffic prior to failure rollover.

5. All wireless connections shall be Federal Information Processing Standard (FIPS) 140-2 Level 1 certified (connections may either be WEI to WLAS if both support FIPS 140-2 Level 1, or WEI to a FIPS 140-2 compliant product through a WLAS if the WLAS is not capable of FIPS 140-2 Level 1). Wireless products that comprise the WLAN shall be secured in accordance with their wireless security profile as follows:

a. FIPS 140-2, Level 1. Wireless components must be operated from within a "limited access, secure room" and be under user positive control at all times. However, if the wireless end item is designed to be left unattended, such as a wireless free-standing desk telephone, then that wireless end item must be Level 2 compliant.

b. FIPS 140-2, Level 2. Wireless components can be operated in an open public area such as an "open hallway," but recommend the use of a "limited access, secure room" if available and/or operationally feasible.

6. The use of wireless in the LAN shall not increase latency by more than 10 ms above the specified maximum latency for a wired LAN.

7. The WLAN shall support LAN Traffic Prioritization and QoS IAW the following based on the wireless interface type:

a. 802.11 Interfaces. Wireless products using 802.11 shall utilize the settable Service Class tagging/QoS parameters within 802.11e to implement, as a minimum, DSCP.

b. 802.16 Interfaces. Wireless products using 802.16d and/or 802.16e, QoS/Service Class tagging shall meet the following requirements:

(1) The WLAN products may use 802.16 services to provide QoS over the wireless portion of the transport. Services associated with the granular service class are listed in Table 5.3.1-7, Cable Grade Capabilities.

(2) The WLAS and WABs shall mark traffic traversing into the wired portion of the LAN with appropriate wired DSCPs (see Table 5.3.1-8, 802.16 Service Scheduling).

8. Wireless products shall meet the WLAN security requirements as stipulated in the Wireless Security Technical Implementation Guide (STIG) and the following specified requirements:

a. All 802.11 wireless components shall:

(1) Use the Advanced Encryption Standard-Counter with Cipher Block Chaining-Message Authentication Code Protocol (AES-CCMP). It will be implemented in 802.11i system encryption modules.

Table 5.3.1-8. 802.16 Service Scheduling

AGGREGATE SERVICE CLASS	GRANULAR SERVICE CLASS	802.16 SERVICE	RADIO SERVICE TRAFFIC PRIORITY	WIRED LANs DEFAULT DSCPs	
				BASE 2	BASE 10
Control	Network Control	NA	NA	110 000-110 111	48-56
Inelastic/ Real-Time	User Signaling	UGS	7	101 000-101 111	40-47
	Circuit Emulation	UGS	6		
	Voice	UGS	6		
	Short messages	ertPS	5		
	Video/VTC	ertPS	4	100 000-100 111	32-39
	Streaming	rtPS	3	011 000-011 111	24-31
Preferred Elastic	Interactive Transactions and OA&M	nrtPS	2	010 000-010 111	16-23
	File Transfers and OA&M	nrtPS	1	001 000-001 111	8-15
Elastic	Default	BE	0	000 000-000 111	0-7

LEGEND

BE	Best Effort	OA&M	Operations, Administration and Management
DSCP	Differentiated Services Code Point	NA	Not Applicable
ertPS	Extended Real-Time Polling Service	rtPS	Real-Time Polling Service
LAN	Local Area Network	UGS	Unsolicited Grant Service
NA	Not Applicable	VTC	Video Teleconferencing
nrtPS	Non-Real Time Polling Service		

(2) Implement the Extensible Authentication Protocol - Transport Layer Security (EAP-TLS) mutual authentication for the EAP component of Wi-Fi Protected

Access (WPA2). This requirement does not apply to connections between 802.11 WABs.

5.3.1.7.2.2 WLAS, WAB Wireless Intrusion Detection System

[Required: WLAS, WAB] The WLAS and/or WAB wireless network shall be monitored by a Wireless Intrusion Detection System (WIDS). The system will have the following capabilities:

1. Continuous-scanning: The WIDS will scan continuously 24 hours/day, 7 days/week to detect authorized and unauthorized activity.

2. Location-sensing WIDS: The WIDS will include a location sensing protection scheme for authorized and unauthorized wireless products.

3. Deployed systems shall be properly engineered so that the WLAN and wireless products achieve the required performance requirements in their specific structural environment. Users shall submit their network design with their request for DSN connection. The Unified Capabilities Connection Office (UCCO) submittal shall include wireless security compliancy FIPS 140 and proposed accessibility as well as WIDS National Information Assurance Partnership (NIAP) Common Criteria validation for basic robustness. Medium robustness will be applied, as determined by the Designated Approving Authority (DAA), when the NIAP Common Criteria for that level is approved.

5.3.1.7.2.3 Wireless Interface Requirements

[Required: WEI, WLAS, and WAB]

1. If a wireless product is used, the wireless product shall support at least one of the following approved wireless LAN standards interfaces:

    a. 802.11a (WEI, WLAS, WAB)
    b. 802.11b (WEI ,WLAS)
    c. 802.11g (WEI, WLAS, WAB)
    d. 802.16 (WEI, WLAS, WAB)

2. For any of the 802.11 interfaces, the wireless product must support both of the following 802.11 standards:

    a. 802.11e - Part 11: Wireless LAN Medium Access Control (MAC) and Physical Layer (PHY) specifications and Amendment 8: Medium Access Control (MAC)

Quality of Service Enhancements. See Table 5.3.1-7, Cable Grade Capabilities, for priority bit assignment.

b. 802.11i - Part 11: Wireless LAN Medium Access Control (MAC) and Physical Layer (PHY) specifications and Amendment 6: Medium Access Control (MAC) Security Enhancements.

3. For the 802.11a interface, the wireless product must support the standard 802.11h - Part 11: Wireless LAN Medium Access Control (MAC) and Physical Layer (PHY) specifications, Amendment 5: Spectrum and Transmit Power Management Extensions in the 5 GHz band in Europe.

4. For any of the 802.16 interfaces, the wireless product must support the following 802.16 standards dependent on whether the end item attached to the WLAS is "fixed" or "nomadic".

   a. Fixed WEIs are those WEIs that access a single WLAS for the duration of the session and are not expected to traverse between WLASs so that handoffs are not required. Fixed WEIs may support either 802.16d – Part 16: Air Interface for Fixed Broadband Wireless Access Systems or 802.16e – Part 16: Air Interface for Fixed and Mobile Broadband Wireless Access Systems, & Amendment 2: Physical and Medium Access Control Layers for Combined Fixed and Mobile Operation in Licensed Bands and Corrigendum 1.

   b. Nomadic WEIs are those WEIs that are mobile and may traverse different WLASs during a single session. Nomadic WEIs must support 802.16e – Part 16: Air Interface for Fixed and Mobile Broadband Wireless Access Systems, and Amendment 2: Physical and Medium Access Control Layers for Combined Fixed and Mobile Operation in Licensed Bands and Corrigendum 1.

5.3.1.7.2.4 Wireless End Instruments

[Required: WEIs]

If WEIs are used, the following requirements will apply.

1. Wireless VoIP EIs are certified as part of the VoIP solution.

2. Access to/from a WEI shall be provided by either 802.11 or 802.16. Two methods that an IP subscriber can use to access voice services are dedicated wireless service or shared wireless service (see Figure 5.3.1-8, Access Methods for the Wireless Access Layer End

Item Product Telephones). The dedicated access method provides wireless access service for a single type of traffic (i.e., voice, video, or data – three devices are required to support all traffic types). The shared access method allows a single wireless WLAS to provide for all traffic types supported (i.e., voice, video, and data – one device provides all three traffic types), on all computer types and/or Personal Equipment Product (PED) to connect to the wireless WLAS.

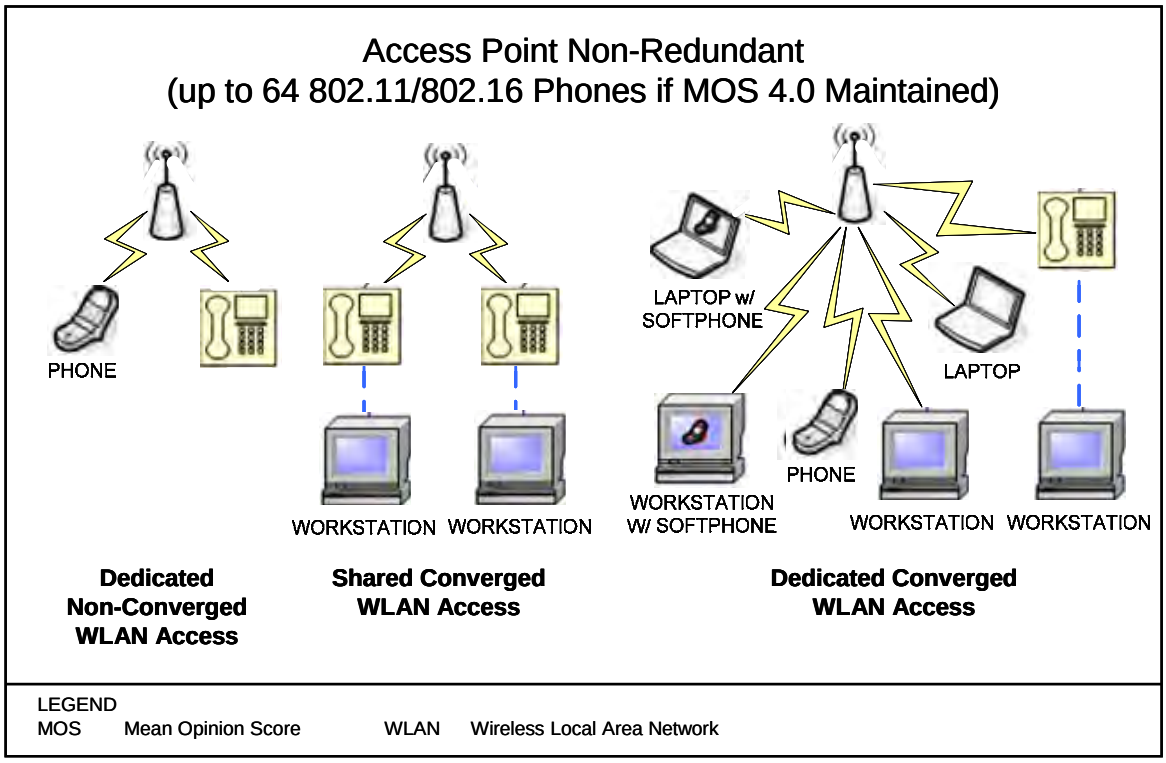


Figure 5.3.1-8. Access Methods for the Wireless Access Layer End Item Product Telephones

3. WEIs may use either method separately or a combination to provide wireless access (see Figure 5.3.1-8).

4. WEIs or soft clients on workstations acting as WEIs shall authenticate to the VoIP system call control. Authentication shall be IAW UCR IA-specified requirements.

5. The WEI is associated with the supporting IP telephone switch. The WEI shall be functionally identical to a traditional IP wired telephone and will be required to provide voice features and functionality IAW other UCR specified requirements unless explicitly stated.

6. Minimally, all WEIs shall be FIPS 140-2 Level 1 certified.

7. If the WEI loses connection with the VoIP switch when using a WLAN, the call will be terminated by the VoIP switch. The termination period shall be determined by the VoIP switch using a configurable time-out parameter with a time-out range of 0-60 seconds; default shall be set to 5 seconds. The subscriber line will be treated as if it were out of service until communication is re-established with the wireless voice end instrument.

5.3.1.7.2.5 Wireless LAN Access System Requirements

A WLAS implementation is considered to be the replacement of the physical layer of the wired Access Layer of a LAN. A WLAS that is used may range in size from less than 96 voice IP subscriber services for non-redundant WLAS(s) to 1024 voice IP subscriber services for a redundant WLAS(s). Wireless products that support 96 or less voice users are not required to be redundant.

[Required: WLAS] If a WLAS is used as part of the LAN design supporting VoIP subscribers, the following requirements must be met:

1. Failure of a WLAS shall not cause the loss of a call as the connection transfers from the primary to alternate system. However, it may allow a single momentary 5-second delay in voice bearer traffic in both directions of the wireless link as wireless VoIP telephone clients are re-authenticated to the standby system. The 5-second voice delay will not be factored into the overall MOS score.

2. The WLAS shall support the following maximum number of EIs per Table 5.3.1-9, Maximum Number of EIs Allowed per WLAS, for converged or non-converged access for redundant and non-redundant WLAS; while not degrading any of the individual EIs' voice quality below the specified MOS scores for strategic and tactical situations, in an open air environment at a distance of 100 feet, except for the 5-second re-authentication as stated in item 1, (i.e., strategic MOS 4.0, strategic-to-tactical MOS 3.6, tactical-to- tactical MOS 3.2).

3. At the point when voice quality degradation occurs, defined as a MOS score below appropriate levels (i.e., strategic 4.0, strategic-to-tactical 3.6, and tactical-to-tactical 3.2), when all telephones are off-hook simultaneously, this becomes the maximum number of telephones and/or other wireless non-voice end item products that the WLAS can support for the WLAS transmitter coverage distance.

4. The WLAS shall not drop an active call as the WEI roams from one WLAS transmitter zone into another WLAS transmitter zone.

Table 5.3.1-9. Maximum Number of EIs Allowed per WLAS

WLAN CONVERGENCE TYPE	ACCESS TYPE	WLAS REDUNDANCY	L2/L3 SWITCH LINK(S)	L2/L3 CONNECTION LINK ETHERNET SPEED	MAXIMUM # WIRELESS PHONE SUBSCRIBERS
Non-Converged	Non-Sharing	Non-Redundant	Single	10 Mbps	96
		Redundant	Link Pair	10 Mbps	100
				100 Mbps	1,000
				1 Gbps	10,000
				10 Gbps	100,000
Converged	Shared and/or Dedicated	Non-Redundant	Single	100 Mbps	96
		Redundant	Link Pair	100 Mbps	250
				1 Gbps	2,500
				10 Gbps	25,000

NOTE
This table defines the maximum number of telephones allowed. This number greatly exceeds the expected WLAS capability for maintaining appropriate MOS (strategic 4.0, strategic-to-tactical 3.6, and tactical-to-tactical 3.2) when all telephones are off-hook simultaneously.

LEGEND

Gbps	Gigabits per second	MOS	Mean Opinion Score
L2	OSI Layer 2	OSI	Open System Interconnect
L3	OSI Layer 3	WLAN	Wireless Local Area Network
Mbps	Megabits per second	WLAS	Wireless LAN Access System

5.3.1.7.2.6 Wireless Access Bridge

Wireless access bridges can be used to replace the physical layer of the wired L2/L3 Access Layer of the ASLAN or non-ASLAN with wireless technology. IEEE 802.11 and/or 802.16 systems can be used to provide a wireless communications link (or bridge) between two or more wired LANs, typically located in adjacent buildings. The WAB functions within the LAN primarily as a wireless NE. The hardware used in a wireless LAN bridge is similar to a WLAS, but instead of connecting only wireless clients to the wired network, bridges are used primarily to connect other wireless LAN bridges to the network. Simultaneously, the WAB may provide connection services to wireless end item products too (i.e., act simultaneously as a WLAS). An example of a combination WLAS/WAB and WAB is provided in Figure 5.3.1-9, Example of Combined WLAS/WAB and Second Layer WAB (a combination protocol WLAN/WAB (802.11 WLAS with 802.16)).

[Required: WAB] If provided, the WAB will be required to meet all the requirements for each individual type interface.

1. For any of the 802.16 interfaces, the WAB must support any of the following 802.16 standards:

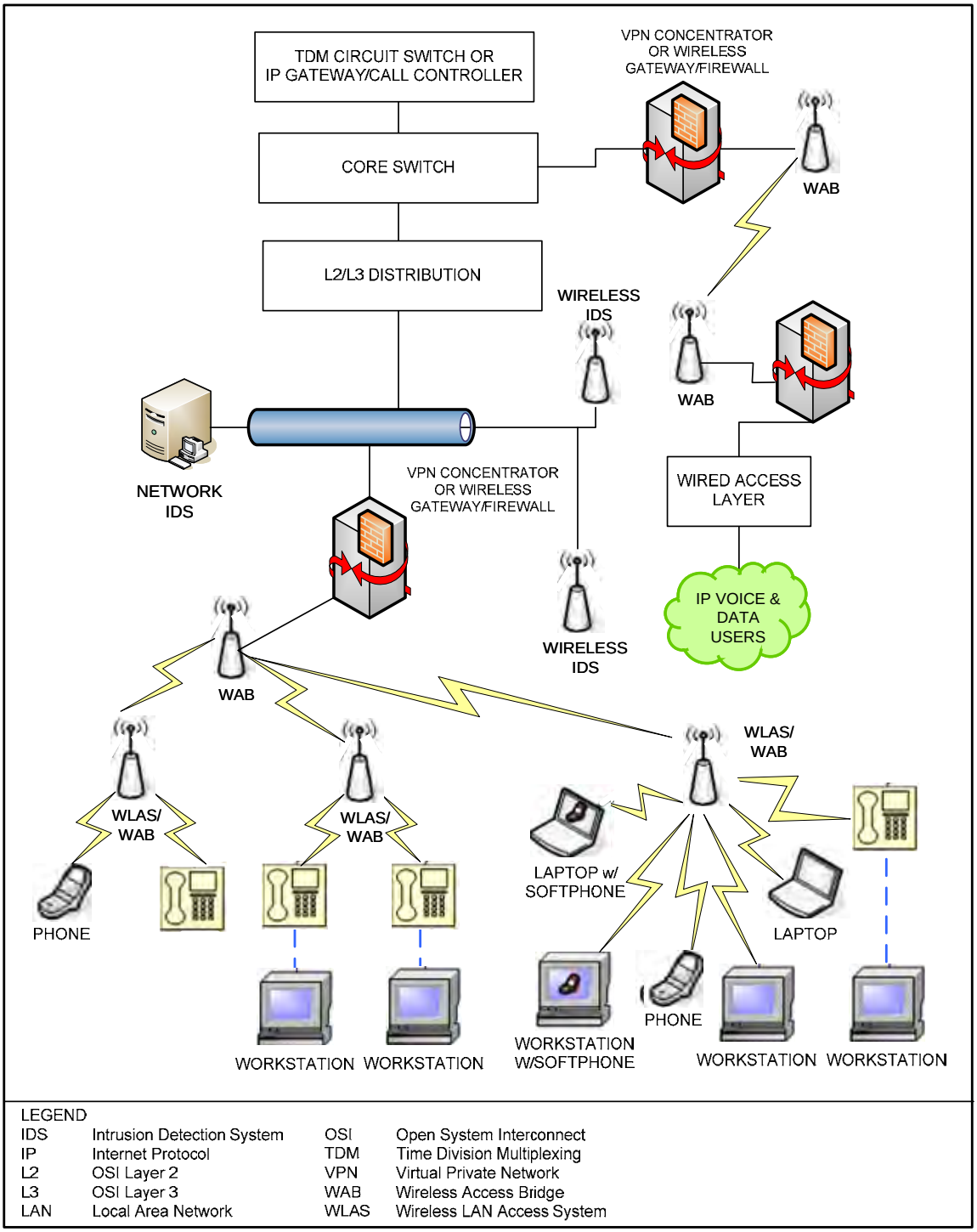


Figure 5.3.1-9. Example of Combined WLAS/WAB and Second Layer WAB

a. 802.16d – Part 16: Air Interface for Fixed Broadband Wireless Access Systems, or

b. 802.16e – Part 16: Air Interface for Fixed and Mobile Broadband Wireless Access Systems, & Amendment 2: Physical and Medium Access Control Layers for Combined Fixed and Mobile Operation in Licensed Bands and Corrigendum 1.

2. The maximum number of voice calls transported across the WAB shall be in accordance with UCR 2008, Section 5.3.1.7.3, Traffic Engineering. Maximum voice users will be determined by the smallest link size (i.e., Ethernet connection to the WAB or the WAB wireless link speed of the WAB itself).

3. The introduction of a WAB(s) shall not cause the end-to-end average MOS to fall below appropriate levels (strategic 4.0, strategic-to-tactical 3.6, and tactical-to-tactical 3.2) as measured over any 5-minute time interval.

4. The introduction of a WAB(s) shall not exceed the end-to-end digital BER requirement of less than 1 error in $1x10^{-8}$ (averaged over a 9-hour period).

5. The introduction of a WAB(s) shall not degrade secure transmission for secure end products as defined in UCR 2008, Section 5.2.12.6, DoD Secure Communications Devices (DSCDs).

6. The WAB shall transport all call control signals transparently on an end-to-end basis.

7. The addition of a WAB(s) shall not cause the one-way delay measured from ingress to egress to increase by more than 3 ms for each WAB used, averaged over any 5-minute period.

8. The addition of the WAB shall not increase the LAN jitter requirements previously specified in this section.

A WAB may simultaneously act as a WLAS.

[Required: WLAS/WAB] The WLAS/WAB combination must meet all the requirements for access (WLAS) and bridging (WAB).

1. The WAB(s) and/or WLAS/WAB shall support Service Class tagging/QoS as previously specified in this section.

2. The WABs may support special C2 calls, C2, C2(R), and non-C2 calls. All calls must meet other specified performance requirements for these users.

5.3.1.7.3 Traffic Engineering

5.3.1.7.3.1 Voice Services

[Required: ASLAN and Non-ASLAN] Bandwidth required per voice subscriber is calculated as 102 kbps (each direction) for each IP call (for IPv4). This is based on G.711 (20 ms codec) with IP overhead as depicted in Figure 5.3.1-10 (97 kbps for Ethernet IPv4) plus 5 kbps for SRTCP.

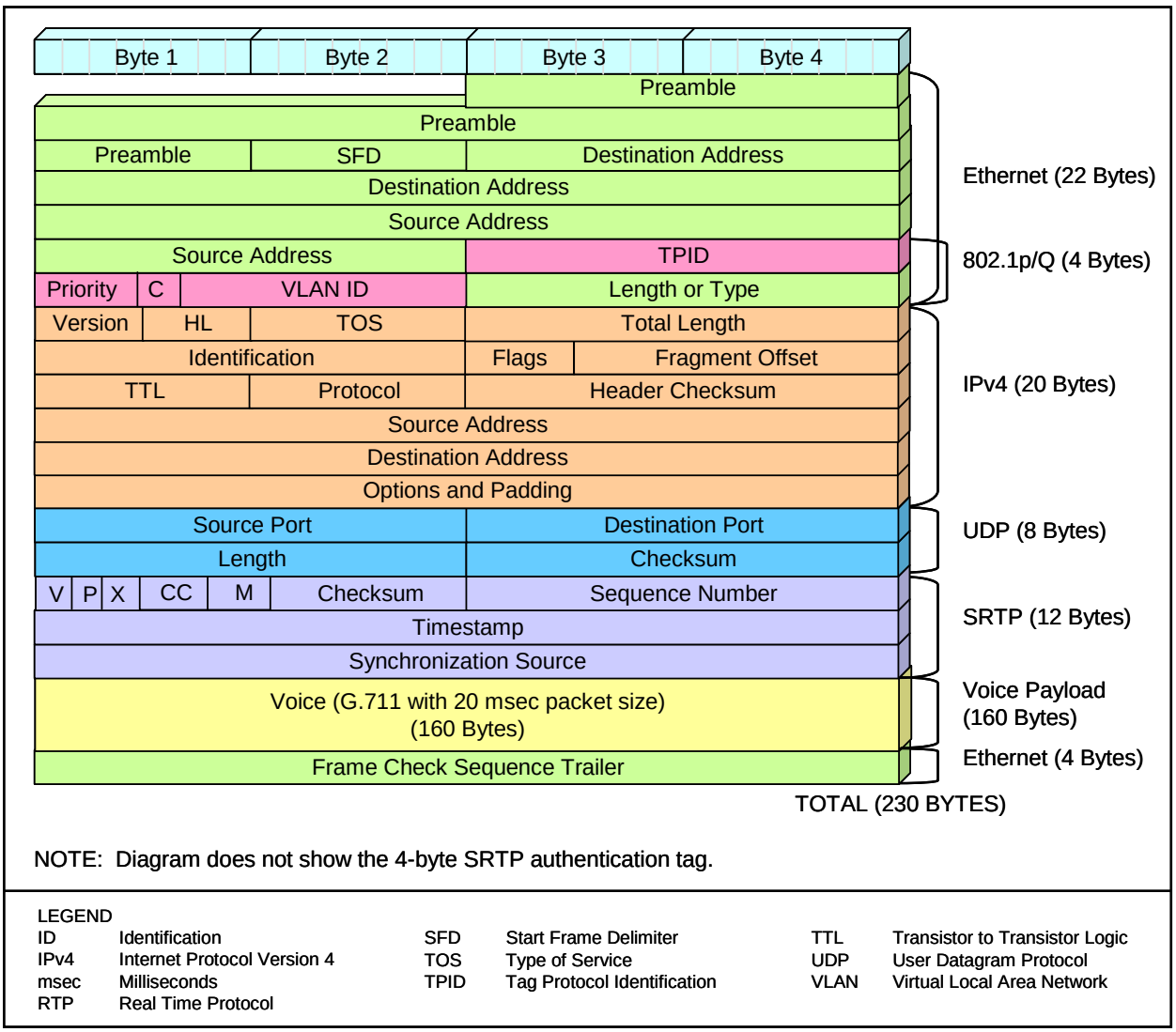


Figure 5.3.1-10. Voice over IP Bandwidth

Based on overhead bits included in the bandwidth calculations, vendor implementations may use different calculations and hence arrive at slightly different numbers. IPv6 adds an additional 20

bytes in the IP header (40 bytes instead of 20 bytes). The increase of 20 bytes to 250 bytes increases the IPv6 bandwidth to 110.0 kbps. This calculation includes a 12-byte Ethernet Interframe gap and the SRTCP overhead.

Bandwidth in the LAN shall be engineered so the following stipulations are met:

1. Voice IP subscribers do not exceed more than 25 percent of available bandwidth (see examples of number of users based on common link sizes in Table 5.3.1-10.

2. No single point of failure within the ASLAN can cause a voice service outage to more than 96 users. Based on the previous constraints, the recommended number of voice subscribers based on available link sizes is shown in Table 5.3.1-10.

Table 5.3.1-10. LAN VoIP Subscribers for IPv4 and IPv6

PRODUCT	LINK TYPE	LINK SIZE	# C2 VoIP SUBSCRIBERS (ASLAN)	# NON-C2 VoIP SUBSCRIBERS (NON-ASLAN)
Core	IP Trunk Link	10 Mbps, 100 Mbps 1 Gbps, and 10 Gbps	96[1]	50, 500, 5000, and 50,000
	IP Trunk Link Pair	10 Gbps	25000[2]	50000
	IP Trunk Link Pair	**1 Gbps**	**2500**	**5000**
	IP Trunk Link Pair	100 Mbps	250	500
	IP Trunk Link Pair	10 Mbps	25	50
	IP Subscriber (voice only)	10 Mbps	1[3]	1
	IP Subscriber (converged)	100 Mbps	1[4]	1
Distribution	IP Trunk Link	10 Mbps, 100 Mbps 1 Gbps, and 10 Gbps	96[1]	50, 500, 5000, and 50,000
	IP Trunk Link Pair	10 Gbps	25000	50000
	IP Trunk Link Pair	1 Gbps	2500	5000
	IP Trunk Link Pair	**100 Mbps**	**250**	**500**
	IP Trunk Link Pair	10 Mbps	25	50
	IP Subscriber (voice only)	10 Mbps	1[3]	1
	IP Subscriber (converged)	100 Mbps	1[4]	1
Access	IP Trunk Link	10 Mbps, 100 Mbps 1 Gbps, and 10 Gbps	96[1]	50, 500, 5000, and 50,000
	IP Trunk Link Pair	10 Gbps	25000	50000
	IP Trunk Link Pair	1 Gbps	2500	5000
	IP Trunk Link Pair	**100 Mbps**	**250**	**500**
	IP Trunk Link Pair	10 Mbps	25	50
	IP Subscriber (voice only)	10 Mbps	1[3]	1
	IP Subscriber (converged)	100 Mbps	1[4]	1

PRODUCT	LINK TYPE	LINK SIZE	# C2 VoIP SUBSCRIBERS (ASLAN)	# NON-C2 VoIP SUBSCRIBERS (NON-ASLAN)
NOTES 1. All trunks must be link pairs to meet assured service requirements. For single links, number of users is limited to 96 because of single point of failure requirements. 2. For the converged network, voice traffic was engineered not to exceed 25 percent of total utilization. 3. The minimum link for VoIP subscriber is 10 Mbps. 4. For subscribers that share voice and data (converged), minimum recommended bandwidth for the link is 100 Mbps. • Numbers in bold represent the minimum recommended trunk sizes. • Link pairs may use stand-by link or load balancing. Number of subscribers is calculated at one half the total link pair capacity.				
LEGEND: ASLAN Assured Services LAN C2 Command and Control Gbps Gigabits per second IP Internet Protocol IPv4 IP Version 4 IPv6 IP Version 6 LAN Local Area Network Mbps Megabits per second VoIP Voice over IP				

5.3.1.7.3.2 Video Services

The amount of video bandwidth required over the ASLAN varies depending on the codec and other features that are negotiated at setup. Unlike voice, video over IP is not a constant rate. Video packets may range in size from hundreds of bytes up to 1500 bytes. Table 5.3.1-11, Video Rates and IP Overhead, lists the common video rates and associated IP overhead.

Table 5.3.1-11. Video Rates and IP Overhead

VIDEO STREAM BANDWIDTH	IP OVERHEAD	TOTAL IP BANDWIDTH
128 kbps	32 kbps	160 kbps
256 kbps	64 kbps	320 kbps
384 kbps	96 kbps	480 kbps
768 kbps	192 kbps	960 kbps
2 Mbps	0.5 Mbps	2.5 Mbps
4.5 Mbps	1.125 Mbps	5.625 Mbps
6 Mbps	1.5 Mbps	7.5 Mbps
Legend: IP Internet Protocol kbps Kilobits per second Mbps Megabits per second		

Table 5.3.1-9, Maximum Number of EIs Allowed per WLAS, lists the bandwidth available based on an engineered solution of 25 percent allocation of the bandwidth to video. Unlike voice, video does not have the single point of failure requirements. Thus, the capacity or available bandwidth on a link pair is based on the aggregate total, not one half used in the voice calculations. Table 5.3.1-12, Video over IP Bandwidth, lists available video BW based on 25

percent traffic engineering and how many sessions are possible at a video rate of 384 kbps (480 kbps with IP overhead).

Table 5.3.1-12. Video over IP Bandwidth

ASLAN PRODUCT	LINK TYPE	LINK SIZE	# VIDEO OVER IP BW	# 384 kbps SESSIONS
Core	IP Trunk Link	10 Gbps	2.5 Gbps	5000
	IP Trunk Link	1 Gbps	250 Mbps	500
	IP Trunk Link	100 Mbps	25 Mbps	50
	IP Trunk Link	10 Mbps	2.5 Mbps	5
	IP Subscriber (video only)	10 Mbps	1	NA
	IP Subscriber (converged)	100 Mbps	1	NA
Distribution	IP Trunk	10 Gbps	2.5 Gbps	5000
	IP Trunk	1 Gbps	250 Mbps	500
	IP Trunk	100 Mbps	25 Mbps	50
	IP Trunk	10 Mbps	2.5 Mbps	5
	IP Subscriber (video)	10 Mbps	1	NA
	IP Subscriber (converged)	100 Mbps	1	NA
Access	IP Trunk	10 Gbps	2.5 Gbps	5000
	IP Trunk	1 Gbps	250 Mbps	500
	IP Trunk	100 Mbps	25 Mbps	50
	IP Trunk	10 Mbps	2.5 Mbps	5
	IP Subscriber (video)	10 Mbps	1	NA
	IP Subscriber (converged)	100 Mbps	1	NA

NOTES
1. All trunks must be link pairs to meet assured service requirements. For single links, number of users is limited to 96 because of single point of failure requirements.
2. For the converged network, voice traffic was engineered not to exceed 25% of total utilization.
3. The minimum link for VoIP subscriber is 10 Mbps.
4. For subscribers that share voice and data (converged), minimum recommended bandwidth for the link is 100 Mbps.
5. Numbers in bold represent the minimum recommended trunk sizes.
6. Link pairs may use stand-by link or load balancing. Number of subscribers is calculated at one half the total link pair capacity.

Legend

ASLAN	Assured Services LAN	kbps	kilobits per second
BW	Bandwidth	Mbps	Megabits per second
Gbps	Gigabits per second	NA	Not Applicable
IP	Internet Protocol		

5.3.1.7.3.3 Data Services

[Required: ASLAN and Non-ASLAN]. The LAN will be engineered for a ratio of 25 percent voice, 25 percent video, and 50 percent data. Data traffic can burst up to the full link capacity if voice and video are not present.

5.3.1.7.4 VLAN Design and Configuration

VLANs offer the following features:

1. Broadcast Control. Just as switches isolate collision domains for attached hosts and only forward appropriate traffic out a particular port, VLANs refine this concept further and provide complete isolation between VLANs. A VLAN is a bridging domain, and all broadcast and multicast traffic is contained within it.

2. Security. VLANs provide security in two ways:

   a. High-security users can be grouped into a VLAN, possibly on the same physical segment, and no users outside of that VLAN can communicate with them.

   b. VLANs are logical groups that behave like physically separate entities, inter-VLAN communication is achieved through a router. When inter-VLAN communication occurs through a router, all the security and filtering functionality that routers traditionally provide can be used because routers are able to look at Layer 3 information.

Three ways of defining a VLAN are as follows:

1. Port-Based. Port-based VLANs are VLANs that are dependent on the physical port that a product is connected to. All traffic that traverses the port is marked with the VLAN configured for that port. Each physical port on the switch can support only one VLAN. With port-based VLANs, no Layer 3 address recognition takes place. All traffic within the VLAN is switched, and traffic between VLANs is routed (by an external router or by a router within the switch). This type of VLAN is also known as a segment-based VLAN (see Figure 5.3.1-11, Port-Based VLANs).

2. IEEE 802.1Q. VLANs can be assigned by end products IAW the IEEE 802.1Q VLAN ID tag.

   [Required: ASLAN] The ASLAN products must be capable of accepting VLAN tagged frames and assigning them to the VLAN identified in the 802.1Q VID field (see Figure 5.3.1-12, IEEE 802.1Q-Based VLANs).

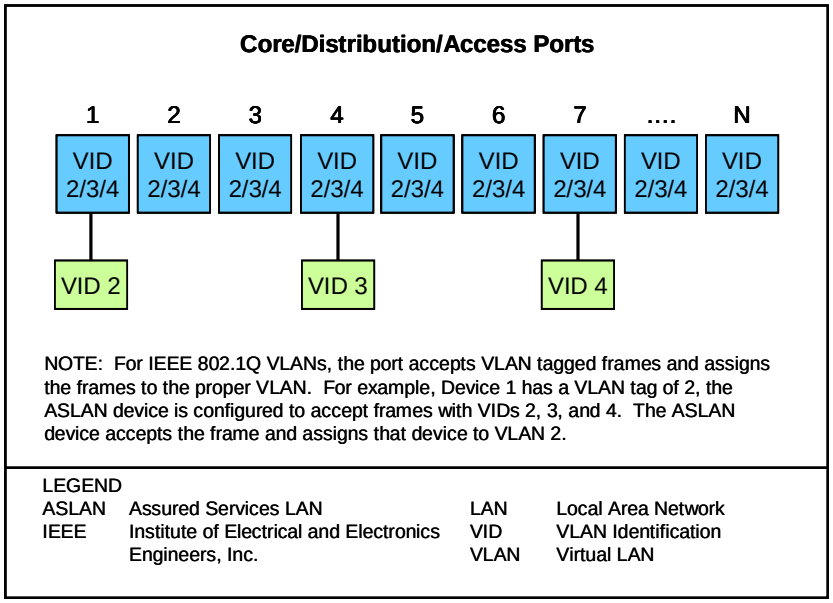


Figure 5.3.1-12. IEEE 802.1Q-Based VLANs

3. By a User-Defined Value. This type of VLAN is typically the most flexible, allowing VLANs to be defined based on the value of any field in a packet or frame. For example, VLANs could be defined on a protocol basis or could be dependent on a particular address (Layer 2 or Layer 3). The simplest form of this type of VLAN is to group users according to their MAC addresses (see Figure 5.3.1-13, User-Defined VLANs). The LAN shall be designed so RTS and data reside in separate VLANs. Depending on whether a product is performing converged services or a single service will decide how VLANs are designed.

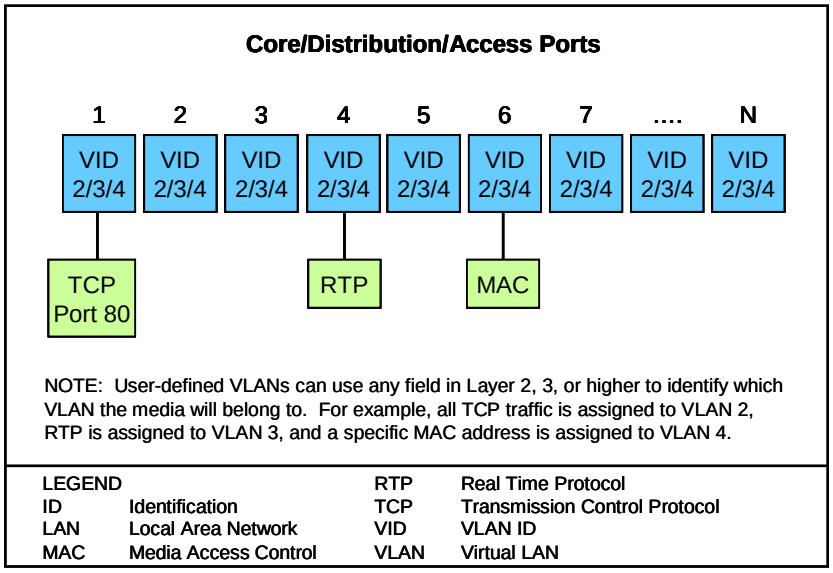


Figure 5.3.1-13. User-Defined VLANs

The recommended VLAN types are port-based and IEEE 802.1Q tagged frames. For VoIP, video, and data end products, any end system that supports convergence (i.e., more than one media) the end-system must preassign the VLAN using IEEE 802.1Q tags prior to the frames entering the ASLAN. For end-systems that support just one media (i.e., voice or video or data), the LAN can assign the VLAN based on port-based VLAN assignment.

Real time services and data must be placed in separate VLANs for security purpose. The LAN may be designed with more than one VLAN per media type. Signaling for voice and video can be placed in the same VLAN as the respective media, or placed in an entirely different signaling VLAN.

5.3.1.7.5 Power Backup

[Required: ASLAN – Conditional: Non-ASLAN] To meet CJCS requirements for assured services, equipment serving special C2 and C2 users must be provided with backup power. The ASLAN must meet the power requirements outlined. The following requirements for uninterruptible power systems (UPS) are bare minimum requirements. These requirements should be increased following the guidance in Telcordia Technologies GR-513-CORE to meet site operational requirements and extenuating characteristics of the application environment. Figure 5.3.1-14, ASLAN UPS Power Requirements, illustrates a typical arrangement of how the minimum power backup requirements can be met.

1. Special C2. The ASLAN must provide an 8-hour backup capability in the event of primary power loss to special C2 users. Any ASLAN product, Core, Distribution, or Access, that supplies service to the special C2 user must have an 8-hour UPS.

2. C2. The ASLAN must provide 2 hour backup capability in the event of primary power loss to C2 users. Any ASLAN product, core, distribution or access, that supplies service to the C2 user must have a 2 hour uninterruptible power system (UPS).

3. C2(R) or Non-C2. C2(R) or non-C2 users may lose telephony service in the event of a power failure.

   NOTE: Backup Power (Environmental). The backup power system shall have the capacity to operate environmental systems needed to sustain continuous equipment operation. Power to the environmental systems may not need to be continuous.

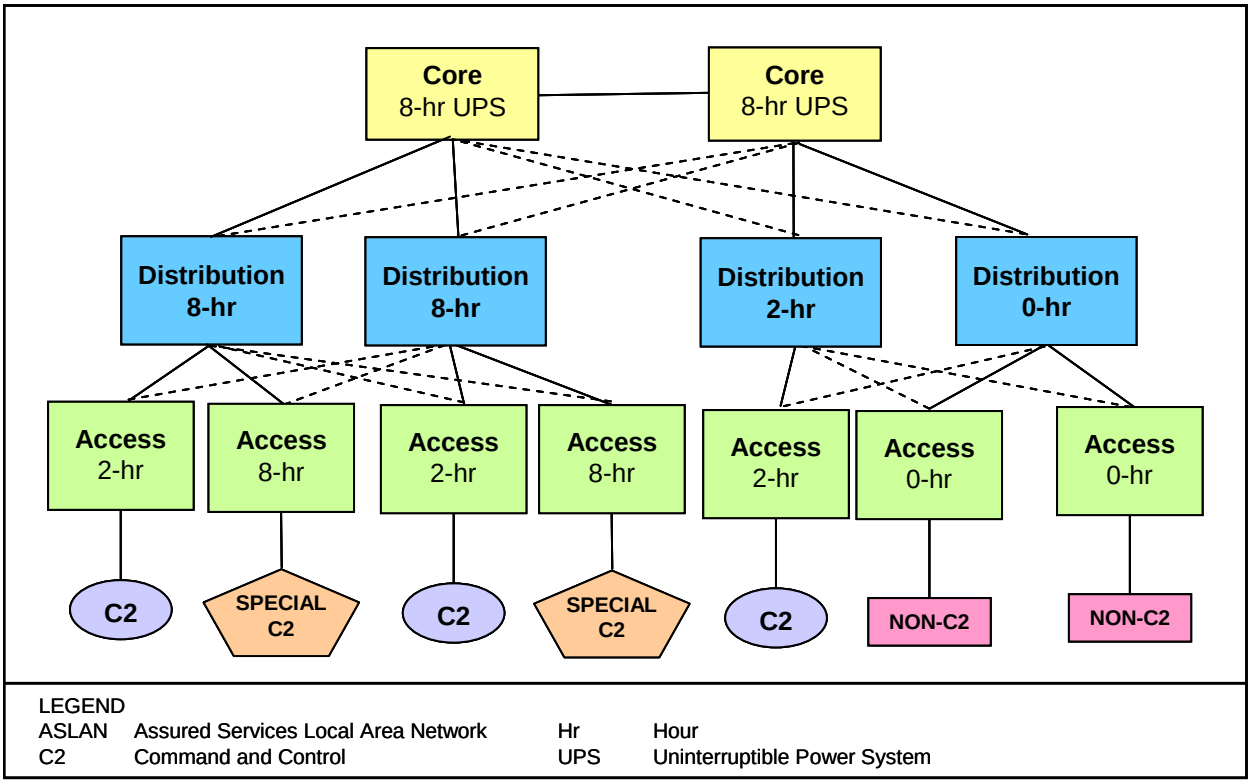


Figure 5.3.1-14. ASLAN UPS Power Requirements

5.3.1.7.6 Availability

The terms reliability, resiliency, and availability are sometimes used interchangeably. However, although all three terms are related to the concept of high availability, it is important to note the differences in terminology. Reliability is the probability that a system will not fail during a specified period of time. Resiliency is the ability of a system to recover to its normal operating form after a failure or an outage. Availability is the ratio of time that a service is available to total time.

Availability can be expressed as mean time between failure (MTBF) and mean time to repair (MTTR), and expressed in mathematical terms as:

$$\text{Availability} = \text{MTBF}/(\text{MTBF}+\text{MTTR})$$

MTBF is tied to the reliability of the system, while MTTR and resiliency are closely related. Thus system availability increases as the reliability and/or resiliency of the system is increased. Availability is typically expressed in percentage of time the system is available or in downtime per year. The two methods of expressing availability are equivalent and related as shown in Table 5.3.1-13, Methods of Expressing Availability.

Table 5.3.1-13. Methods of Expressing Availability

NUMBER OF 9'S	AVAILABILITY	DOWNTIME PER YEAR
1	90.0%	36 days, 12 hrs
2	99.0%	87 hrs, 36 mins
3	99.9%	8 hrs, 46 mins
4	99.99%	52 mins, 33 secs
5	99.997%	15 mins, 46 secs
6	99.999%	5 mins, 15 secs
7	99.9999%	31.5 secs
Legend: hrs hours secs seconds mins minutes		

[Required: ASLAN – Conditional: Non-ASLAN] The ASLAN has two configurations depending on whether it supports special C2 or C2 users. The ASLAN shall have a hardware availability designed to meet the needs of its subscribers:

1. Special C2. An ASLAN that supports special C2 users is classified a High Availability ASLAN and must meet 99.999 percent availability to include scheduled maintenance.

2. C2. An ASLAN that supports C2 users is classified as a Medium Availability ASLAN and must have 99.997 percent availability to include scheduled maintenance.

[Required: Non-ASLAN] The non-ASLAN shall provide an availability of 99.9 percent to include scheduled maintenance. C2(R) users who originate ROUTINE-only precedence calls but terminate any precedence level may be supported on a non-ASLAN, but the non-ASLAN must support MLPP for the C2(R) users. Special C2 or C2 users shall not be supported on a non-ASLAN.

The methods for calculating reliability are found in UCR 2008, Section 5.3.2, Assured Services Requirements.

5.3.1.7.7 Redundancy

The following paragraphs outline the redundancy requirements for the LAN.

[Required: ASLAN – Conditional: Non-ASLAN] The ASLAN shall have no single point of failure that can cause an outage of more than 96 IP telephony subscribers. In order to meet the availability requirements, all switching/routing platforms that offer service to more than 96 telephony subscribers shall provide redundancy in either of two ways:

1. The product itself (Core, Distribution, or Access) provides redundancy internally.

2. A secondary product is added to the ASLAN to provide redundancy to the primary product.

5.3.1.7.7.1 Single Product Redundancy

[Conditional: ASLAN – Conditional: non-ASLAN] Single product redundancy may be met with a modular chassis that at a minimum provides the following:

1. Dual Power Supplies. The platform shall provide a minimum of two power supplies each with the power capacity to support the entire chassis. Loss of a single power supply shall not cause any loss of ongoing functions within the chassis.

2. Dual Processors (Control Supervisors). The chassis shall support dual control processors. Failure of any one processor shall not cause loss of any ongoing functions within the chassis (e.g., no loss of active calls).

3. Termination Sparing. The chassis shall support a (N + 1) sparing capability for available 10/100Base-T modules used to terminate to an IP subscriber.

4. Redundancy Protocol. Routing equipment shall support a protocol that allows for dynamic rerouting of IP packets so that no single point of failure exists in the ASLAN that could cause an outage to more than 96 IP subscribers.

5. No Single Failure Point. No single point shall exist in the LAN that would cause loss of voice service to more than 96 IP telephony instruments.

6. Switch Fabric or Backplane Redundancy. Switching platforms within the ASLAN shall support a redundant (1 + 1) switching fabric or backplane. The second fabric's backplane shall be in active standby so that failure of the first shall not cause loss of ongoing events within the switch.

In the event of a component failure in the network, all calls that are active shall not be disrupted (loss of existing connection requiring redialing) and the path through the network shall be restored within 5 seconds.

5.3.1.7.7.2 Dual Product Redundancy

[Conditional: ASLAN – Conditional: Non-ASLAN] In the case where a secondary product has been added to provide redundancy to a primary product, the failover over to the secondary product must not result in any lost calls. The secondary product may be in 'standby mode' or

”active mode,” regardless of the mode of operation the traffic engineering of the links between primary and secondary must meet the requirements provided in UCR 2008, Section 5.3.1.7.3, Traffic Engineering.

In the event of a primary product failure, all calls that are active shall not be disrupted (loss of existing connection requiring redialing) and the failover to the secondary product must be restored within 5 seconds.

5.3.1.7.8 Maintainability

The following information is proved as an engineering guideline:

Maintainability is described in MIL-HDBK-470A as:

“The relative ease and economy of time and resources with which an item can be retained in, or restored to, a specified condition when maintenance is performed by personnel having specified skill levels, using prescribed procedures and resources, at each prescribed level of maintenance and repair. In this context, it is a function of design.”

Operational availability is similar to inherent availability but includes the effects of maintenance delays and other nondesign factors.

The equation for operational availability, or Ao, is:

$$Ao = MTBM/(MTBM + MDT)$$

where MTBM is the mean time between maintenance and MDT is the mean downtime. (NOTE: MTBM addresses all maintenance, corrective and preventive, whereas MTBF only accounts for failures. MDT includes MTTR and all other time involved with downtime, such as delays. Thus, Ao reflects the totality of the inherent design of the product, the availability of maintenance personnel and spares, maintenance policy and concepts, and other non-design factors, whereas availability reflects only the inherent design.

When acquiring products for the ASLAN, maintainability of the products must be taken into consideration. Based on the need to meet operational availability for special C2 and C2 users, it is recommended that all ASLAN components have maintenance contracts in place that can replace key components in 24 hours or less.

5.3.1.7.9 Survivability

Network survivability refers to the capability of the network to maintain service continuity in the presence of faults within the network. This can be accomplished by recovering quickly from network failures quickly and maintaining the required QoS for existing services.

For the ASLAN, survivability needs to be inherent in the design. The following guidelines are provided for the ASLAN:

1. Layer 3 Dynamic Rerouting. The ASLAN products that route (normally the Distribution and Core Layers) shall use routing protocols IAW the DISR to provide survivability. The routing protocols of choice per the DISR are:

    a. Border Gateway Protocol (BGP) for interdomain routing

    b. Open Shortest Path First (OSPF), Version 2, for IPv4 and (OSPF) Version 3 for IPv6 or Intermediate System-Intermediate System (IS-IS) (IAW RFC 1629) for intradomain routing

2. Layer 2 Dynamic Rerouting.

    - Virtual Router Redundancy Protocol (VRRP) – RFCs 2787 and 3768. VRRP is able to provide redundancy to Layer 2 switches that lose connectivity to a Layer 3 router. The ASLAN shall employ VRRP to provide survivability to any product running Layer 2 (normally the Access Layer).

5.3.1.7.10 Summary of LAN Requirements by Subscriber Mission

Table 5.3.1-14, Summary of LAN Requirements by Subscriber Mission, summarizes selected LAN requirements in terms of LAN types and subscriber missions.

Table 5.3.1-14. Summary of LAN Requirements by Subscriber Mission

REQUIREMENT ITEM	SUBSCRIBER MISSION CATEGORY			
	SPECIAL C2	C2	C2(R)	NON-C2
ASLAN High	R	P	P	P
ASLAN Medium	NP	P	P	P
Non-ASLAN	NP	NP	P	P
MLPP	R	R	R	N
Diversity	R	R	NR	NR
Redundancy	R	R	NR	NR
Battery Backup	8 hours	2 hours	NR	NR
Single Point of Failure User > 96 Allowed	No	No	Yes	Yes
LAN GOS p=	0.0	0.0	0.0	N/A
Availability	99.999	99.997	99.9	99.9

LEGEND

ASLAN	Assured Services LAN
C2	Command and Control
C2(R)	C2 Routine
GOS	Grade of Service
LAN	Local Area Network
MLPP	Multilevel Precedence and Preemption
NP	Not Permitted
NR	Not Required
p	Probability of Blocking
P	Permitted
R	Required

TABLE OF CONTENTS

SECTION **PAGE**

5.3.2 Assured Services Requirements....403
5.3.2.1 Introduction....403
5.3.2.1.1 Requirements Terminology....403
5.3.2.1.2 Network Reference Model....404
5.3.2.1.3 General Assumptions....406
5.3.2.1.4 Information Assurance....408
5.3.2.1.5 Functional Reference Terminology – APL Products and Appliances....409
5.3.2.2 Assured Services System Features and Capabilities....413
5.3.2.2.1 Overview of VoIP and Video over IP System Design Attributes....413
5.3.2.2.2 Assured Services Subsystem....417
5.3.2.2.3 Signaling Protocols....431
5.3.2.2.4 Signaling Performance....431
5.3.2.3 Registration, Authentication, and Failover....432
5.3.2.3.1 Registration and Authentication....432
5.3.2.3.2 LSC and MFSS Failover Requirements....432
5.3.2.4 System Interface Requirements....437
5.3.2.4.1 Internal Interface Requirements....437
5.3.2.4.2 External Physical Interfaces between Network Components....438
5.3.2.4.3 Interfaces to Other Networks....438
5.3.2.4.4 VVoIP Network Management System Interface Requirements....439
5.3.2.5 System Physical, Quality, and Environmental Factors....439
5.3.2.5.1 Physical Characteristics....439
5.3.2.5.2 System Quality Factors....439
5.3.2.5.3 Environmental Conditions....441
5.3.2.6 End Instruments....441
5.3.2.6.1 Voice Instrument....442
5.3.2.6.2 Video End Instrument....444
5.3.2.6.3 End Instrument to ASLAN Interface....445
5.3.2.7 Local Session Controller....445
5.3.2.7.1 LSC Functional Reference Model and Assumptions....447
5.3.2.7.2 Summary of LSC Functions and Features....450

5.3.2.8 Multifunction Softswitch 455
5.3.2.8.1 MFSS Functional Reference Model and Assumptions.....455
5.3.2.8.2 Summary of MFSS Functions and Features ..459
5.3.2.8.3 Network Management Requirements for the MFSS 464
5.3.2.9 Call Connection Agent.....465
5.3.2.9.1 Introduction.....465
5.3.2.9.2 Functional Overview of the CCA 467
5.3.2.9.3 CCA Requirements Assumptions 470
5.3.2.9.4 Role of the CCA in Network Appliances 473
5.3.2.9.5 CCA-IWF Signaling Protocol Support Requirements 474
5.3.2.10 CCA Interaction with Network Appliances and Functions.....490
5.3.2.10.1 CCA Interactions between the Softswitch and TDM Sides of the MFSS.....490
5.3.2.10.2 CCA Support for Appliance Management Functions.....492
5.3.2.10.3 CCA Interactions with Transport Interface Functions.....492
5.3.2.10.4 CCA Interactions with the EBC.....494
5.3.2.10.5 CCA Support for Admission Control 495
5.3.2.10.6 CCA Support for UFS.....496
5.3.2.10.7 CCA Support for Information Assurance 497
5.3.2.10.8 CCA Interactions with Local Location Service.....499
5.3.2.10.9 CCA Interactions with Global Location Service.....499
5.3.2.10.10 CCA Interactions with End Instrument(s) 500
5.3.2.10.11 CCA Support for Assured Services Voice and Video.....501
5.3.2.10.12 CCA Interactions with Service Control Functions.....503
5.3.2.11 CCA Interworking between AS-SIP and DoD CCS7.....504
5.3.2.11.1 Purpose and Scope 504
5.3.2.11.2 Background.....505
5.3.2.11.3 General Considerations.....506
5.3.2.11.4 Interworking for a Call Originating in an AS-SIP Network toward an ISUP Network...507

5.3.2.11.5 Interworking for a Call Originating in an ISUP Network toward an AS-SIP Network...527
5.3.2.11.6 Interworking Timer.....548
5.3.2.12 Media Gateway Requirements.....549
5.3.2.12.1 Introduction.....549
5.3.2.12.2 Overview of the MG and MGC Functions 551
5.3.2.12.3 Role of the MG in Appliances 555
5.3.2.12.4 MG Interaction with Network Elements and Functions.....562
5.3.2.12.5 MG Interfaces to TDM Network Elements in DoD Networks: PBXs, EOs, and MFSs.....571
5.3.2.12.6 MG Interfaces to TDM Network Elements in Allied and Coalition Partner Networks.....572
5.3.2.12.7 MG Interfaces to TDM Network Elements in the PSTN in the United States 573
5.3.2.12.8 MG Interfaces to TDM Network Elements in OCONUS PTT Networks 574
5.3.2.12.9 MG Support for DoD CCS7 Trunks 575
5.3.2.12.10 MG Support for ISDN PRI Trunks.....576
5.3.2.12.11 MG Support for CAS Trunks.....577
5.3.2.12.12 MG Requirements: VoIP Interfaces, Internal to an Appliance.....579
5.3.2.12.13 Echo Cancellation 599
5.3.2.12.14 MG Requirements for Clock Timing.....602
5.3.2.12.15 MGC-MG CCA Functions.....602
5.3.2.13 Signaling Gateway Requirements.....611
5.3.2.13.1 Introduction.....611
5.3.2.13.2 Role of the SG in Appliances.....612
5.3.2.13.3 SG's Role – Interacting with MFSS Functions and Elements 613
5.3.2.13.4 SG Protocol Design.....617
5.3.2.13.5 Detailed SG Requirements.....621
5.3.2.14 Customer Edge Router Requirements.....643
5.3.2.14.1 Traffic Conditioning 643
5.3.2.14.2 Differentiated Services Support.....643
5.3.2.14.3 Per Hop Behavior Support 644
5.3.2.14.4 Interface to the LSC/MFSS for Traffic Conditioning 644
5.3.2.14.5 Interface to the LSC/MFSS for Bandwidth Allocation.....644
5.3.2.14.6 Network Management.....645

5.3.2.14.7 Availability 645
5.3.2.14.8 Packet Transit Time 645
5.3.2.14.9 Customer Edge Router Throughput Support 645
5.3.2.15 EBC Requirements 647
5.3.2.15.1 AS-SIP Back-to-Back User Agent.....647
5.3.2.15.2 Call Processing Load 649
5.3.2.15.3 Network Management.....649
5.3.2.15.4 DSCP Policing 649
5.3.2.15.5 Codec Bandwidth Policing 649
5.3.2.15.6 Availability 650
5.3.2.15.7 IEEE 802.1Q Support 650
5.3.2.15.8 Packet Transit Time 651
5.3.2.15.9 H.323 Support.....651
5.3.2.16 World Wide Numbering and Dialing Plan 651
5.3.2.16.1 DSN Worldwide Numbering and Dialing Plan 651
5.3.2.17 Management of Network Appliances 666
5.3.2.17.1 Voice and Video Network Management Domain.....667
5.3.2.17.2 General Management Requirements.....668
5.3.2.17.3 Requirements for FCAPS Management.....670
5.3.2.17.4 Data Classification.....680
5.3.2.17.5 Management of Appliance Software 683
5.3.2.18 Network Management Requirements of Appliance Functions.....687
5.3.2.18.1 Management Requirements of the CCA Function 687
5.3.2.18.2 Management Requirements of the SG Function 693
5.3.2.18.3 Management Requirements of the MG Function 712
5.3.2.19 Accounting Management.....720
5.3.2.19.1 Accounting Data 721
5.3.2.19.2 Processing of Data Sets.....731

5.3.2 Assured Services Requirements

5.3.2.1 Introduction

This section addresses required functionality, performance, capabilities, and associated technical parameters for the assured services components of the DISN Voice over IP (VoIP) and Video over IP services. The assured services components described include the End Instrument (EI), Local Session Controller (LSC), Multifunction Softswitch (MFSS), Edge Boundary Controller (EBC), and Customer Edge Router (CE Router). In addition, appliance functions associated with the assured services components, which include the Call Connection Agent (CCA), Media Gateway (MG), Signaling Gateway (SG), Network Management (NM), and the Open Loop Assured Services Admission Control (ASAC) technique, to be employed by the system, are described and specified in detail.

The sensitive, but unclassified (SBU) Voice and Video over IP (VVoIP) services are specified; the classified VVoIP services are specified in UCR 2008, Section 6.2, Unique Classified Requirements. These voice and video services are assumed to be implemented on a converged base/post/camp/station (B/P/C/S) local area network (LAN) and the converged DISN wide area network (WAN). For the purposes of this UCR section, converged means that all types of services, as defined by the Net-Centric Implementation Document (NCID) Version 2 (NCIDv2) Quality of Service (QoS) (T300), are existing simultaneously on the same IP network. Nevertheless, networks may still be separated due to security issues, as specified in UCR 2008, Section 5.4, Information Assurance Requirements. However, the Global Information Grid (GIG) goal is one "black core" transporting all service types and all classification levels using High Assurance Internet Protocol Encryptor (HAIPE) encryption beginning at the DISN Service Delivery Nodes (SDNs), then moving to the B/P/C/Ss and eventually moving to the EIs/servers.

A "call" is a VoIP or Video over IP call that is placed or answered by an EI end user, and a "session" is the underlying Assured Service Session Initiation Protocol (AS-SIP)/Proprietary VoIP session that is processed by the EI and the LSC. The human end users see the VoIP or Video over IP "call," and the assured services network devices, such as the EI and the LSC, see the underlying AS-SIP or Proprietary VoIP "session." "Call" is a "human end-user perspective" term, and "session" is a technical term describing the VoIP signaling and media streams in the appliance that supports an individual end user's call.

5.3.2.1.1 Requirements Terminology

The terms Required and Objective are used in this section.

Requirements are designated as Required or Conditional as defined in the UCR 2008, Section 5.1.4, General Specification Language. In addition, the term Objective is used in this section.

Objective requirements are desirable, but do not have to be deployed until the Final Operational Capability (FOC) of the system. A function or capability may be desired for Initial Operational Capability (IOC) **[Objective: IOC]** and required for FOC **[Required: FOC]**.

In addition, some requirements may be labeled as "Conditional – Tactical." This is a variation of the "Conditional" case, where the requirement is Required for strategic appliances, such as LSCs and MFSSs in strategic DoD networks, but is Conditional for tactical appliances, such as LSCs in tactical DoD networks. In other words, Conditional – Tactical means "Required for Strategic Appliances but Conditional for Tactical Appliances."

The term appliance and its relationship to Approved Product List (APL) products are defined in UCR 2008, Section 5.3.2.1.5, Functional Reference Terminology – APL Products and Appliances.

5.3.2.1.2 Network Reference Model

Figure 5.3.2-1, High-Level DISN Assured Services Network Model, shows a typical arrangement of an LSC and an MFSS in the DISN Assured Services voice and video network. This high-level DISN network model was used as the basis for the requirements for the LSC and MFSS in this section.

The network is a hierarchical network supporting:

- Local services and features within an Edge Segment (B/P/C/S)
- Global services and features across the GIG network
- Services and features to DoD allied networks, DoD coalition networks, and the external Public Switched Telephone Network (PSTN)

The network consists of UC APL products, such as the LSC and the MFSS. These products are interconnected via the converged IP transport network to support the following necessary functions for global services and features:

- Signaling functions (e.g., call control and feature control signaling)
- Bearer functions (e.g., interworking between packetized voice and Time-Division Multiplexing (TDM) voice media streams, support for various media stream Coder/Decoders (codecs))

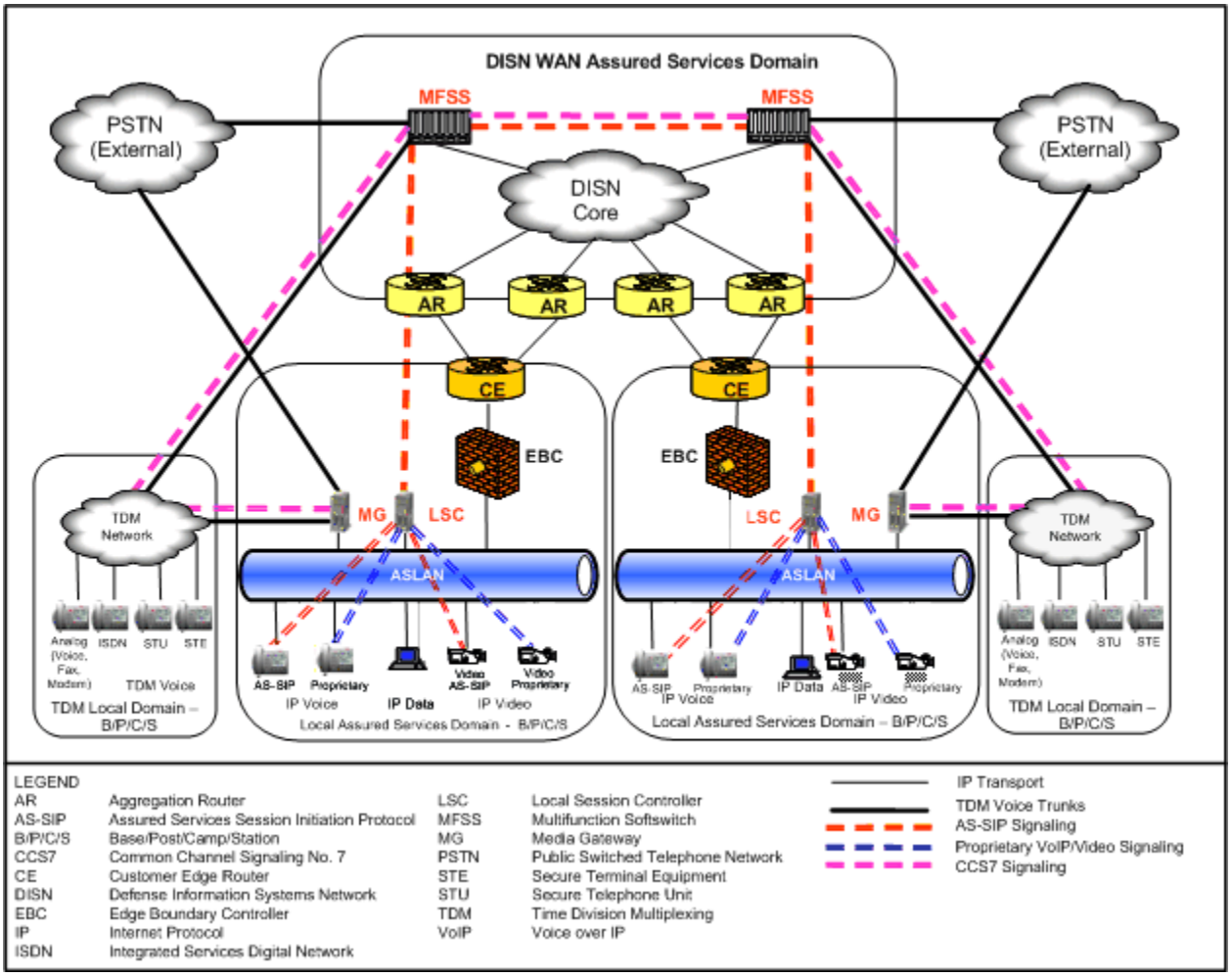


Figure 5.3.2-1. High-Level DISN Assured Services Network Model

- Management functions (e.g., appliance fault, configuration, accounting, performance, and security (FCAPS) management)

- Information Assurance (IA) functions

At IOC, the network is expected to allow existing TDM trunk and signaling link connectivity to remain, including

- Primary Rate Interface (PRI), Channel Associated Signaling (CAS), and DoD Common Channel Signaling No. 7 (CCS7) trunks and signaling links between MFSSs, and

- PRI, CAS, and DoD CCS7 trunks and signaling links between LSCs and MFSSs.

In addition, PRI, CAS, and DoD CCS7 connectivity from MFSSs to other DoD TDM switches will still exist in the network.

5.3.2.1.3 General Assumptions

The following five general assumptions apply to the components described throughout this section (The assumptions apply to the CCA, SG, and NM. In addition, the assumptions were used to develop VoIP, Facsimile over IP (FoIP), Modem over IP (MoIP), Secure Communications Interoperability Protocol (SCIP) over IP, and Integrated Services Digital Network (ISDN) over IP requirements for the MG within the UCR 2008.):

1. The LSC and MFSS will support 911 services for VoIP and TDM end users. Within the United States, 911 calls from VoIP and TDM lines may be routed to either a DoD Emergency Response Center, or to a PSTN 911 Selective Router (SR) and Public Safety Answering Point (PSAP), depending on the LSC or MFSS configuration. The emergency services network that handles DoD and PSTN 911 calls may be TDM-based or IP-based. Outside the United States, 911 calls from VoIP and TDM lines may be routed to a DoD Emergency Response Center (if one exists within the DoD location), depending on the LSC or MFSS configuration.

   The details of the 911 service infrastructure within the network are outside of the scope of the CCA VoIP and Video over IP requirements in this section.

2. In some cases a function like an Media Gateway Controller (MGC) or MG will be labeled as Conditional – Tactical in this section. In these cases, Conditional – Tactical means that normally this function is not used in a tactical environment, but may be used in that environment under certain conditions. When this function is used in that environment, the function should conform to the MG requirements in this section. For example, an LSC deployed in one camp in a war zone overseas may not use an MGC or an MG, while another LSC deployed in another camp in the same zone may use both of them.

3. The CCA VoIP, FoIP, MoIP, SCIP over IP, and ISDN over IP requirements in this section assume that all functions within an individual appliance (LSC or MFSS) are provided by the same appliance supplier. Within a collection of network appliances, all appliances may be provided by the same supplier, or some appliances may be provided by one supplier and other appliances may be provided by other suppliers.

4. Interoperability between LSCs, MFSSs, and the MG requirements in this section is the goal of the UCR 2008. Integration between the functions within an individual LSC or MFSS is the responsibility of the network appliance supplier.

5. "Assured Services for Voice and Video" supports VoIP, voiceband FoIP, voiceband data (modems) over IP, SCIP over IP, ISDN over IP, and Video over IP. The voice budgets used to manage end users' VoIP calls will collectively manage those users' VoIP calls, FoIP calls, MoIP calls, and SCIP over IP calls. The separate video budgets used to manage end users' Video over IP calls will manage those users' Video over IP calls only, and will not manage any VoIP, FoIP, MoIP, or SCIP over IP calls for those users. In short, VoIP budgets and Video over IP budgets are maintained and managed separately in Voice and Video Assured Services.

Other assumptions are as follows:

1. The MFSS is assumed to support AS-SIP connectivity (for connections to other MFSSs and LSCs) and TDM connectivity (for connections to other MFSSs and DoD TDM switches). The TDM connectivity can use CCS7, PRI, or CAS signaling.

2. The LSC is assumed to include an MGC and an MG **[Required: Strategic – Conditional: Tactical]**, and an SG **[Conditional]**, which means that the TDM trunk groups that terminate on the LSC MG can use PRI, CAS, or CCS7 signaling.

3. The MFSS supports end users on both the softswitch (VoIP) side (i.e., VoIP end users using VoIP EIs) and on the TDM/End Office (EO) side (i.e., end users with traditional TDM-based telephones).

4. The MFSS supports TDM trunks on both its softswitch side (through the MGC and MG) and the TDM side. Interworking between the TDM side and the softswitch side of the MFSS is considered to be an internal interface within the MFSS product. The internal interface may employ CCS7 to AS-SIP conversion via an SG or ISDN-PRI, or CAS via an MG.

5. The VoIP signaling protocol used between the VoIP EI and the LSC (and between the VoIP EI and the LSC part of an MFSS) can be vendor-proprietary. The VoIP signaling protocol does not need to be AS-SIP between a VoIP EI and LSC (or between the VoIP EI and the LSC component of an MFSS) in the IOC time frame. However, the VoIP signaling protocol used between VVoIP signaling appliances (i.e., LSCs and MFSSs) is required to be AS-SIP in the IOC time frame.

6. The LSC and the MFSS will both use Location Services (Local or Global, as needed) to route calls to their intended destination. Location Services will be supported as an internal function of the LSC or MFSS, instead of an external function that the LSC or MFSS would have to access over an external interface using an industry-standard Location Services protocol.

7. Route selections at the LSCs and the MFSS will be based on the originating call signaling type (i.e., either IP or TDM signaling). If the originating signaling is IP based, it is assumed that the call signaling will stay IP based for as long as possible, as the signaling transits the network. Similarly, if the originating call signaling is TDM based, the call signaling will stay TDM-based for as long as possible as the signaling transits the network.

8. Tones and announcements that are provided to VoIP end users will be provided from an internal media server, which is a functional component of the LSC or MFSS. An external media server that is separate from the LSC or MFSS is not envisioned.

9. The CCA VoIP and Video over IP requirements in this section assume that all functions within an individual appliance (e.g., LSC or MFSS) are provided by the same appliance supplier. Within a collection of network appliances, all appliances may be provided by the same supplier, or some appliances may be provided by one supplier and other appliances may be provided by other suppliers, but will be offered as part of a single APL product.

10. The LSC supports MGC and MG functionality, so that LSCs can support access to DoD TDM networks, allied TDM networks, coalition partner TDM networks, and the local PSTN, when this access is needed in both strategic and tactical environments. In addition, the LSC supports MGC and MG functionality to enable TDM connectivity (i.e., PRI, CAS, and CCS7 trunks and signaling links) to interconnecting MFSSs when it is needed.

11. The LSCs and MFSSs will support proprietary VoIP videophones (using the vendor's version of Session Initiation Protocol (SIP) or H.323, Cisco's Skinny protocol) in the IOC time frame. The LSC and MFSS suppliers may support AS-SIP videophones in the IOC time frame, but are not required to. The LSC and MFSS suppliers are required to support protocol interworking between their videophones (Proprietary VoIP and AS-SIP) and the AS-SIP protocol used on network-side interfaces between LSCs and MFSSs (and between LSCs, and between MFSSs) in the IOC time frame.

5.3.2.1.4 Information Assurance

Information Assurance Requirements are described in UCR 2008, Section 5.4, Information Assurance Requirements.

The IA function within the products and appliance functions ensures that end users, EIs, MGs, SGs, and EBCs that use the appliance are all properly authenticated by the appliance. The IA function also ensures that VoIP signaling streams and media streams that traverse the appliance and its Assured Services Local Area Network (ASLAN) are encrypted properly (using SIP/Transport Layer Security (TLS) and Secure Real Time Protocol (RTP) (SRTP), respectively).

5.3.2.1.5 Functional Reference Terminology – APL Products and Appliances

This paragraph describes relationships between VoIP and Video over IP network components, appliance functions, and UC products to be tested for APL certification. The term "appliance function" is introduced because IP-based UC APL products will often consist of software functions and features (e.g., appliances) that are distributed over several hardware components connected over a network infrastructure (e.g., LAN), while a TDM-based APL product, such as an EO,consists of a single unit containing all required telephony functions. Appliances operate at the signaling, bearer, and NM planes. Appliance functions are described and referred to throughout the UCR 2008, but are not considered products for APL certification, but rather functions and features that form a part of a UC APL product. Table 5.3.2-1, Summary of Appliances and UC APL Products, provides a summary of appliances and APL products.

Table 5.3.2-1. Summary of Appliances and UC APL Products

ITEM	ITEM CATEGORY	ROLE AND FUNCTIONS
EI	Appliance	Appliance part of LSC
MG	Appliance	Media conversion function as part of the LSC and MFSS
SG	Appliance	Signaling conversion function as part of the LSC and MFSS
AS-SIP Signaling Appliance	Appliance	Appliance function within an LSC and MFSS that provides AS-SIP signaling capability
CCA	Appliance	Appliance function within an LSC and MFSS that performs parts of session control and signaling functions
Registrar	Appliance	Appliance function that stores the location of a registrant and its profile
Registrant	Appliance	Appliance function used to register with the network to seek and gain authority to invoke services or resources from the network
LAN Switch/Router (Access, Distribution, and Core)	APL Products	APL products used in an ASLAN
SEI	APL Product	System consisting of a single appliance
LSC	APL Product	System providing many local telephony functions
MFSS	APL Product	Large, complex system providing many local and WAN-related telephony functions
EBC	APL Product	System providing firewall functions
CE Router	APL Product	System providing routing functions at the enclave boundary
DISN WAN P/PE Router	APL product	System providing routing of IP packets
DISN MSPP	APL Product	System providing transport access to the DISN WAN
M1-3 Multiplexer	APL Product	System providing transport interface to the DISN
DISN Optical Switch	APL product	System serving as an optical transport node

ITEM	ITEM CATEGORY	ROLE AND FUNCTIONS

LEGEND

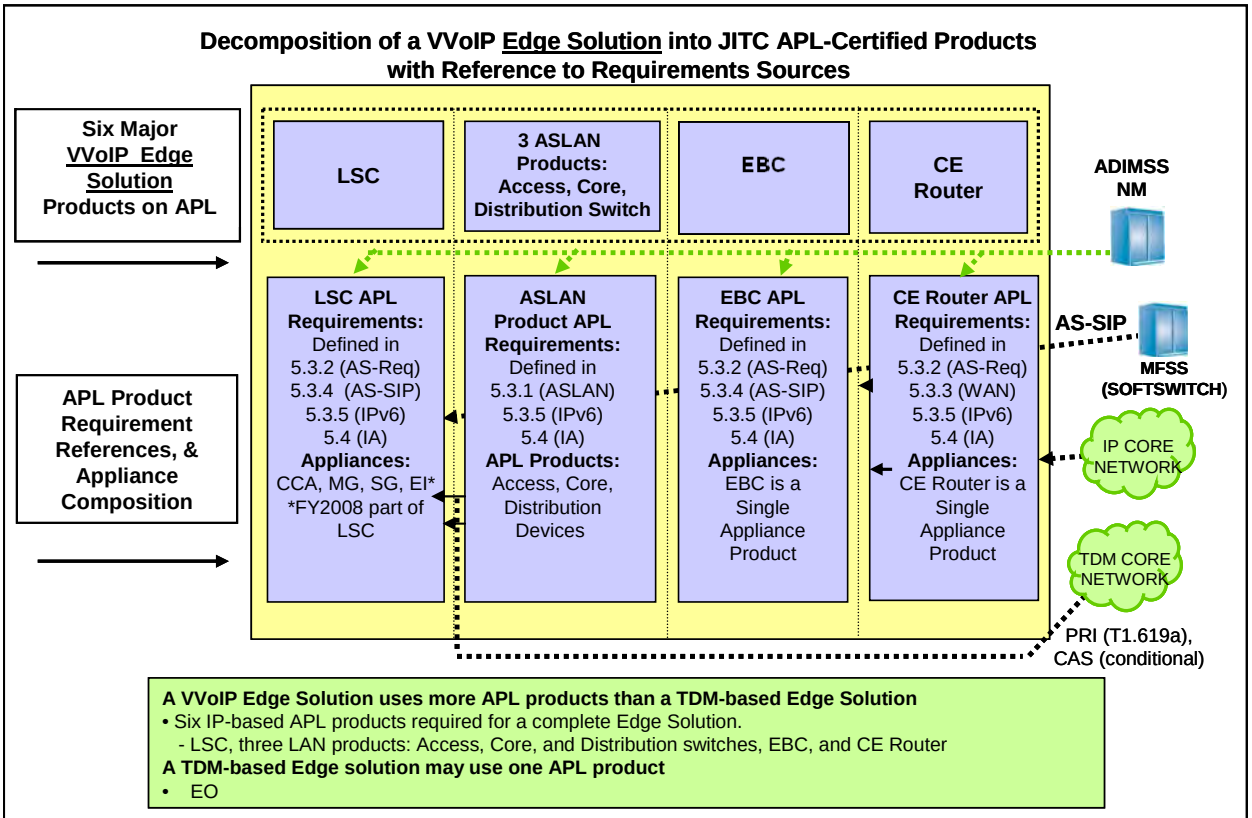
APL	Approved Products List	LSC	Local Session Controller
ASLAN	Assured Services Local Area Network	MFSS	Multifunction Softswitch
AS-SIP	Assured Services Session Initiation Protocol	MG	Media Gateway
CCA	Call Connection Agent	MSPP	Multi-Service Provisioning Platforms
CE	Customer Edge	P	Provider
DISN	Defense Information Systems Network	PE	Provider Edge
EBC	Edge Boundary Controller	SEI	Secure End Instrument
EI	End Instrument	SG	Signaling Gateway
IP	Internet Protocol	WAN	Wide Area Network
LAN	Local Area Network		

The architectural differences between TDM-based APL products and IP-based APL products are illustrated further in Figure 5.3.2-2, IP-Based RTS Edge Solution in Terms of the Joint Interoperability Test Command (JITC) APL Approved Systems. The figure illustrates how several appliance functions and APL products replace what is provided by a single TDM-based APL product (e.g., DSN EO) to provide telephone service on a B/P/C/S.

Figure 5.3.2-2 illustrates how an IP-based edge solution is composed of JITC APL components.

Figure 5.3.2-3, Functional Reference Model for an MFSS, and Figure 5.3.2-4, Functional Reference Model for an LSC, represent the DISN Reference Functional Model for an MFSS and for an LSC. The two figures illustrate appliance functions internal to the MFSS and LSC UC products configurations. The appliance functions, which include the CCA, Interworking Function (IWF), MGC, SG, and MG are described in subsequent paragraphs within this section.

All interfaces between appliances contained with the MFSS and LSC shown in Figure 5.3.2-3 and Figure 5.3.2-4 are internal, proprietary interfaces. Interfaces between one APL product and functional entities in physically different APL products are standards-based external interfaces.



LEGEND

ADIMSS	Advanced DSN Integrated Management Support System	IPv6	Internet Protocol Version 6
APL	Approved Products List	JITC	Joint Interoperability Test Command
ASLAN	Assured Service Local Area Network	LAN	Local Area Network
AS-SIP	Assured Services Session Initiation Protocol	LSC	Local Session Controller
CAS	Channel Associated Signaling	MFSS	Multifunction Softswtich
CCA	Call Connection Agent	MG	Media Gateway
CE	Customer Edge Router	NM	Network Management
FY	Fiscal Year	PRI	Primary Rate Interface
EBC	Edge Boundary Controller	SG	Signaling Gateway
EI	End Instrument	TDM	Time Division Multiplexing
IA	Information Assurance	VVoIP	Voice and Video over IP
IP	Internet Protocol	WAN	Wide Area Network

Figure 5.3.2-2. IP-Based Voice Edge Solution in Term of JITC APL Approved Systems

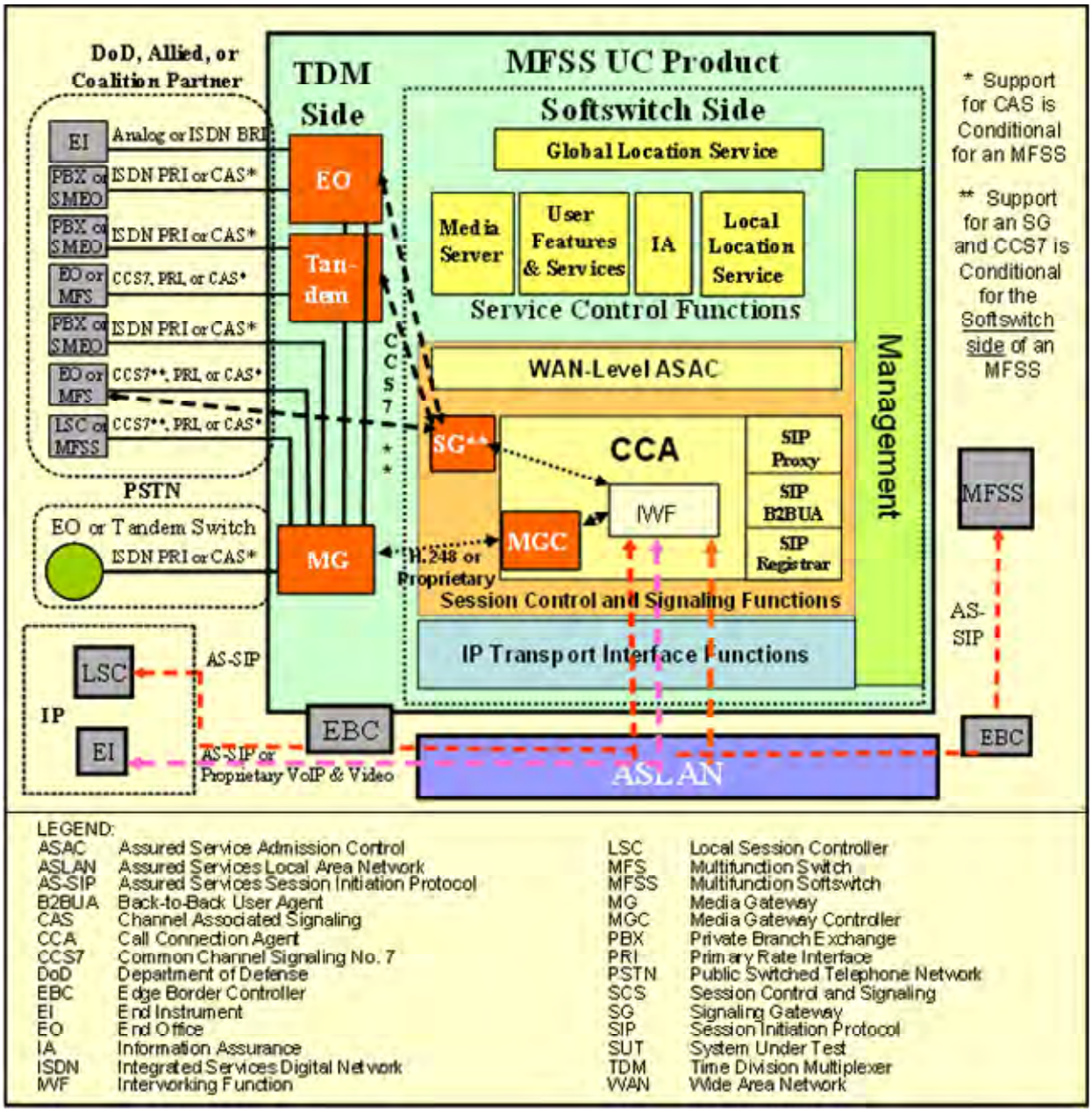


Figure 5.3.2-3. Functional Reference Model – MFSS

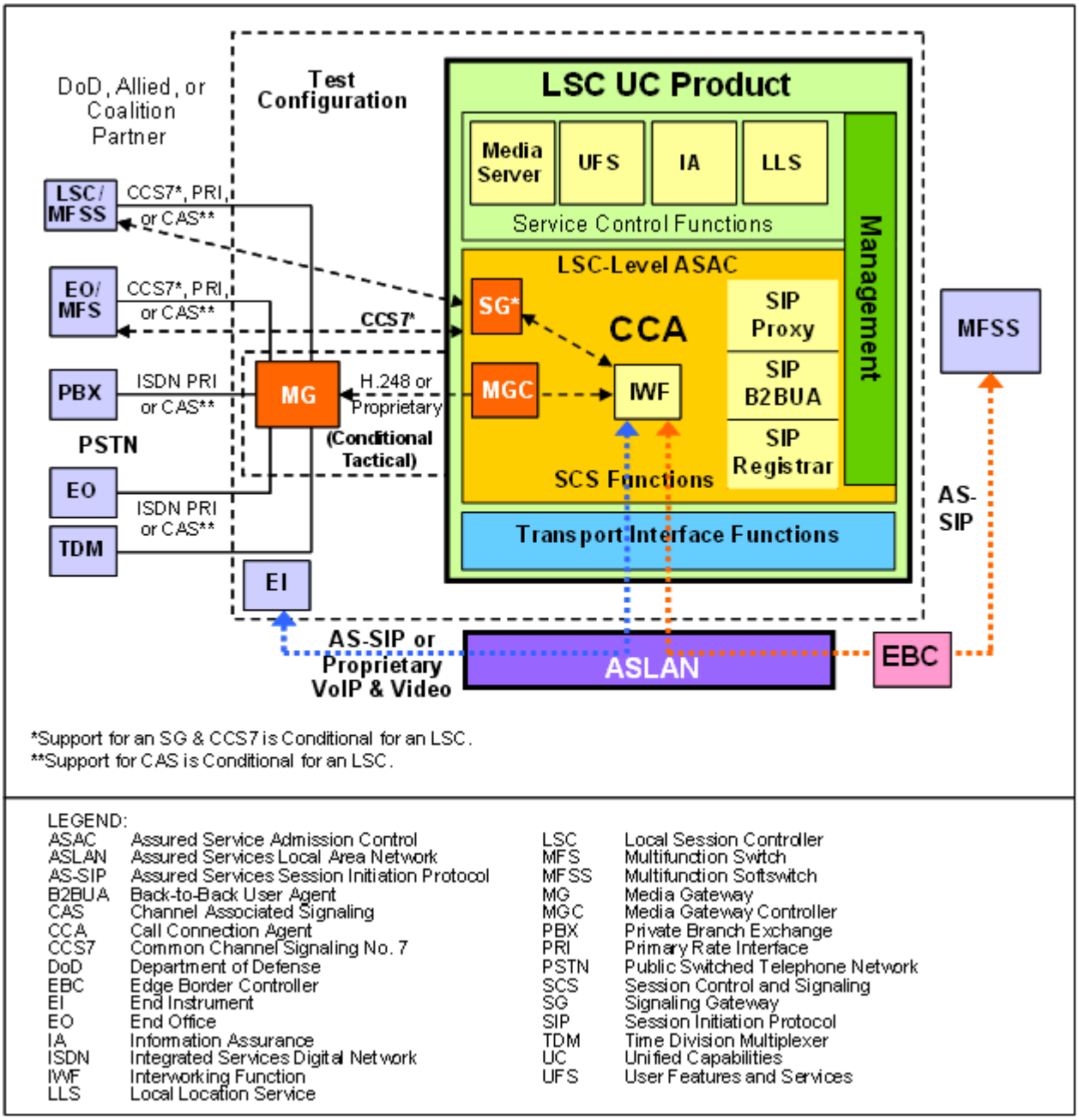


Figure 5.3.2-4. Functional Reference Model – LSC

5.3.2.2 Assured Services System Features and Capabilities

5.3.2.2.1 Overview of VoIP and Video over IP System Design Attributes

A key component of the military robust VoIP and Video over IP system design is the Assured Services subsystem. The Assured Services subsystem addresses Military-Unique Features

(MUFs) by replacing the current TDM-based Multilevel Precedence and Preemption (MLPP) functionality with IP-based ASLANs and ASAC. The Assured Services subsystem, in conjunction with the ASLAN subsystem, and the DISN WAN subsystem make up the total system that is required to initiate, supervise, and terminate voice and video, precedence and preemption sessions on an EI to EI basis, while functioning within a converged total DoD GIG network.

The logical location of the major VoIP and Video over IP attributes within the GIG End-to-End (E2E) system is shown in Figure 5.3.2-5, Overview of VVoIP System Design Attributes. The location of attributes in terms of Edge (B/P/C/S), the network infrastructure (access and DISN Core) is depicted, and the differentiation between assured service and non-assured service is shown between the top half of the diagram and the bottom half of the diagram, respectively.

The functions contained in the boxes located within the top half of Figure 5.3.2-5 constitute the scope of the Assured Services subsystem while the placement of the boxes indicates where in the overall VoIP and Video over IP system design (WAN to Edge) the functions logically reside. Voice, video, and data sessions are converged in the DISN WAN and the ASLAN, while the Assured Services subsystem in FOC is anticipated to support voice, video, and non-real-time sessions with priority.

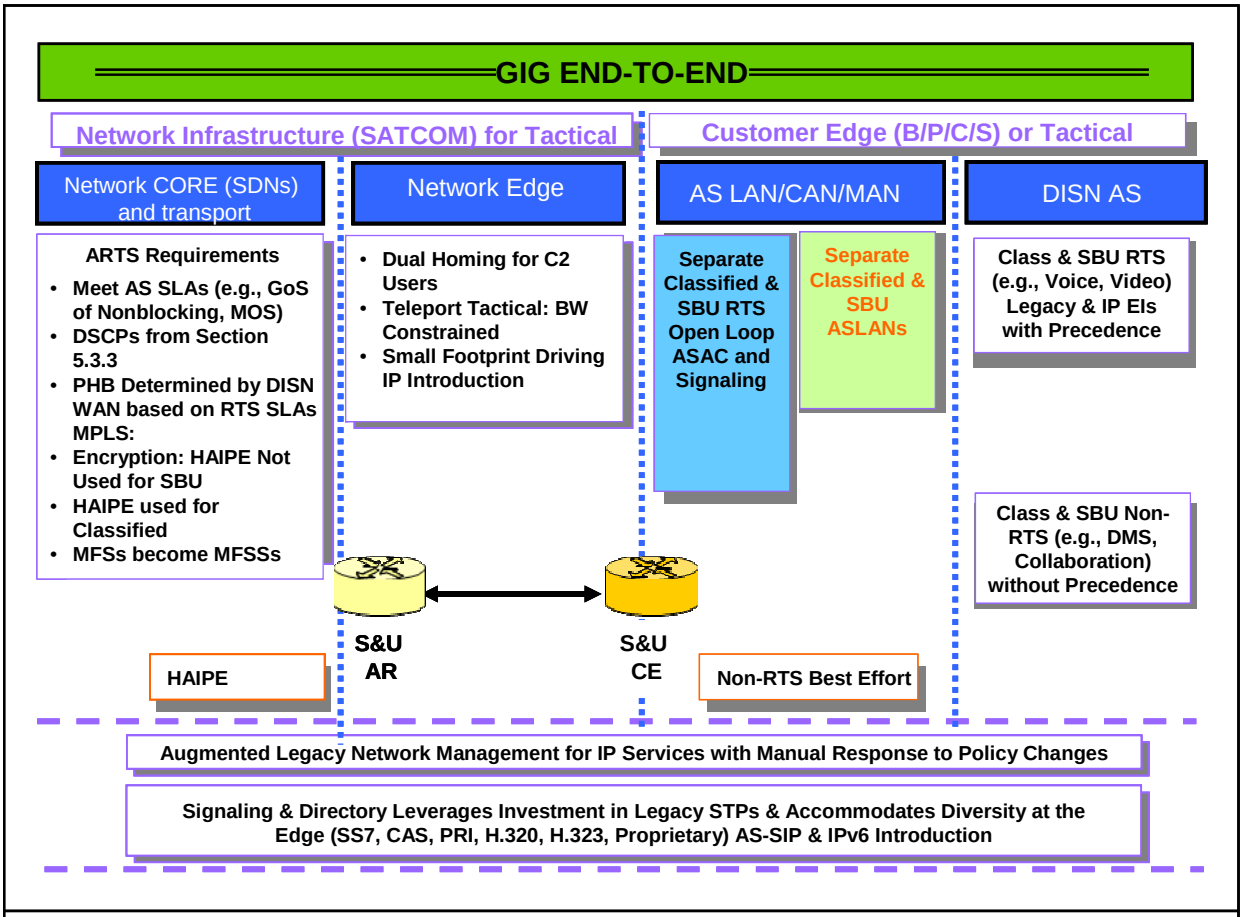
5.3.2.2.1.1 Attributes within the Edge Segment

The attributes within the Edge Segment include the following:

- Non-blocking ASLAN. At the Edge, the IOC design has an ASLAN that is designed as non-blocking for voice and video traffic.

- Traffic Admission Control. The LSCs on a B/P/C/S employ an Open Loop ASAC technique to ensure that only as many user originated sessions (voice and video) in precedence order are permitted on the traffic- engineered access circuit, consistent with maintaining a voice quality of 4.0 as measured by the Mean Opinion Score (MOS) method.

- Call Preemption. Lower precedence sessions will be preempted on the access circuit in order to accept the LSC setup of a higher precedence level outgoing or incoming session establishment requests.



LEGEND:

AR	Aggregated Router	DSCP	Differentiated Services Code Point	MPLS	Multiprotocol Label Switching
ARTS	Assured Real Time Services	EI	End Instrument	NCID	Net-Centric Implementation Document
AS	Assured Services	GIG	Global Information Grid	PHB	Per Hop Behavior
ASAC	Assured Services Admission Control	GOS	Grade of Service	PRI	Primary Rate Interface
ASLAN	Assured Services LAN	HAIPE	High Assurance Internet Protocol Encryptor	RTS	Real Time Services
AS-SIP	Assured Services SIP	IP	Internet Protocol	S&U	Secure and Unsecure
B/P/C/S	Base/Post/Camp/Station	IPv6	Internet Protocol version 6	SATCOM	Satellite Communications
BW	Bandwidth	LAN	Local Area Network	SBU	Sensitive But Unclassified
C2	Command and Control	MAN	Metropolitan Area Network	SDN	Service Delivery Node
CAS	Channel Associated Signaling	MFS	Multifunction Switch	SLA	Service Level Agreement
DISN	Defense Information Systems Network	MFSS	Multifunction Softswitch	SS7	Signaling System No. 7
DMS	Defense Message System	MOS	Mean Opinion Score	STP	Signal Transfer Point

Figure 5.3.2-5. Overview of VVoIP System Design Attributes

- Voice and Video Traffic Service Classification and Priority Queues. In terms of the Customer Edge Router (CE Router) queuing structure, voice and video traffic will be assigned to the higher priority queues by Aggregated Service Class as described in UCR 2008, Section 5.3.3, Network Infrastructure End-to-End Performance Requirements.

5.3.2.2.1.2 Attributes within the DISN WAN (Access/Distribution and Core)

Note that under the access part of the DISN WAN, dual homing is required between the CE Router and the Aggregation Router (AR) that serve an ASLAN. In 2008, SBU ASLANs do not use HAIPEs. The DISN Core part of the DISN WAN is assumed to be bandwidth rich, i.e., the bandwidth from the AR to AR, for whatever AR queue the voice and video traffic is placed in, is greater than or equal to the voice and video traffic-engineered load/bandwidth required for the voice/video busy hour traffic in each of the DISN worldwide geographic locations. Since the ASLAN is required to be implemented as non-blocking for voice and video traffic, the access circuit from the Customer Edge Segment to the DISN Core SDN is the only potential bandwidth limited resource requiring the use of ASAC to prevent session overload from the Edge Segment. The DISN WAN provides high availability (99.96 percent or greater) through the use of dual-homed access circuits and the Multiprotocol Label Switching (MPLS) fast reroute (FRR) in the Network Core. Naturally, users are provided a lower availability if they choose not to or cannot implement dual homing.

5.3.2.2.1.3 End-to-End Protocol Planes

End-to-end services are set up, managed, and controlled by a series of functions or protocols that operate in three planes commonly referred to as: signaling, bearer, and NM planes.

The signaling plane is associated with the signaling and control protocols, such as AS-SIP, H.323, and Resource Reservation Protocol (RSVP).

The transport plane is associated with the bearer traffic and protocols, such as SRTP and Real-Time Control Protocol (RTCP).

The NM plane is associated with NM protocols and is used to transfer status and configuration information between a Network Management System (NMS) and a network appliance. Network management protocols include: Simple Network Management Protocol (SNMP), Common Open Policy Service (COPS), and Secure Shell Version 2 (SSHv2).

5.3.2.2.1.4 Differentiated Services Code Point Packet Marking

[Required: EI, LSC, MFSS] As part of the session setup process, the LSC controls what Differentiated Services Code Point (DSCP) to use in the subsequent session media stream packets.

For inter-LSC media sessions (across the WAN):

- the EI shall be commanded by the LSC as to what DSCP to insert in the session media stream packets, or
- the EI shall populate the DSCP marking on its own.

[Required: EI, LSC, MFSS] The exact DSCP method employed by the implementer shall comply with UCR 2008, Section 5.3.3 Network Infrastructure End-to-End Performance Requirements. The condition here is that the NCIDv3 QoS document is approved and available to implementers of VVoIP.

[Required: EI, LSC, MFSS] For intra-LSC media streams (internal to the enclave):

- the EI shall be commanded by the LSC as to what DSCP to insert in the session media stream packets; or
- the EI shall populate the DSCP marking on its own; or
- the EI shall use a standard ROUTINE DSCP marking for all voice media streams (or video media streams) in accordance with UCR 2008, Section 5.3.3, Wide Area Network Requirements.

5.3.2.2.2 Assured Services Subsystem

The Assured Services subsystem, shown in Figure 5.3.2-6, Assured Services Subsystem Functional Diagram, the DISN WAN subsystem (see UCR 2008, Section 5.3.3, Network Infrastructure End-to-End Performance Requirements), and the ASLAN subsystem (see UCR 2008, Section 5.3.1, ASLAN Infrastructure Product Requirements) make up the total system. These subsystems are required to initiate, supervise, and terminate voice and video, precedence and preemption sessions on an EI-to-EI basis, while functioning within a converged DoD network.

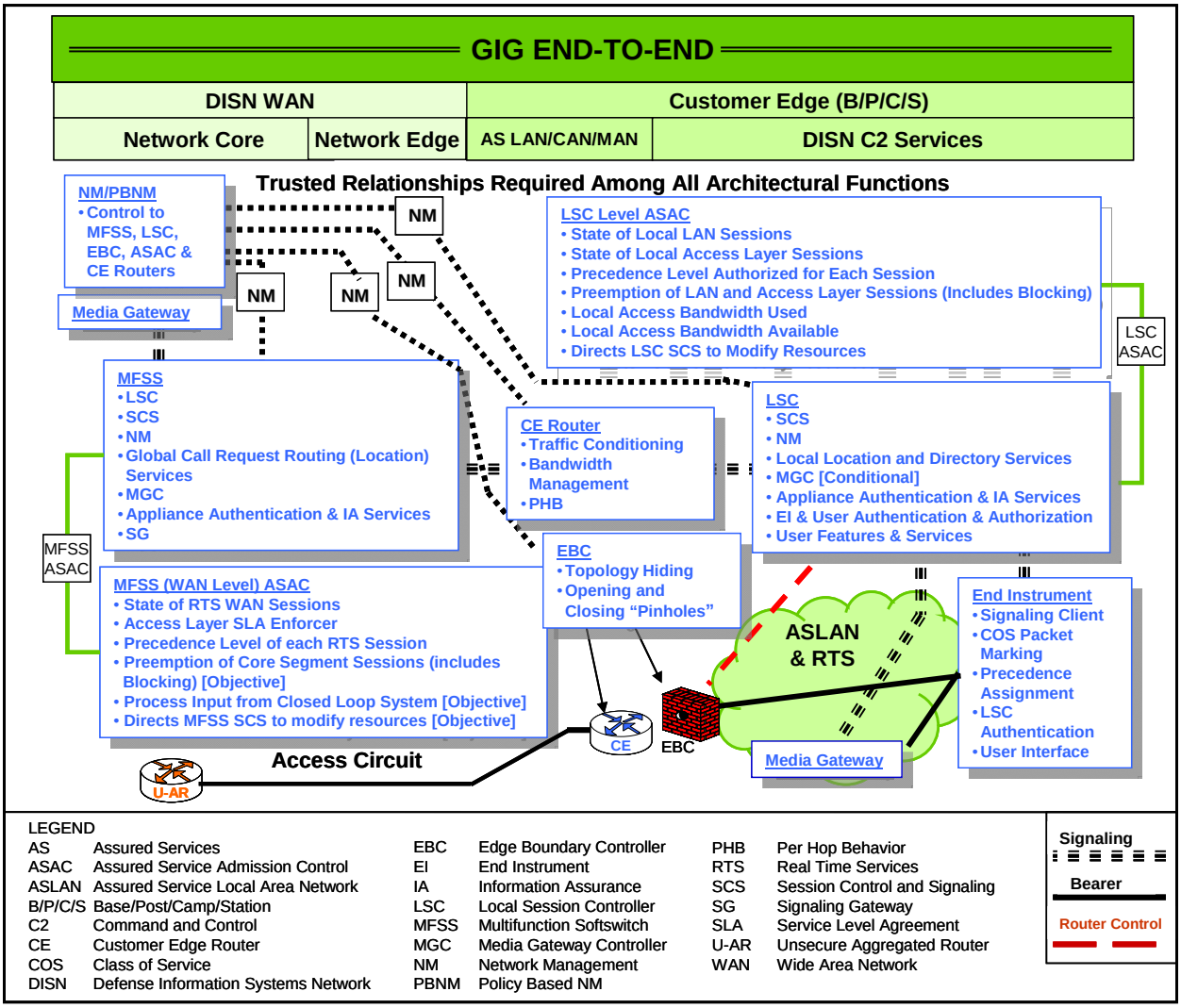


Figure 5.3.2-6. Assured Services Subsystem Functional Diagram

The functions contained in the Figure 5.3.2-6 boxes and the EBC router symbol constitute the scope of the Assured Services subsystem while the placement of the boxes indicates where in the overall system (WAN to Edge) the functions logically reside.

Voice, video, and data sessions are converged in the DISN WAN and the ASLAN, while in IOC assured services are provided for voice and video sessions only.

The functional behavior and performance metrics for each of the assured services major functions defined by a box in Figure 5.3.2-6 and subordinate functions listed within each box are specified in this section. Also, the interfaces between the major functional groupings (defined by a box) are specified in terms of electrical interfaces, protocols operating over these electrical interfaces, and their associated parameters. Best commercial practices and existing standards

will be specified to the maximum extent possible, and any deviations or enhancements to these will be specified in detail.

The following list of capabilities and functional elements are defined and specified:

- Legacy and IP EIs with precedence marking capability
- The ability to complete a higher precedence session to a busy EI by interrupting the current session
- ASAC as part of the LSC functions
- EBC (firewall/ CE Router)
- Local call control (LSC)
- Session control and signaling (SCS)
- Local and global directories
- User Features and Services (UFS) (voicemail and attendant services)
- Network level call control (MFSS)
- MGC
- MGs
- Media gatekeeper (H.323)
- NM with Policy Based Network Management (PBNM)

5.3.2.2.2.1 Voice Features and Capabilities

This section describes assured services capabilities and characteristics together with the design and performance metrics associated with each capability or characteristic. For the sake of brevity, the rationale behind the selected metrics will not be provided in this section, but references to other sections and documents will be provided where available. The Government retains the right to change, modify, or alter any of the specified capabilities or characteristics and performance metrics as requirements and technology mature. Table 5.3.2-2, Assured Services System Features and Capabilities, summarizes the system feaures and capabilities

Table 5.3.2-2. Assured Services System Features and Capabilities

	FEATURE AND CAPABILITY	UCR 2008 SECTION	UCR 2008 GRAPHIC	REFERENCE DOCUMENT
1.	Precedence Call (Session) Waiting **[Required]**	• Sections 5.2.2.2.1 through 5.2.2.2.4 • Section 5.2.2.1.1 • Section 5.2.2.1.4 • Section 5.2.2.3 • Section 5.2.2.6.2.1 • Sections 5.2.2.8.1 through 5.2.2.8.1.4 • Section 5.2.2.8.6	• Table 5.2.4-5	• Telcordia Technologies GR-571-CORE • Telcordia Technologies GR-572-CORE
2.	Call (Session) Forwarding **[Required]**	• Sections 5.2.2.2.1 through 5.2.2.2.4 • Section 5.2.2.3		• Telcordia Technologies GR-580-CORE • Telcordia Technologies GR-586-CORE
3.	Call (Session) Transfer **[Required]**	• Section 5.2.2.2 • Sections 5.2.2.8.3 through 5.2.2.8.3.2		
4.	Call (Session) Hold **[Required]**	• Section 5.2.2.2 • Section 5.2.2.3		
5.	Preset Conferencing **[Objective]**	• Section 5.2.1.6.1		
6.	Three-Way Calling **[Required]**	• Section 5.2.1.1.6		
7.	Release to Pivot **[Objective]**	• Section 5.2.1.2.8		
8.	Hotline Service **[Required]**	• Sections 5.2.1.12 through 5.2.1.12.4 (inclusive) • Sections 5.2.2.4 through 5.2.2.4.3		
9.	Calling Party and Called Party ID (number only) **[Required]**			• Telcordia Technologies GR-317-CORE

5.3.2.2.2.2 Public Safety Features

5.3.2.2.2.2.1 Basic Emergency Service (911)

[Required: LSC, MFSS] The Basic 911 Emergency Service feature provides a 3-digit universal telephone number (911) that gives the public direct access to an emergency service

bureau. The emergency service is one-way only, terminating to the service bureau. A given local switching system shall serve no more than one emergency service bureau. When the originating line and the emergency service bureau are served by the same switching system, the bureau has the capability of holding and disconnecting the connection and monitoring the supervisory state, and ringing the originating station back. When the local switching system is in an area with enhanced emergency service (E911) served through a tandem switch, the emergency call is advanced to the tandem switch with calling line Automatic Number Identification (ANI) or Calling Number Delivery (CND).

The LSC and MFSS may support 911 services for VoIP and TDM end users. Within the United States, 911 calls from VoIP and TDM lines may be routed to either a DoD Emergency Response Center, or to a PSTN 911 SR and PSAP, depending on the LSC or MFSS configuration. The emergency services network that handles DoD and PSTN 911 calls may be TDM-based or IP-based. Outside of the United States, 911 calls from VoIP and TDM lines may be routed to a DoD Emergency Response Center (if one exists within the DoD location), depending on the LSC or MFSS configuration.

Calling 911 from an LSC or MFSS shall not require the use of access codes such as 99. Dialing 911 only shall connect to the public emergency service bureau. If this feature is provided, it shall be in accordance with Telcordia Technologies GR-529-CORE, as interpreted for VoIP calls. This feature does not apply to video calls or sessions.

Calls to 911 shall be preempted in accordance with assured service priority rules specified in UCR 2008, Section 5.2.2, Multilevel Precedence and Preemption. This is to reinforce the concept that critical military mission requirements take precedence over other uses of the DISN. NOTE: Precedence calls above ROUTINE can and should preempt 911 calls.

5.3.2.2.2.2.2 Tracing of Terminating Calls

[Required: LSC, MFSS] The Tracing of Terminating Calls feature identifies the calling number on intraoffice and interoffice for calls terminating to a specified directory number (DN). When this feature is activated, the originating DN, the terminating DN, and the time and date are printed out for each call to the specified line.

Requirements for this feature shall be in accordance with Telcordia Technologies GR-529-CORE, FSD 15-03-0000, as interpreted for VoIP calls.

5.3.2.2.2.2.3 Outgoing Call Tracing

[Required: LSC, MFSS] The Outgoing Call Tracing feature allows the tracing of nuisance calls to a specified DN suspected of originating from a given local office. The tracing is

activated when the specified DN is entered. A printout of the originating DN and the time and date, are generated for every call to the specified DN.

Requirements for this feature shall be in accordance with Telcordia Technologies GR-529-CORE, FSD 15-03-0000, as interpreted for VoIP calls.

5.3.2.2.2.2.4 Tracing of a Call in Progress

[Required: LSC, MFSS] The Tracing of a Call in Progress feature identifies the originating DN for a call in progress. The feature is activated by authorized personnel entering a request that includes the specific terminating DN involved in the call.

Requirements for this feature shall be in accordance with Telcordia Technologies GR-529-CORE, FSD 15-03-0000, as interpreted for VoIP calls.

5.3.2.2.2.2.5 Tandem Call Trace

[Required: LSC, MFSS] The Tandem Call Trace feature identifies the incoming trunk of a tandem call to a specified office DN. The feature is activated by entering the specified distant office DN for a tandem call trace. A printout of the incoming trunk number and terminating DN, and the time and date is generated for every call to the specified DN.

Requirements for this feature shall be in accordance with Telcordia Technologies GR-529-CORE, FSD 15-03-0000.

5.3.2.2.2.3 ASAC – Open Loop

[Required: LSC, MFSS] This section presents the ASAC requirements for the LSC and the MFSS. In the execution of ASAC, certain procedures need to be followed, such as (a) actions to be taken if a precedence session request cannot be completed because existing sessions are at equal or higher precedence, or (b) tones to be generated when a session is preempted. UCR 2008, Section 5.2.2, Multilevel Precedence and Preemption, addresses these issues. UCR 2008, Section 5.3.4, AS-SIP Generic System Specification, provides a more detailed description of the session control signaling requirements of the LSC and the MFSS.

5.3.2.2.2.3.1 ASAC Requirements for the LSC and MFSS Related to Voice

[Required: LSC, MFSS] One voice session budget unit shall be equivalent to 110 kilobits per second (kbps) of access circuit bandwidth independent of the EI codec used. This includes ITU-T Recommendation G.711 encoding rate plus Internet Protocol Version 6 (IPv6) packet overhead

plus ASLAN Ethernet overhead. IPv6 overhead, not IPv4 overhead, is used to determine bandwidth equivalents here.

5.3.2.2.2.3.1.1 ASAC Requirements for LSC Related to Voice

5.3.2.2.2.3.1.1.1 LSC States

The states that the LSC must maintain for ASAC purposes are as follows:

1. Line Side States. As a minimum, the LSC shall maintain the session state of each local EI in its domain as follows:

    a. Busy/Not Busy. The Busy State includes the session set up phase and the active session phase.

    b. Session Precedence. If the EI is busy, the state shall include the precedence level of the session (FLASH OVERRIDE (FO), FLASH (F), IMMEDIATE (I), PRIORITY (P), and ROUTINE (R)).

    c. The Line Side States also apply to multi-appearance EIs, but at this time, no more than two line appearances are dealt with, and the procedures are the same as for ISDN Basic Rate Interface (BRI) instruments, as specified in the UCR 2008, Section 5.2, Circuit-Switched Capabilities and Features.

2. Trunk Side States. The following applies only to the CE Router to WAN access circuit and not to multi-appearance EIs:

    a. VoIP Session Budget. If directionalization is not implemented, the LSC and its associated MFSS shall manage the total number of sessions on its IP access link. If directionalization is implemented, the LSC and its associated MFSS shall manage the number of inbound sessions and outbound sessions. An inbound session is one that has been initiated by an EI outside the LSC's domain, whereas an outbound session is one that is initiated by an EI within the LSC's domain. The LSC and its associated MFSS shall be configurable with the following VoIP budgets:

        (1) IPB. The total budget of VoIP sessions plus session attempts in the session set-up phase that are allowed on the IP access link.

        (2) IPBo. The budget for outbound VoIP sessions plus session attempts in the session set-up phase that are allowed on the IP access link.

(a) IPBo may take any value in the range (0, IPB) or "null."
(b) Null implies that there are no outbound directionalization restrictions.

(3) IPBi. The budget for inbound VoIP sessions plus session attempts in the session set-up phase that are allowed on the IP access link.

(a) IPBi may take any value in the range (0, IPB) or "null."
(b) Null implies that there are no inbound directionalization restrictions.

(4) Relationship among IPB, IPBo, and IPBi.

(a) IPBi plus IPBo equals IPB, if there is directionalization.
(b) IPBi equals null if, and only if, IPBo equals null.

b. VoIP Session Counts. The LSC and its associated MFSS shall maintain a running session count for the following VoIP sessions:

(1) IPC. The total number of interbase IP sessions in progress plus the number of session attempts in the session set-up phase.

(2) IPCo. The number of outbound IP sessions in progress plus the number of outbound session attempts in the session set-up phase.

(3) IPCi. The number of inbound IP sessions in progress plus the number of inbound session attempts in the session set-up phase.

c. TDM Session Budget. The following session budget is maintained at each LSC, at its associated gateway, and corresponding EO/Small End Office (SMEO)/Private Branch Exchange 1 (PBX1)/Private Branch Exchange 2 (PBX2) (The LSC and the associated EO/SMEO/PBX1/PBX2 reside on the same B/P/C/S; hence no directionalization is required for TDM sessions.):

– TDMB. The overall number of TDM sessions plus sessions in the session set-up phase on the TDM link. This equals the number of digital signal level 0s (DS0s) on the trunk between the LSC MG and the EO/SMEO/PBX1/PBX2.

d. TDM Session Count. The following session count is maintained at each LSC, at the associated medium gateway, and corresponding EO/SMEO/PBX1/PBX2:

– TDMC. The total number of sessions in progress between the TDM switch and the media gateway plus the total number of session attempts in the session set-up phase.

5.3.2.2.2.3.1.1.2 Session Control Processing with No Directionalization

This section considers the functions carried out by the LSC and the MFSS when IPBo equals IPBi equals null.

1. LSC Processing for an Outbound Session.

a. VoIP Session Processing. If IPBo equals IPBi equals null, the LSC will manage the aggregate session count to assure that IPC does not exceed IPB. If IPBo and IPBi are not null, then the LSC will process the inbound sessions and the outbound sessions individually and independently to assure that they do not exceed IPBi and IPBo, respectively. This section describes the processing for the case when IPBo equals IPBi equals null. The alternate case is identical to this except the LSC performs this function on both the inbound and the outbound VoIP sessions.

Actions taken when an outbound session request is initiated by a local EI are as follows:

(1) Users and/or EIs that place sessions shall be authenticated as per UCR 2008, Section 5.4, Information Assurance Requirement, prior to processing the outbound session.

(2) If IPC is less than IPB, the session request shall be forwarded to the WAN MFSS for forwarding to the sessioned LSC for processing (see item 2, LSC Processing for an Inbound Sessions).

(3) If IPC equals IPB and all existing sessions are at precedence equal to or greater than the new session request, then the LSC shall not place the session and the caller shall receive a Blocked Precedence Announcement (BPA). If it is a ROUTINE call, the caller shall receive a Fast Busy Announcement as per UCR 2008, Section 5.2.2.1.3, Announcements.

(4) If IPC equals IPB and at least one existing session is of lower precedence than the new session, the LSC shall preempt one of the lowest precedence sessions and shall forward the session INVITE (via the MFSS) to the sessioned LSC for processing. The algorithm for selecting the session to preempt shall be deterministic.

(5) IPC is greater than IPB is not an allowed state. If this occurs, the LSC shall deterministically preempt sessions starting with those of lowest precedence until IPC equals IPB, and then proceed as specified in items (3) and (4). The LSC shall notify the NMS of this fault state.

(6) The LSC shall increment and decrement its IPC as follows:

(a) The LSC increments its IPC upon forwarding a session request to the MFSS, which it received from its local EI.

(b) The LSC decrements its IPC upon determining that a session request is completely terminated or an established session is completely terminated.

2. LSC Processing for an Inbound Session. Actions taken by the LSC when a new inbound session INVITE is received from a remote LSC are as follows:

a. If IPC is less than IPB and the local EI is not busy, then the LSC shall place the session.

b. If IPC is less than IPB and the local EI is busy with a session that is of lower precedence than the one being placed, the LSC shall preempt the existing session and place the new session.

c. If IPC is less than IPB and the local EI is busy with a session that is of an equal or higher precedence than the session being placed, the new session is not placed. The caller shall receive a BPA, and if it is a ROUTINE call, the caller shall receive a Fast Busy Announcement as per UCR 2008, Section 5.2.2.1.3, Announcements,

d. If IPC equals IPB and the local EI is not busy, and all existing sessions on the access link are at a precedence equal to or greater than the new session, the LSC shall not place the new session. The caller shall receive a Blocked Precedence Announcement (BPA), and if it is a ROUTINE call, the caller shall receive a Fast Busy Announcement as per UCR 2008, Section 5.2.2.1.3, Announcements.

e. If IPC equals IPB and the local EI is not busy, and at least one existing session on the access link is of a lower precedence than the new session, the LSC shall deterministically preempt one of the lowest precedence sessions, and then shall forward the session INVITE to the sessioned LSC via the MFSS for processing.

f. If IPC equals IPB and the local EI is busy with a session that is of a lower precedence than the new session, then the LSC shall preempt the session and forward the session INVITE to the local EI.

g. If IPC equals IPB and the local EI is busy with a session that is of an equal to or higher precedence than the new session, the LSC shall not place the session. The caller shall receive a BPA, and if it is a ROUTINE call, the caller shall receive a Fast Busy Announcement as per UCR 2008, Section 5.2.2.1.3, Announcements.

h. The IPC is greater than IPB is not an allowed state. If this occurs, the LSC shall deterministically preempt sessions starting with those of the lowest precedence until IPC equals IPB, and then proceed as specified in items d, e, f, and g. The LSC shall notify the NMS of this fault state.

3. Incrementing and Decrementing the Session Count. The LSC shall increment and decrement its IPC as specified in UCR 2008, Section 5.3.4, AS-SIP Generic System Specification.

4. LSC Processing for a Local Session. A local session is one that is initiated by a local EI intended for another local EI.

a. If the sessioned EI is not busy, the LSC shall complete the session.

b. If the sessioned EI is busy with a session that is of a lower precedence than the new session, the LSC shall preempt the session, and then complete the new session.

c. If the call attempt is at a precedence level above ROUTINE and the local EI is busy with a session that is of an equal to or higher precedence than the new session, the LSC shall not complete it. The caller shall receive a BPA. If the call attempt is a ROUTINE call and the local EI is busy with a session, the caller shall receive a Slow Busy tone as per UCR 2008, Section 5.2.4.5.1, Ringing.

d. The LSC does not modify its IPC when local sessions are connected or disconnected because they do not impact traffic in the access link to the WAN.

e. **[Conditional]** An intrabase session count shall be maintained separately independent of precedence, and when this valve is reached no more ROUTINE precedence level session requests shall be processed for intrabase connection. PRIORITY, IMMEDIATE, FLASH, and FLASH OVERRIDE session requests shall be processed as specified in items a, b, and c.

5.3.2.2.2.3.1.1.3 LSC Session Control Processing with Directionalization

The LSC directionalization requirements are applicable to VoIP sessions transmitted over an IP access link. They are not applicable to TDM sessions because they are transmitted via a local EO/SMEO/PBX1/PBX2. Any directionalization for these sessions will be implemented by the EO/SMEO/PBX1/PBX2.

When IPBo and IPBi are not null, the LSC will keep a running count of IPCo and IPCi to assure that these counts do not exceed their respective budgets. The IPCo processing is carried out independently from that of IPCi. Each process is identical to that carried for IPC for non-directionalization as specified earlier. Since the IPCo and IPCi control processes are independent, an FLASH OVERRIDE inbound session will not be able to preempt a ROUTINE outbound session.

5.3.2.2.2.3.1.2 ASAC Requirements for the MFSS Related to Voice

The signaling for the TDM voice sessions is processed by the media gateway in conjunction with the EO/SMEO/PBX1/PBX2. The MFSS is not involved with intrabase signaling. Consequently, this section considers only those VoIP sessions that are transmitted over the IP access link.

1. MFSS States. The MFSS shall be configurable with the IPB, IPBi, and IPBo budget parameters for each LSC in its domain.

2. MFSS Session Counts. The MFSS shall maintain a running count of IPC, IPCo, and IPCi for each LSC in its domain. It shall do this by monitoring the AS-SIP messages associated with each of its subordinate LSCs as specified in UCR 2008, Section 5.3.4, AS-SIP Generic System Specification.

3. MFSS Session Processing with no Directionalization. Initially, the IPC for each LSC is set to zero. The MFSS shall increment and decrement the IPC as follows:

    a. For outbound sessions:

        (1) After having received a session request (i.e., INVITE) from its local LSC, the MFSS increments the corresponding IPC upon forwarding that session request to the far-end LSC.

        (2) The MFSS decrements its IPC when it determines that a session request is completely terminated or an established session is completely terminated.

b. For inbound sessions:

(1) The MFSS increments its IPC upon transmitting to the far-end LSC a "session accepted" (i.e., 1XX or 2XX) response to an INVITE request that it received from the far-end LSC. (The IPC is not incremented for INVITE requests.)

(2) The LSC decrements its IPC when it determines that a session request is completely terminated or an established session is completely terminated.

4. MFSS Policing. The MFSS shall police each LSC in its domain to assure that the IPC does not exceed IPB.

a. If IPC equals IPB and a LSC attempts to place another session by forwarding a session INVITE to its MFSS, the MFSS shall not forward the session INVITE and shall send an error message to the NMS. The caller shall receive a busy announcement as per UCR 2008, Section 5.2.2.1.3, Announcements.

b. If IPC equals IPB at an LSC_a and its $MFSS_a$ receives a session INVITE intended for LSC_a from another LSC_b or another $MFSS_b$, the $MFSS_a$ shall forward the session INVITE to LSC_a. If LSC_a accepts the session (without preempting another session so that IPC would be greater than IPB), the $MFSS_a$ shall not forward the "session accepted" to the sessioning LSC, and shall send an error message to the NMS. The caller shall receive a busy announcement as per UCR 2008, Section 5.2.2.1.3, Announcements.

[Required: MFSS] If the MFSS's count of an IPC is greater than or equal to the corresponding IPB, and it receives an INVITE request for a precedence session, the MFSS shall preempt a lower priority session (if such a session exists), and then proceed with processing the higher precedence session connect request.

5. MFSS Session Processing with Directionalization. When directionalization is applied, the MFSS shall police IPCi and IPCo to assure that they do not exceed their respective budgets. The IPCi processing is independent of that for IPCo and both are identical to that carried out for IPC in the no-directionalization case.

5.3.2.2.2.3.2 ASAC Requirements for the LSC and the MFSS Related to Video Services

The LSC and the MFSS will process only AS-SIP video. H.323 video will be processed by a gatekeeper appliance and H.320 video will be processed by TDM appliances. Consequently, this section considers ASAC requirements for LSC and MFSS in processing AS-SIP video.

Since the bandwidth of a video session can vary, video sessions will be budgeted in terms of video session units (VSUs). One VSU equals 500 kbps and bandwidth for video sessions will be allocated in multiples of VSUs. For example, the bandwidth allocated to video sessions may be 500 kbps, 1000 kbps, and 2500 kbps. Thus, a video session that requires 2500 kbps will be allocated five VSUs.

1. VSU Budgets. The LSC and its corresponding MFSS shall be configurable with the following budgets:

    - VDB. The total number of inbound and outbound VSUs plus the in-progress VSUs connection attempts that an LSC is allowed to have over the IP access link.

Video and voice will each be allocated adequate bandwidth to support its traffic-engineered budgets. Since each of these two services is allocated its own bandwidth, preemption of low precedence video sessions by high precedence voice sessions (and vice versa) will not be necessary and will not be implemented. Voice sessions will strictly preempt within their allocated bandwidth and video sessions likewise.

The LSC processing requirements of video sessions will be similar to its processing of VoIP sessions. For the no-directionalization case (i.e., VDBi = VDBo = null), the LSC shall manage VDC to assure that it does not exceed VDB. For the directionalization case where VDBi and VDBo are null, the LSC will manage VDCo and VDBi independently to assure that neither one exceeds its corresponding budget. The preemption rules for video sessions are the same as for voice sessions as specified in UCR 2008, Section 5.2.2, Multilevel Precedence and Preemption. However, some extensions to the rules are required to take into account that video sessions can be of different budgets (i.e., 1, 2, or 5 budgets corresponding to 500 kbps, 1000 kbps, and 2500 kbps, respectively). The following rule extensions apply to a video session request of 1, 2, or 5 budgets:

1. Preempt sessions in the process of signaling setup (progress) before preempting active sessions.

2. Preempt the minimum number of sessions in order to accumulate the number of budgets needed to satisfy the video session request.

3. Accumulate the needed number of budgets by preempting all sessions of a lower precedence level (starting at the ROUTINE level) before proceeding to preempt from sessions of the next higher precedence level for the remaining required budgets.

4. When the number of sessions selected for preemption result is more budgets (excess) then are required to satisfy the video session request, return the excess budgets to the ASAC pool.

The MFSS processing requirements of video sessions will be similar to its processing of VoIP sessions. For the no-directionalization case (i.e., VDBi equals VDBo equals null), the MFSS shall police by blocking to assure that the respective budgets are not exceeded: VDC to assure that it does not exceed VDB.

[Required: MFSS] If necessary, the MFSS will preempt for a session request that is at precedence level FLASH OVERRIDE or FLASH and the counts equal the budgets.

5.3.2.2.3 Signaling Protocols

[Required: EI, LSC, MFSS] The control/management protocol between the EI and the LSC is in general proprietary.

[Required: LSC, MFSS] The signaling protocol used on DSN IP trunks is AS-SIP as specified in UCR 2008, Section 5.3.4, AS-SIP Generic System Specification.

[Required: MFSS] The TDM-side of an MFSS uses DSN CCS7 signaling (see UCR 2008, Section 5.2.2.9.1, General Description) on CCS7-like trunks.

[Required: LSC, MFSS] The MFSS uses DSN T1-619a PRI signaling on DSN PRI trunks.

[Conditional: LSC, MFSS] The LSC and MFSS use CAS signaling on CAS trunks.

5.3.2.2.4 Signaling Performance

Call set-up times should adhere to the following guidelines:

1. **[Conditional: Intra-Enclave Calls]** For intra-enclave calls, the average delay should be no more than one second. For 95 percent of calls, the delay should not exceed 1.5 seconds during normal traffic conditions.

2. **[Conditional: Inter-Enclave calls]** For inter-enclave and worldwide calls within the IP environment, average delay should not exceed 6 seconds, with 95 percent of calls not to exceed 8 seconds during normal traffic conditions.

5.3.2.3 Registration, Authentication, and Failover

5.3.2.3.1 Registration and Authentication

[Required: LSC, MFSS] Registration and authentication between network elements shall follow the requirements set forth in UCR 2008, Section 5.4, Information Assurance Requirements.

5.3.2.3.2 LSC and MFSS Failover Requirements

[Conditional FY 08: LSC, MFSS, EBC; Required FY 10: LSC, MFSS, EBC]. LSCs shall be registered to a primary and backup MFSS. In case of failure of the primary MFSS, the LSC will default to the backup MFSS.

5.3.2.3.2.1 General Description

The MFSS (Softswitches) will be deployed as active-active pairs whereby one MFSS will act as the primary for one set of LSCs (set A) and as the secondary for another set of LSCs (set B). Similarly, the other MFSS will act as primary for the set B LSCs and secondary for the set A LSCs. LSCs shall be registered to a primary and a secondary (backup) MFSS during network configuration. In case of the loss of connectivity (either a transport or MFSS failure) to the primary MFSS, the LSC in conjunction with its EBC will default to sending the AS-SIP signaling messages to the secondary MFSS. Sessions (calls) that were established with the primary MFSS will remain in progress until SIP keep-alive timers expire and the sessions are closed by the LSC. If desired, the caller can redial the DN and re-establish the session through the secondary MFSS. Each MFSS (softswitch part) in the network will know the primary and the secondary MFSS of every LSC; this will be done by operations personnel during MFSS configuration. The failover detection mechanism will be accomplished through employing a periodic AS-SIP OPTIONS request between each LSC and it primary and secondary MFSSs, and between each MFSS network pair. Through this an LSC can learn when its primary MFSS has failed and subsequently relay AS-SIP messages to the secondary MFSS, and an MFSS can learn when any other MFSS has failed and subsequently relay AS-SIP messages to the secondary MFSS for delivery to the LSC. When a softswitch receives an OPTIONS request from an LSC or another MFSS it responds with a 200 OK message. Consequently, through the periodic "pinging" of all network signaling appliances using the AS-SIP OPTIONS request and 200 OK response messages, each signaling appliance learns of the operational status of its neighbors and can route around the failure of any individual signaling appliance. The specific LSC, MFSS, and EBC failover requirements are discussed in the following subsections.

5.3.2.3.2.2 LSC Monitors Primary MFSS (Softswitch) for Status

[Conditional] The LSC shall send an OPTIONS request with a Request-URI identifying the primary softswitch (the Request-URI does not have a userinfo part) on a configurable periodic time interval (default = 15 seconds).

[Conditional] When a properly functioning primary softswitch receives the OPTIONS request from a served LSC, the primary softswitch shall respond with a 200 OK message that includes the Accept header and the Supported header.

[Conditional] The OPTIONS requests sent by the LSC include a route set comprised of two Route Headers where the first Route Header is the SIP Universal Resource Identifier (URI) for the EBC at the enclave and the second Route Header is the SIP URI for the EBC serving the primary softswitch.

[Conditional] Whenever the LSC sends an INVITE request to its EBC and receives either a 408 (Request Time-Out), 503 (Service Unavailable), or 504 (Server Time-Out) response, then the LSC shall send an OPTIONS request with a Request-URI identifying the primary softswitch (the Request-URI does not have a userinfo part).

[Conditional] The LSC shall be capable of sending OPTIONS requests to the primary softswitch, or to both the primary and the secondary softswitch via a configuration setting.

5.3.2.3.2.3 LSC Failover to Secondary MFSS (Softswitch)

1. **[Conditional]** When the LSC sends a defined configurable number of successive OPTIONS requests (default = 2) for which there is either no response or the response is either a 408 (Request Time-Out), 503 (Service Unavailable), or 504 (Server Time-Out) response, then:

    a. **[Conditional]** All new outbound SIP messages (with the exception of OPTIONS requests destined for the primary softswitch) are sent to the secondary softswitch. The OPTIONS requests generated by the LSC continue to be sent to the primary softswitch.

    b. **[Conditional]** All outbound SIP requests sent by the LSC to its EBC (with the exception of OPTIONS requests) include a route set comprised of two Route Headers where the first Route Header is the SIP URI for the EBC at the enclave and the second Route Header is the SIP URI for the EBC serving the secondary softswitch.

c. **[Conditional]** Upon failover from the primary softswitch to the secondary softswitch, the EBC serving the secondary softswitch shall respond with a 481 (Call/Transaction Does Not Exist) response upon receipt of any Re-INVITE, UPDATE, or BYE request on behalf of an existing call that had been established through the primary softswitch.

d. **[Conditional]** If the LSC receives a 200 OK response to an OPTIONS request from the primary softwitch before the configurable number of successive failures to the OPTIONS requests (default = 2) has been reached, then no action is taken to failover to the secondary softswitch. For example, using the default of two successive failures, if one OPTIONS request to the primary softswitch fails, then if the next OPTIONS request receives a 200 OK response, no action is taken to fail over to the secondary softswitch.

5.3.2.3.2.4 LSC Failback to Primary MFSS (Softswitch)

[Conditional] Upon failover, the LSC will send OPTIONS requests to the primary softswitch at a failback configurable periodic time interval (default = 5 seconds).

[Conditional] The OPTIONS requests sent by the LSC shall include a route set comprised of two Route Headers where the first Route Header is the SIP URI for the EBC at the enclave and the second Route Header is the SIP URI for the EBC serving the primary softswitch.

[Conditional] When the LSC receives a 200 OK response to an OPTIONS request from the primary softswitch, then the LSC shall send the INVITE requests corresponding to new call requests to the primary softswitch and shall continue to send SIP messages pertaining to existing calls that were established through the secondary softswitch to the secondary softswitch until those calls terminate normally.

[Conditional] When the LSC sends INVITE requests (as well as the subsequent SIP requests) for new call requests, then the INVITE requests (and the subsequent SIP requests) shall include a route set comprised of two Route Headers where the first Route Header is the SIP URI for the EBC at the enclave and the second Route Header is the SIP URI for the EBC serving the primary softswitch.

[Conditional] Upon failback, the LSC returns to the original configurable periodic time interval (default = 15 seconds) for sending OPTIONS requests to the primary softswitch.

5.3.2.3.2.5 MFSS (Softswitch) Monitors the Other MFSSs (Softswitches) in the Network

[Conditional] Each softswitch shall send an OPTIONS request to every other softswitch on a "standard" configurable periodic time interval (default = 15 seconds). In each OPTIONS request, the Request-URI identifies the destination softswitch (the Request-URI does not have a userinfo part). The OPTIONS requests shall include a route set comprised of two Route Headers where the first Route Header is the SIP URI for the EBC of the softswitch originating the OPTIONS request and the second Route Header is the SIP URI for the EBC serving the destination softswitch.

[Conditional] Whenever an originating softswitch sends an INVITE request to another softswitch and receives either a 408 (Request Time-Out), 503 (Service Unavailable), or 504 (Server Time-Out) response, then the originating softswitch shall send an OPTIONS request with a Request-URI identifying the softswitch. The OPTIONS request shall include a route set comprised of two Route Headers where the first Route Header is the SIP URI for the EBC of the softswitch originating the OPTIONS request and the second Route Header is the SIP URI for the EBC serving the destination softswitch.

[Conditional] When a properly functioning softswitch receives the OPTIONS request, the softswitch shall respond with a 200 OK response that includes the Accept header and the Supported header.

5.3.2.3.2.6 MFSS Failover to Secondary MFSS (Softswitch)

1. **[Conditional]** Each MFSS (softswitch) shall be configured with knowledge of each pair of softswitches that operate as primary or secondary softswitches for a set of LSCs.

2. **[Conditional]** When the originating softswitch sends a defined configurable number of successive OPTIONS requests (default = 2) to another softswitch (that is NOT its own paired secondary softswitch) for which there is either no response or the response is either a 408 (Request Time-Out), 503 (Service Unavailable), or 504 (Server Time-Out) response, then:

    a. **[Conditional]** The originating softswitch sends all new SIP messages intended for the failed softswitch (with the exception of OPTIONS requests that it generates for the failed softswitch) to the paired secondary softswitch for the failed softswitch. The SIP requests shall include a route set comprised of two Route Headers where the first Route Header is the SIP URI for the EBC at the originating softswitch, and the second Route Header is the SIP URI for the EBC serving the paired secondary softswitch for the failed softswitch. The originating softswitch will continue to send

OPTIONS requests to the failed softswitch whereby the OPTIONS requests include a route set comprised of two Route Headers where the first Route Header is the SIP URI for the originating softswitch and the second Route Header is the SIP URI for the EBC serving the failed softswitch.

b. **[Conditional]** Upon failover from the primary softswitch to the secondary softswitch, the EBC serving the secondary softswitch shall respond with a 481 (Call/Transaction does not exist) upon receipt of any Re-INVITE, UPDATE, or BYE request received on behalf of an existing call that had been established through the primary softswitch.

c. **[Conditional]** If the originating Softwitch receives a 200 OK response to an OPTIONS request from its paired softswitch or another softswitch before the configurable number of successive failures to the OPTIONS requests (default = 2) has been reached, then no action is taken to fail over to the paired softswitch. For example, using the default of two successive failures, if one OPTIONS request to the other softswitch fails, then the next OPTIONS request receives a 200 OK response, no action is taken to fail over to the paired softswitch.

3. **[Conditional]** When the originating softswitch sends a defined configurable number of successive OPTIONS requests (default = 2) to its own paired softswitch for which there is either no response or the response is either a 408 (Request Time-Out), 503 (Service Unavailable), or 504 (Server Time-Out) response, then:

a. **[Conditional]** The softswitch sends all new SIP messages intended for its paired softswitch (with the exception of OPTIONS requests it generates for its failed paired softswitch) directly to the LSCs served by its paired softswitch. The SIP requests shall include a route set comprised of two Route Headers where the first Route Header is the SIP URI for its own EBC, and the second Route Header is the SIP URI for the EBC for the intended LSC. The softswitch will continue to send OPTIONS messages to its failed paired softswitch whereby the OPTIONS messages include a route set comprised of two Route Headers where the first Route header is the SIP URI for its own EBC, and the second Route Header is the SIP URI for its failed paired softswitch.

b. **[Conditional]** Upon failover of its paired softswitch, the EBC serving the operational softswitch shall respond with a 481 (Call/Transaction does not exist) upon receipt of any Re-INVITE, UPDATE, or BYE request received on behalf of an existing call that had been established through its paired softswitch.

5.3.2.3.2.7 MFSS Failback to Original MFSS (Softswitch)

[Conditional] Upon failover, the softswitch will send OPTIONS requests to the failed softswitch at a "failback" configurable periodic time interval (default = 5 seconds). The OPTIONS requests shall include a route set comprised of two Route Headers where the first Route Header is the SIP URI for the EBC of the originating softswitch, and the second Route Header is the SIP URI for the EBC serving the failed softswitch.

[Conditional] When the softswitch receives a 200 OK response to an OPTIONS request from a failed softswitch (that is NOT its paired softswitch), then the softswitch shall send to the newly recovered softswitch the INVITE requests corresponding to new call requests intended for LSCs whose primary softswitch is supposed to be the newly recovered softswitch. The new INVITE requests shall include a route set comprised of two Route Headers where the first Route Header is the SIP URI for the originating softswitch and the second Route Header is the SIP URI for the EBC serving the newly recovered softswitch.

[Conditional] The softswitch will continue to send SIP messages pertaining to existing calls that were established through the secondary softswitch to the secondary softswitch until those calls terminate normally.

[Conditional] When the softswitch receives a 200 OK response to an OPTIONS request from its paired softswitch, then the softswitch shall send its newly recovered paired softswitch the INVITE requests corresponding to new call requests intended for LSCs whose primary softswitch is supposed to be the newly recovered paired softswitch. The new INVITE requests shall include a route set comprised of two Route Headers where the first Route Header is the SIP URI for the originating softswitch and the second Route Header is the SIP URI for the EBC serving its newly recovered paired softswitch.

[Conditional] The softswitch will continue to send SIP messages pertaining to existing calls that were established through itself to its served secondary LSCs until the calls terminate normally.

[Conditional] Upon failback, the softswitch returns to the original configurable periodic time interval (default = 15 seconds) for sending OPTIONS requests to the newly recovered softswitch.

5.3.2.4 System Interface Requirements

5.3.2.4.1 Internal Interface Requirements

[Required: EI, LSC (including the MG, SG, and media server), MFSS, EBC, and CE Router] Internal interfaces are functions that operate internal to a System Under Test (SUT) or

UC Approved Product (e.g., LSC, MFSS). The interfaces between the Session Control and Signaling (SCS) functions within an LSC, e.g., between the Call Admission Control (CAC), IWF, MGC, MG, and SG are considered internal to the LSC regardless of the physical packaging. These interfaces are vendor proprietary and unique, especially the protocol used over the interface. Whenever the physical interfaces use Institute of Electrical and Electronics Engineers, Inc. (IEEE) 802.3 Ethernet standards, then they shall support auto-negotiation even when the IEEE 802.3 standard has it as optional. This applies to 10/100/1000-T Ethernet standards; i.e., IEEE, Ethernet Standard 802.3, 1993; or IEEE, Fast Ethernet Standard 802.3u, 1995; and IEEE, Gigabit Ethernet Standard 802.3ab, 1999.

5.3.2.4.2 External Physical Interfaces between Network Components

External physical interfaces between components are functions that cross the demarcation point between SUTs and other external network components. The following subparagraphs provide requirements and specifications for external component physical interfaces.

[Required: LSC, MFSS, EBC, CE Router, ASLAN, EI] The physical interfaces between an LSC (and its appliances), the EBC, the ASLAN switches/routers and the CE Router shall be a 10/100/1000-T megabits per second (Mbps) Ethernet interface. Whenever the physical interfaces use IEEE 802.3 Ethernet standards, then they shall support auto-negotiation even when the IEEE 802.3 standard has it as optional. This applies to 10/100/1000-T Ethernet standards; i.e., IEEE, Ethernet Standard 802.3, 1993; or IEEE, Fast Ethernet Standard 802.3u, 1995; and IEEE, Gigabit Ethernet Standard 802.3ab, 1999.

5.3.2.4.3 Interfaces to Other Networks

Interfaces to other networks are interfaces where traffic flows from one network (e.g., DSN) to another network (e.g., PSTN).

5.3.2.4.3.1 Tactical Networks Interface Requirements

[Conditional] The tactical interface requirements are specified is UCR 2008, Section 6.1, Tactical Requirements, Section 5.3.3, Wide Area Network Requirements, and Section 7, Requirements Matrix.

5.3.2.4.3.2 DISN Teleport Site Interface Requirements

[Required] The Assured Services subsystem shall interface the Teleport sites on both a TDM basis and an IP basis. A T1.619a MG with PRI signaling will be used for T1 trunks to the Teleport sites. If the Teleport site contains an LSC, then the interface will be via the DISN

WAN for both the media and signaling, with the signaling being AS-SIP (UCR 2008, Section 5.3.4, AS-SIP Generic System Specification) between the Teleport LSC and the DSN MFSS.

5.3.2.4.3.3 PSTN Interface Requirements

[Required] The Assured Services subsystem shall interface with the PSTN and host-nation Public Telephones and Telegraphs (PTTs) via the signaling gateway or media gateway interfaces as specified elsewhere in this section.

5.3.2.4.3.4 Allied and Coalition Network Interface Requirements

[Conditional] Voice and video interfaces with allied and coalition networks have not yet been defined. Therefore, for IOC the interface will remain TDM as specified in the UCR 2008, Figure 4-45, DSN Design and Components.

5.3.2.4.4 VVoIP Network Management System Interface Requirements

[Required] The physical interface between the DISA VVoIP NMS (Advanced DSN Integrated Management Support System (ADIMSS)) and the network components (i.e., LSC, MFSS, EBC, CE Router) is a 10/100 Mbps Ethernet interface. The interface will work in either of the two following modes using auto-negotiation: Institute of Electrical and Electronic Engineers (IEEE), Ethernet Standard 802.3, 1993, or IEEE, Fast Ethernet Standard 802.3u, 1995.

5.3.2.5 System Physical, Quality, and Environmental Factors

5.3.2.5.1 Physical Characteristics

[Required] The physical characteristics of network equipment with respect to weight, dimensions, transportation, storage, durability, safety, and color are required to be those of best commercial practices, and will be specified by the acquiring DoD organization.

5.3.2.5.2 System Quality Factors

The system quality factors associated with reliability, maintainability, and availability, are based on the requirements in Telcordia Technologies GR-512-CORE. The explanation and format for these requirements are in GR-512-CORE, Sections 1 through 5. However, the types and values of the following requirements have been modified from the Generic Requirement to reflect a judged application to voice and video over IP systems. Equipment capabilities are still expected to meet best commercial practices as reflected in the Generic Requirement including those of “carrier grade” or central office equipments. The following paragraphs outline the availability requirements for the Assured Services subsystem.

5.3.2.5.2.1 System Availability

[Required: LSC, MFSS] The subsystem shall have a hardware/software availability of 0.99999 (nonavailability of no more than 5 minutes per year). The vendor shall provide an availability model for the system showing all calculations and showing how the overall availability will be met. The subsystem shall have no single point of failure that can cause an outage of more than 96 voice and/or video subscribers. In order to meet the availability requirements, all subsystem platforms that offer service to more than 96 voice and/or video subscribers shall have a modular chassis that provides, at a minimum, the following:

1. Dual Power Supplies. The platform shall provide a minimum of two power supplies, each with a power capacity to support the entire chassis electrical load.

2. Dual Processors/Swappable Sparing (Control Supervisors). The chassis shall support dual active processors, or processor card automatic swappable sparing. Failure of any one processor or swappable processor cards shall not cause loss of any ongoing functions within the chassis (e.g., no loss of active calls).

3. Termination Sparing. The chassis shall support a (N+1) sparing capability for available 10/100 Mbps Ethernet modules used to terminate an IP voice or video subscriber.

4. Redundancy Protocol. The routing equipment shall support a protocol that allows for dynamic rerouting of IP packets or Ethernet frames so that no single point of failure exists in the Assured Services subsystem.

5. No Single Failure Point. No single point shall exist in the subsystem that could cause the loss of voice and/or video service to more than 96 voice or video EIs.

6. Switch Fabric or Backplane Redundancy for Active Backplanes. Active switching platforms within the subsystem components shall support a redundant (1+1) switching fabric or backplane. The second fabric's backplane shall be in active standby so failure of the first backplane shall not cause the loss of any ongoing events within the platform.

7. Software Upgrades and Patches. Software upgrades and patches shall be able to be implemented without incurring any subsystem downtime.

8. Backup Power Uninterruptible Power Supply (UPS) Requirements. The components that comprise the subsystem for Special Command and Control (C2) users shall meet the appropriate UCR 2008, Section 5.2.11.3, Backup Power, switch type backup power UPS requirements (e.g., 8 hours for an MFSS and LSC) for all devices including the EIs. If a base has automatic UPS switchover 72-hour power capability that feeds all the Voice and

Video equipments including the EIs, then it naturally meets the 8-hour backup power requirement with no need to do anything special or extra at the LSC or MFSS. Backup power is only required for as many hours as it will take the base to switch over to backup generator power, but the total combination of backup times shall not be less than 8 hours.

9. No Loss of Active Sessions. In the event of component failure in the subsystem, all active sessions shall not be disrupted (namely, the loss of existing connection requiring redialing), and the path through the network shall be restored within 5 seconds. All devices used to implement redundancy shall be capable of handling the entire session processing load in the event that its counterpart device fails.

5.3.2.5.2.2 Maximum Downtimes

[Required: LSC, MFSS, ASLAN] The performance parameters associated with the ASLAN, MFSS, and LSC, when combined, shall meet the following maximum downtime requirements:

- IP (10/100 Ethernet) network links – 35 minutes/year
- IP subscriber – 12 minutes/year

5.3.2.5.3 Environmental Conditions

[Required] Environmental conditions requirements are contained in Telcordia Technologies GR-63-CORE. This document identifies the minimum generic spatial and environmental criteria for all new telecommunications equipment systems used in a telecommunications network. Included with these equipment systems are associated cable distribution systems, distributing and interconnecting frames, power equipment, operations support systems, and cable entrance facilities. The detailed specifications of this section are those of best commercial practice and will be specified by the acquiring DoD organization.

5.3.2.6 End Instruments

The IP voice and IP video EIs are addressed in this section. Legacy voice and video EIs, secure and nonsecure, are addressed in UCR 2008, Section 5.2, Circuit-Switched Capabilities and Features. Data/PC EIs will not be addressed in this section. Secure IP EIs are addressed in UCR 2008, Section 5.2.12.6, DoD Secure Communications Devices, and in UCR 2008, Section 6.2, Unique Classified Requirements. Softphones are addressed in UCR 2008, Section 5.2.12.8.3, Softphones, when used with circuit switches. Softphones and collaboration will be addressed in future versions of this document when softphones and softvideophones are added to the Security Technical Implementation Guides (STIGs).

5.3.2.6.1 Voice Instrument

Voice instruments are considered associated with the LSC and must have been designed in conjunction with the LSC design. An IP voice instrument shall be designed in accordance with the acquiring activity requirements, but the following capabilities are specifically required as indicated:

- **[Objective]** DoD Common Access Card (CAC) reader
- **[Required]** Display calling number
- **[Required]** Display precedence level of the session

[Required] For multiple line appearance, only two-appearance IP voice instruments are specified, and shall function as specified in UCR 2008, Section 5.2.2.6, ISDN MLPP BRI.

5.3.2.6.1.1 Tones and Announcements

[Required: EI, LSC, MFSS] Tones and announcements, as required in UCR 2008, Section 5.2.4.5.2, DSN Information Signals, and Section 5.2.2.1.3, Announcements, shall be supported by the EI. Only announcements pertinent to VoIP need to be supported. These tones and announcements may be generated locally by the EI upon command of the LSC, or generated upon command of the LSC by an internal LSC media server or an external media server (not part of the LSC), connected to the ASLAN and passed as a media stream to the EI.

5.3.2.6.1.2 Codecs

[Required: EI, LSC-MG, MFSS] The system shall support the origination and termination of a voice session using the following codecs:

1. ITU-T Recommendation G.711, to include both the μ-law and A-law algorithms

2. ITU-T Recommendation G.723.1

3. ITU-T Recommendation G.729, G.729A

The system is not required to do transcoding between codec types, but must support, via signaling during session setup, the offer/negotiation between origination and destination EIs of the codec type to be employed for the session. However, support for A-law/μ-law conversion is required as needed by media gateways within the system.

5.3.2.6.1.3 Handset Loudness and Frequency Response Requirement

End instruments must comply with the TIA-810-B requirements for Send Loudness Rating (SLR) and Receive Loudness Rating (RLR) requirements in accordance with the UCR 2008. The requirement is as follows:

1. **[Required: EI]** The system IP EI shall comply with American National Standards Institute (ANSI)/Telecommunication Industries/Industry Association (TIA)-810-B, which will result in the following:

    a. A VoIP EI having a nominal SLR of 8 decibels (dB) and a nominal RLR of 2 dB.

    b. The VoIP EI having a nominal Weighted Terminal Coupling Loss (TCLw) of >= 52 dB, with a desirable TCLw of >= 55 dB.

5.3.2.6.1.4 Voice Over IP Sampling Standard

[Required] The system shall use a 20 milliseconds (ms) voice sampling interval

5.3.2.6.1.5 Authentication to Local Session Controller

[Required: EI, LSC, MFSS] The EI shall be capable of authenticating itself to its associated LSC and vice versa in accordance with UCR 2008, Section 5.4, Information Assurance Requirements.

5.3.2.6.1.6 Analog Telephone Support

[Required: EI, LSC, MFSS] Analog instruments, including secure analog EIs, shall be supported by the LSC either by a Terminal Adapter (TA) or an Integrated Access Device (IAD) connected to an Ethernet port, or by the existing twisted-pair cable plant connected to a line card that is part of the LSC MG.

[Required] Terminal Adapter (RJ-11 Plain Old Telephone System (POTS) telephone to RJ-45 Ethernet interface)

[Required] IAD (4-16 ports of RJ-11 POTS telephone to one port of RJ-45 Ethernet interface)

5.3.2.6.2 Video End Instrument

Video EIs are considered associated with the LSC and must have been designed in conjunction with the LSC design. An IP video instrument shall be designed in accordance with the acquiring activity requirements, but the following capabilities are specifically required as indicated:

1. **[Conditional]** DoD CAC card reader.

2. **[Required]** Automatic enabling of the video camera is not permitted after video session negotiation or acceptance. The called party must take a positive action to enable the camera.

3. **[Required]** Display calling number.

4. **[Required]** Display precedence level of the session.

5.3.2.6.2.1 Display Messages, Tones, and Announcements

[Required: EI, LSC, MFSS] Tones and announcements, as appropriate for video IP and as required in UCR 2008, Section 5.2.4.5.2, DSN Information Signals, and Section 5.2.2.1.3, Announcements, shall be supported by the EI. These tones and announcements may be generated locally by the EI, generated by the LSC or a server connected to the ASLAN, and passed as a media stream to the EI.

5.3.2.6.2.2 Video Codecs

[Required: EI, MCU] The system shall support the origination, maintenance, and termination of a video session using the following codecs: one G.xxx and one H.xxx must be used to create and sustain a video session (All video and audio capabilities in the EI shall be sent to the terminating EI for negotiation as to which video and audio codec to use for the session.):

1. ITU-T Recommendation G.711to include both the μ-law and A-law algorithms.

2. ITU-T Recommendation G.722.

3. ITU-T Recommendation G.723.1.

4. ITU-T Recommendation G.728.

5. ITU-T Recommendation G.729, G.729A.

6. ITU Recommendation H.261.

7. ITU Recommendation H.263. H.263v2 (also known as H.263+ or as the 1998 version of H.263) enhances H.263 capabilities by adding several annexes, which substantially improve encoding efficiency and provide other capabilities, such as enhanced robustness against data loss in the transmission channel (i.e., Advanced Intra Coding, using spatial prediction; Deblocking Filter; Reference Picture Selection; Scalability and B pictures; Reference Picture Resampling).

8. ITU Recommendation H.263++ (also known as H.263 2000). Supports some or all the optional modes (i.e., Data Partitioning, for resilience to bit errors; Enhanced Reference Picture Selection; Annex X defines profiles and levels; two group optional modes and parameters to improve interoperability above the baseline capability).

9. ITU Recommendation H.264/MPEG-4 (Part 10), Advanced video coding for generic audiovisual services, (commonly referred to as H.264/AVC) is the newest entry in the series of international video coding standards.

5.3.2.6.2.3 Authentication to LSC

[Required: EI, LSC, MFSS] The EI shall be capable of authenticating itself to its associated LSC and vice versa in accordance with UCR 2008, Section 5.4, Information Assurance Requirements.

5.3.2.6.3 End Instrument to ASLAN Interface

[Required: EI] The interface to the ASLAN shall be in accordance with Ethernet (Institute of Electrical and Electronics Engineers (IEEE) 802.3) LAN technology. The 10 Mbps and 100 Mbps Fast Ethernet (IEEE 802.3u) shall be supported.

Tones and announcements may be generated locally by the EI upon command of the LSC, or generated upon command of the LSC by an internal LSC media server or an external media server (not part of the LSC), connected to the ASLAN and passed as a media stream to the EI.

5.3.2.7 Local Session Controller

The LSC is a software-based call processing system that provides voice and video services to IP telephones and media processing devices within a local service domain. Additionally, an LSC extends signaling and call control services to allow calls to reach connections outside the local service domain. Connectivity to external networks outside a local service domain is provided via gateways to non-IP networks, or to an IP-based long-haul network.

The LSC software and functions may be distributed physically among several high-availability server platforms with redundant call management modules and subscriber tables to provide robustness.

Figure 5.3.2-7 provides a simple overview of an LSC and its functions.

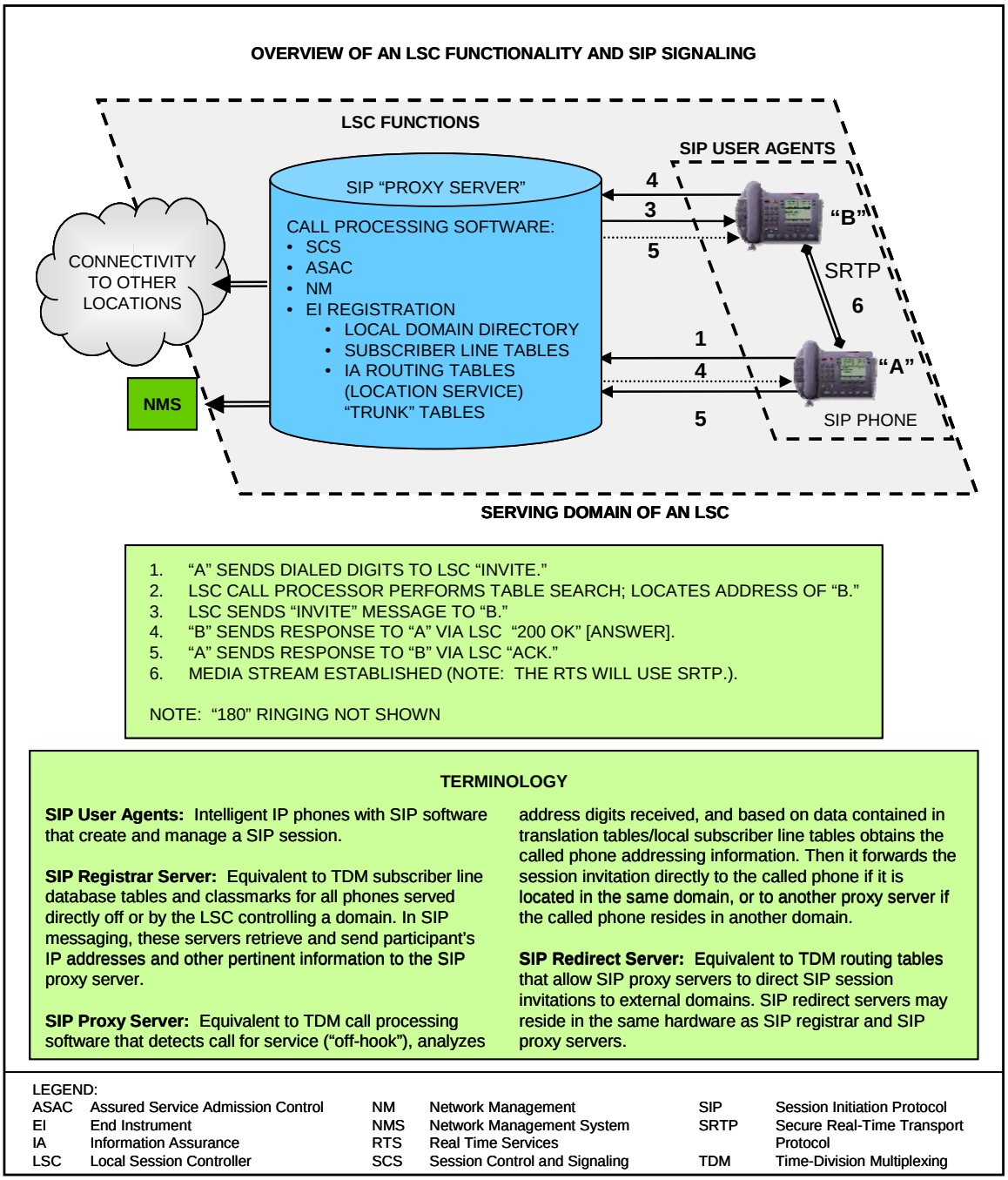


Figure 5.3.2-7. Simple Overview of LSC Functionality

5.3.2.7.1 LSC Functional Reference Model and Assumptions

Figure 5.3.2-8, Functional Reference Model – LSC, shows the reference model for the LSC. The LSC consists of several SCS functions performed by the CCA, IWF, MG, MGC, and SG. These are connected via proprietary internal interface functions. Connectivity to other networks, long-haul transport system (via an ASLAN) and DISA's VVoIP NMS (ADIMSS) are provided by external interfaces.

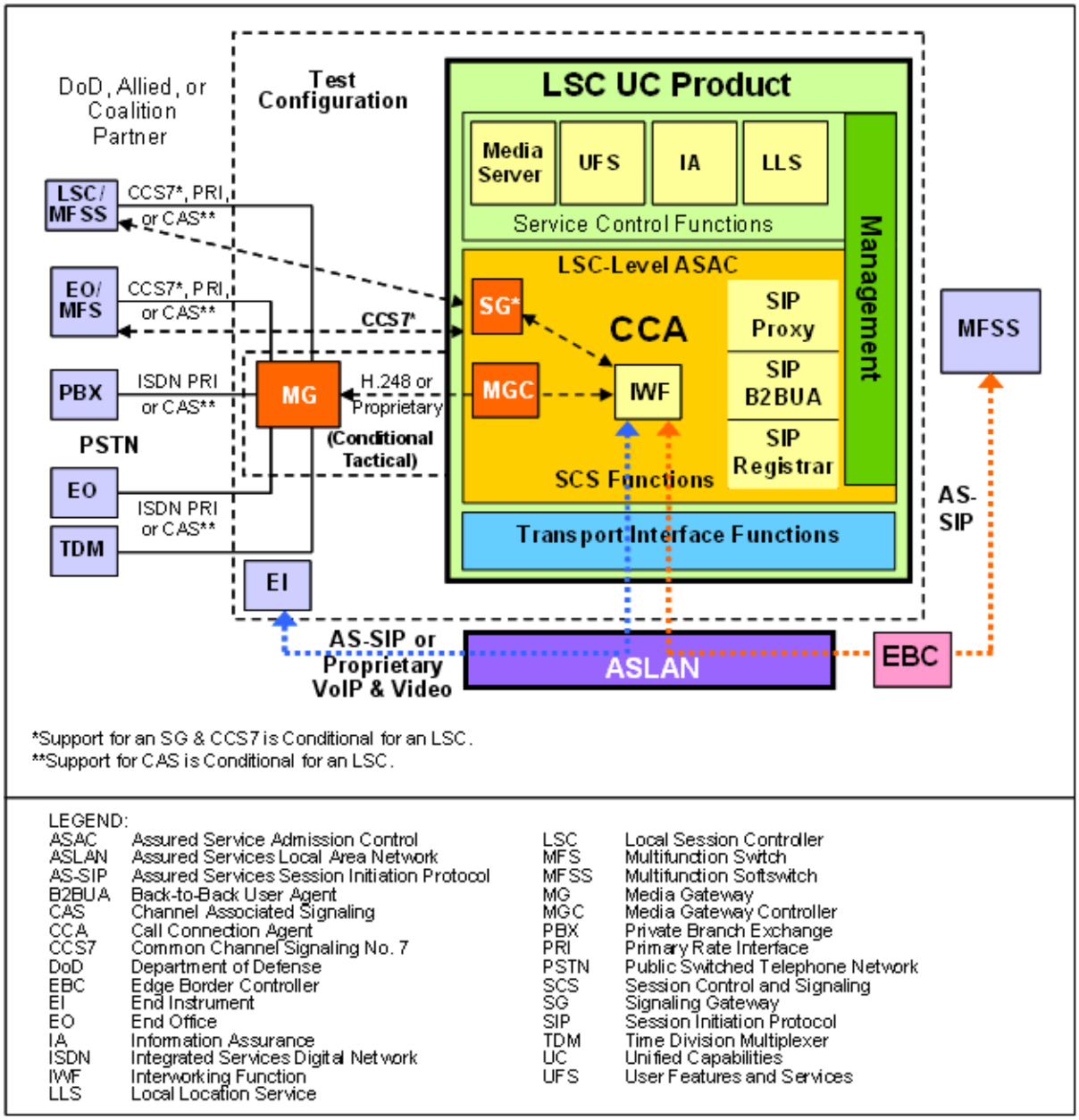


Figure 5.3.2-8. Functional Reference Model – LSC

Generic System Requirements for the CCA, MG, and SG functions and NM are provided in separate sections of the UCR 2008 as follows:

1. Section 5.3.2.9, Call Connection Agent – General Description, contains CCA requirements including the CCA-associated Inter-Working Function (IWF) that apply to both the LSC and the MFSS.

2. Section 5.3.2.12, Media Gateway Requirements, contains MG and MGC requirements.

3. Section 5.3.2.13, Signaling Gateway Requirements, contains SG requirements.

4. Section 5.3.2.17, Management of Network Appliances, contains NM requirements.

5.3.2.7.1.1 Assumptions – LSC

The following assumptions are made based on the LSC reference model:

1. The MGC and IWF are both components of the CCA. The MGC is responsible for controlling the MG in the LSC and the CAS and ISDN TDM trunk groups that are connected to it. The IWF is responsible for supporting all the VoIP and TDM signaling protocols in the LSC, and for interworking the different protocols together (see Table 5.3.2-7, Full IWF Interworking Capabilities for VoIP and TDM Protocols) for the full set of IWF capabilities. For example, the IWF is responsible for interworking AS-SIP on the IP network side with ISDN PRI on the TDM side, and interworking Proprietary VoIP on the EI side with AS-SIP on the MFSS side.

2. The MG provides circuit-switched trunk termination (for DoD PRI and CAS trunks) and TDM/VoIP interworking. The MG is controlled by the MGC. The protocol that the MGC uses to control the MG can be ITU-T Recommendation H.248 (specifically, H.248.1, Gateway Control Protocol, Version 3, September 2005) or a proprietary protocol chosen by the LSC supplier.

3. Figure 5.3.2-8, Functional Reference Model – LSC, shows the LSC supporting a single MG on a single ASLAN. A single LSC can also support multiple MGs on multiple ASLANs, where those ASLANs are interconnected to form a Metropolitan Area Network (MAN) or Community of Interest Network (COIN). In this arrangement, it is expected that the set of ASLANs forming the MAN or COIN can meet the single-ASLAN performance requirements in UCR 2008, Section 5.3.1, Assured Services Local Area Network Infrastructure. In this case, the LSC supports sessions between an MG on one ASLAN and an EI, MG, or EBC on another ASLAN, as long as both ASLANs are part of the same MAN or COIN.

Another way of stating this is that a single LSC is able to support Media Gateways at multiple physical locations. In some deployments, an LSC in one location will serve ASLANs and EIs at distant locations, where both locations are part of the same regional MAN or COIN. In these cases, each distant ASLAN may want to have its own gateway to the local PSTN. In these cases, the LSC supports Media Gateways at multiple locations over MAN or COIN infrastructures that meet the ASLAN performance requirements in UCR 2008."

4. LSC support for (and inclusion of) an MGC and an MG is Conditional-Tactical. That is, LSC support for (and inclusion of) an MGC and an MG is required for strategic deployments, but conditional for tactical deployments.

5. LSC support for (and inclusion of) an SG is Conditional.

6. Each functional component in the LSC has associated management-related functions for FCAPS management and audit logs.

7. The signaling requirements and the Proprietary VoIP requirements for the EI-LSC interface are outside the scope of this section, and are left to the supplier's discretion in the IOC time frame. The CCA IWF is responsible for interworking the supplier's Proprietary VoIP EI implementations with DISN-standard AS-SIP on the LSC/MFSS interface.

8. The CCA interacts with the Service Control functions using internal interfaces and proprietary protocols that vary from one supplier's solution to another.

9. The LSC interactions with its EBC are as follows:

    a. The EBC controls signaling streams between an LSC (connected to an ASLAN) and an MFSS (whose separate ASLAN is connected to the DISN WAN). In doing so, the EBC also controls media streams between LSC EIs and MGs (connected to the ASLAN) and EIs and MGs on other LSCs (whose separate ASLANs are connected to the DISN WAN). The LSC accesses the DISN WAN via the LSC EBC and an associated PE Router on the DISN WAN.

    b. As a result, it is possible for an LSC MG to direct a VoIP media stream (interworked from a TDM media stream from the TDM side of that MG) through an EBC to the DISN WAN, and through the DISN WAN to a remote EI or MG.

5.3.2.7.2 Summary of LSC Functions and Features

The LSC provides voice functions and features similar to a DSN EO switching system. Line-Side (Local) Custom calling features implemented at a vendor's discretion must not interfere with the functional requirements specified within the UCR 2008. Table 5.3.2-3, Summary of LSC Functions, provides a summary of LSC functions.

Table 5.3.2-3. Summary of LSC Functions

FUNCTION	DESCRIPTION
Session Control and Signaling	Verifies call request is consistent with policy rules call management, CAC, AS-SIP signaling function serving EIs: • B2BUA or Call Stateful Proxy Server (assumes that some EIs will not use AS-SIP; AS-SIP used on "trunk side"), intermediary in all inbound and outbound signaling messages to the EI. • Requests Network Resources **[Conditional]** • Control (Master-Slave) to EBC on a per session basis **[Conditional]** • Signaling interworking **[Conditional]** H.323, H.248. • PRI, MGCP, etc...
ASAC **[Required: MFSS]** **[Conditional: LSC]**	Executes AS functions in the local service domain via control of the EI and CE Router. Determines and performs preemption where required. Maintains local active session state knowledge (session precedence level, CoS, local access bandwidth used and available).
Network Management	Provides traffic call information to, and responds to traffic flow control commands from, an NMS.
Local Domain Directory	Subscriber information including telephone number, organization name, code address, and subscriber name.
MGC	**[Conditional]**
EI and User Registration	IA; access control information for authentication and authorization; EI registration: • User identification, authentication, and authorization; numbering and addressing information; user profile; CoS; precedence level.
Dialing, numbering, and routing tables; UFS Administration	Dialing, numbering, and routing tables (location services for sending call requests) re: Local calling features, multiple line appearances, voice mail, speed call.

FUNCTION	DESCRIPTION				
LEGEND					
AS	Assured Services	EBC	Edge Boundary Controller	NMS	Network Management System
ASAC	Assured Service Admission Control	EI	End Instrument	PRI	Primary Rate Interface
AS-SIP	Assured Services Session Initiation Protocol	IA	Information Assurance	RTS	Real Time Services
		LSC	Local Session Controller	UFS	User Features and Services
B2BUA	Back-to-Back User Agent	MGC	Media Gateway Controller		
CAC	Call Admission Control	MGCP	Media Gateway Control Protocol		
CoS	Class of Service				

5.3.2.7.2.1 MLPP Requirements

[Required: LSC] The LSC shall meet all the requirements for MLPP, as appropriate for VoIP and Video over IP services, as specified in UCR 2008, Section 5.2.2, Multilevel Precedence and Preemption.

5.3.2.7.2.2 Calling Number Delivery Requirements

[Required: LSC] The LSC shall support CND, as specified in UCR 2008, Section 5.2.3.5.1.8.2, Calling Number Delivery.

5.3.2.7.2.3 LSC Signaling Requirements

[Required: LSC] The LSC must provide signaling on the line side for local intra-enclave subscriber-to-subscriber calls, and trunk side signaling for calls between an external enclave and a local subscriber. An important element of signaling is the method of addressing used to forward AS-SIP requests within the network. Table 5.3.2-4, LSC Support for VoIP and Video Signaling Interfaces, provides a complete list of the LSC signaling requirements.

5.3.2.7.2.4 Service Requirements under Total Loss of WAN Transport Connectivity

[Required: LSC] In the event that a total loss of connectivity to the DISN WAN occurs, the LSC shall provide the following functions:

1. Completion of local (intra-enclave) calls

2. Routing of calls to the PSTN using a local media gateway (PRI or CAS as required by the local interface)

3. User look-up of local directory information

Table 5.3.2-4. LSC Support for VoIP and Video Signaling Interfaces

FUNCTIONAL COMPONENT	VOIP AND VIDEO SIGNALING INTERFACES	VOIP AND VIDEO SIGNALING PROTOCOLS
CCA	CCA (LSC) – to – CCA (MFSS)	AS-SIP over IP
CCA	CCA (LSC) – to – EI (details outside the scope of the this section)	AS-SIP and/or Proprietary VoIP over IP
CCA/MGC and MG	CCA (MGC) – to – MG	ITU-T H.248 over IP (used with DoD CCS7, ISDN PRI and CAS trunks) **[Objective, not Required]**
CCA/MGC and MG	CCA (MGC) – to – MG	ISDN PRI over IP (North American National ISDN Version, used with ISDN PRI trunks only) **[Objective, not Required]**
CCA/MGC and MG	CCA (MGC) – to – MG	Proprietary Supplier Protocols (used as an alternative to ITU-T Recommendation H.248 over IP and ISDN PRI over IP) (used with DoD CCS7, ISDN PRI, and CAS trunks)
CCA and SG	LSC CCA – to – LSC SG	DoD CCS7 over IP (used with DoD CCS7 trunks) **[Conditional, not Required]**
CCA and SG	LSC CCA – to – LSC SG	Proprietary Supplier Protocols Used as an alternative to DoD CCS7 over IP (used with DoD CCS7 trunks; **[Conditional, not Required]**

LEGEND

AS-SIP	Assured Services Session Initiation Protocol	IP	Internet Protocol	MFSS	Multifunction Softswitch
CAS	Channel Associated Signaling	ISDN	Integrated Services Digital Network	MG	Media Gateway
CCA	Call Connection Agent	ITU-T	International Telecommunications Union – Telecommunication	MGC	Media Gateway Controller
CCS7	Common Channel Signaling No. 7	LSC	Local Session Controller	PRI	Primary Rate Interface
DoD	Department of Defense			SG	Signaling Gateway
EI	End Instrument			VoIP	Voice over IP

5.3.2.7.2.5 Local Location Server and Directory

[Required: LSC] The purpose of the Local Location Server is to provide information on call routing and called address translation (where a called address is contained within the called SIP URI in the form of the called number). The CCA uses the routing information stored in the Local Location Server to:

1. Route internal calls from one LSC EI to another EI on the same LSC.

2. Route outgoing calls from an LSC EI to another LSC, an MFSS, or a TDM network.

3. Route incoming calls from another LSC, an MFSS, or a TDM network to an LSC EI.

5.3.2.7.2.6 LSC Management Function

[Required: LSC] The LSC Management function supports functions for LSC FCAPS management and audit logs. Collectively, these functions are called FCAPS Management and Audit Logs. A complete description of these requirements are provided in

- UCR 2008, Section 5.3.2.17, Management of Network Appliances
- UCR 2008, Section 5.3.2.18, Network Management Requirements of Appliance Functions
- UCR 2008, Section 5.3.2.19, Accounting Management.

The CCA interacts with the LSC Management function by:

1. Making changes to its configuration and to its end users' configurations, in response to commands from the Management function that requests these changes.
2. Returning information to the Management function on its FCAPS, in response to commands from the Management function that requests this information.
3. Sending information to the Management function on a periodic basis (e.g., on a set schedule), keeping the Management function up-to-date on CCA activity. An example of this update would be a periodic transfer of Call Detail Records (CDRs) from the CCA to the Management function, so that the Management function could either store the records locally or transfer them to a remote NMS for remote storage and processing.

5.3.2.7.2.7 LSC Transport Interface Functions

[Required: LSC] The LSC Transport Interface functions provide interface and connectivity functions with the ASLAN and its IP packet transport network. Examples of Transport Interface functions include the following:

- Network Layer functions: IP, IP security (IPSec)
- Transport Layer functions: IP Transport Protocols (Transport Control Protocol (TCP), User Datagram Protocol (UDP), TLS)
- LAN Protocols

The CCA interacts with Transport Interface functions by using them to communicate with EIs and the EBC (and through the EBC to other LSCs and the MFSS) over the ASLAN. The following Local Assured Services Domain elements are all IP end points on the ASLAN:

- Each EI served by the LSC
- Each MG served by the LSC (even though the MG may be physically connected to the CCA/MGC over an internal proprietary interface, instead of being connected logically to the CCA/MGC over the ASLAN)
- The CCA/IWF/MGC itself
- The EBC (for LSC, EI, and MG communication with other LSCs, MFSSs, EIs, and MGs over the DISN WAN)

As an example, the CCA interacts with the LSC Transport Interface functions when it uses IP, TLS, UDP or TCP, and the native ASLAN protocols to exchange SIP signaling messages with EIs and the EBC over the ASLAN.

The MGs controlled by the CCA interact with the LSC Transport Interface functions when they use IP, UDP, and the native ASLAN protocols to route SRTP media streams to and from EIs, other LSC MGs, and the EBC over the ASLAN.

5.3.2.7.2.8 LSC to NMS Interface

[Required: LSC] The LSC shall provide an interface to the DISA NMS. The interface consists of a 10/100 Mbps Ethernet connection as specified in UCR 2008, Section 5.3.2.4.4).

5.3.2.7.2.9 ASAC Requirements for LSC Related to Voice and Video

[Required: LSC] For ASAC requirements, see UCR 2008, Section 5.3.2.2.2.3, ASAC – Open Loop.

5.3.2.7.2.10 LSC to EI and Operator Console Status Verification

[Required: LSC] Periodically, the LSC shall verify the status of its registered and authenticated end instruments, including operator (dial service attendant) consoles. The verification interval shall be configurable with default set at 5 minutes.

5.3.2.7.2.11 Line-Side Custom Features Interference

[Conditional: LSC] Vendors may implement unique custom features applicable to the line side of the LSC.

[Required: LSC] Line side custom features must not interfere with the Assured Services requirements.

5.3.2.8 Multifunction Softswitch

The MFSS is a complex software-based call processing system that provides the full functionality of a TDM-based DSN Multifunction Switch (MFS), the full IP-based capabilities of an LSC with additional features as required to serve as a network-level softswitch. In summary, the MFSS consists of a TDM-based tandem function, TDM-based EO function, and IP-based local and tandem functions.

5.3.2.8.1 MFSS Functional Reference Model and Assumptions

Figure 5.3.2-9, Functional Reference Model – MFSS, shows the reference model for the MFSS. The boxes labeled "EO" and "Tandem" represent the TDM-based functions of the MFSS. The requirements for the TDM portion of the MFSS are entirely the same as for the MFS specified in UCR 2008, Section 5.2, Circuit-Switched Capabilities and Features.

The IP functionality and features are provided by the MFSS component labeled "Softswitch." The IP functionality is provided by several SCS functions performed by the CCA, IWF, MGC, MG, and SG. These are connected via proprietary internal interface functions.

Generic System Requirements for the CCA, MG, and SG functions and NM are provided in separate sections of UCR 2008 as follows:

- Section 5.3.2.9, Call Connection Agent, including the CCA-associated IWF that apply to both the LSC and the MFSS
- Section 5.3.2.12, Media Gateway Requirements, including MG and MGC requirements
- Section 5.3.2.13, Signaling Gateway Requirements, including SG requirements
- Section 5.3.2.17, Management of Network Appliances, including network management requirements

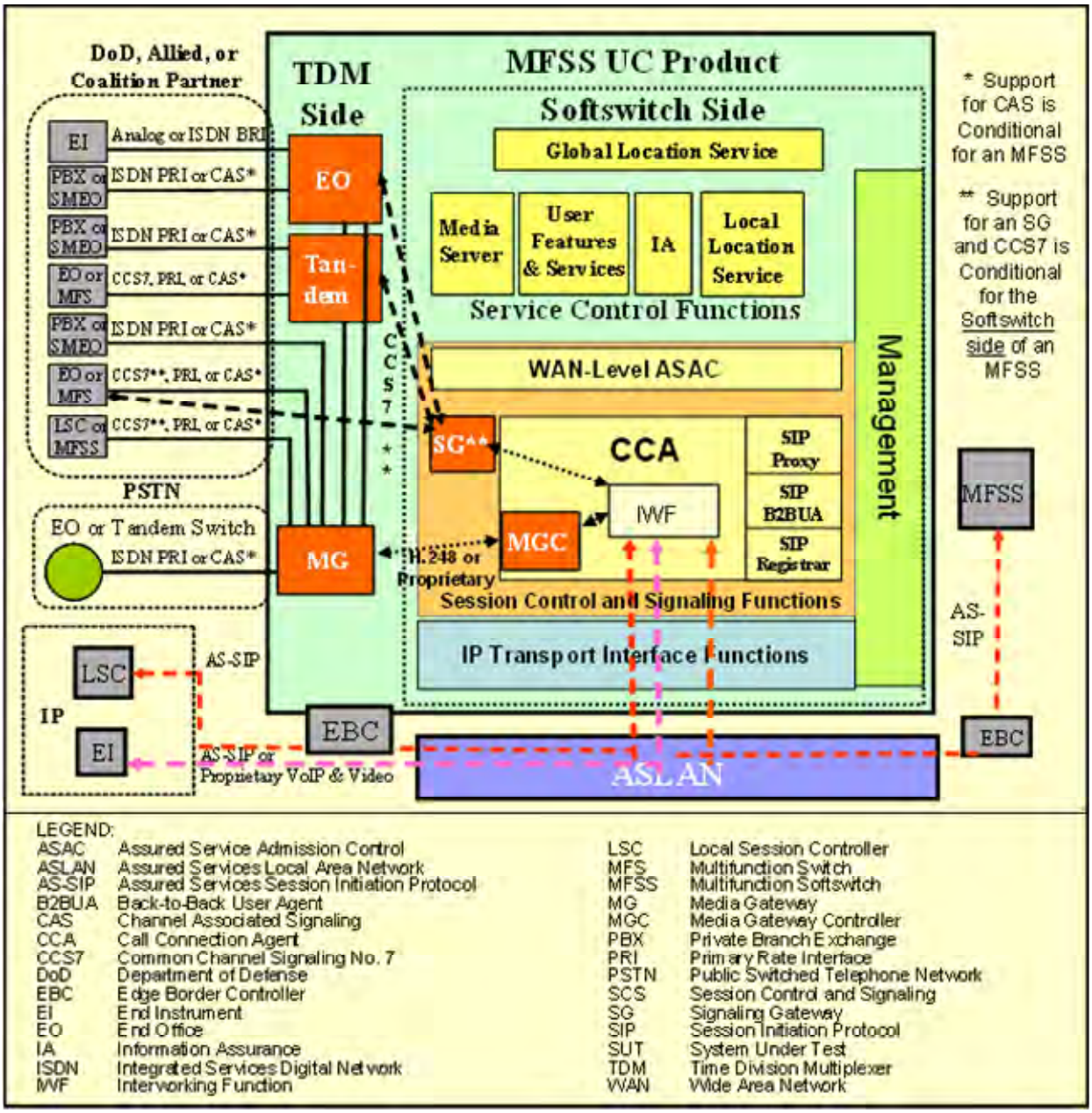


Figure 5.3.2-9. Functional Reference Model – MFSS

5.3.2.8.1.1 Assumptions – MFSS

The following assumptions are made based on the MFSS reference model:

1. Interworking between the TDM side of the MFSS and the softswitch side of the MFSS is via proprietary internal interfaces. (The interfaces will require media conversion and may be implemented using any one of the MG options at the MFSS supplier's discretion.)

2. External connections from an MFSS APL product are as follows:

    a. Connections to other IP-based systems (e.g., LSCs or MFSSs) use AS-SIP signaling.

    b. Connections to other TDM-based systems (e.g., MFS, EO, PBX, PSTN) use one of the following signaling interfaces: ISDN PRI, CCS7, or CAS.

3. The role of the CCA in the MFSS is identical to the role of the CCA in the LSC (including the underlying assumptions, roles of the IWF and MGC, interactions with other LSC components, and VoIP and Video signaling interfaces), with the following exceptions and extensions:

    a. The CCA in the MFSS interacts with both LSC-Level ASAC and WAN-Level ASAC. The MFSS supports LSC-level ASAC for admission control for calls to and from EIs that it directly serves. The MFSS also supports WAN-level ASAC for admission control for calls to and from LSCs that it directly serves.

    b. The CCA IWF in the MFSS is conditionally required to support interworking of the DoD CCS7 protocol with AS-SIP.

    c. The CCA IWF in the MFSS is required to support interworking of the ISDN PRI protocol with AS-SIP.

4. The role of the MG in the MFSS is identical to the role of the MG in the LSC (including the underlying assumptions, roles of the MG and MGC, interactions with other LSC components, and VoIP signaling interfaces), with the following exceptions and extensions:

    a. The MG in the MFSS assists the MFSS CCA in providing call denial treatments for CAC, and call-preemption treatments for LSC-Level ASAC and WAN-Level ASAC. The MFSS supports LSC-Level ASAC for admission control for calls to and from EIs that it directly serves. The MFSS also supports WAN-Level ASAC for admission control for calls to and from LSCs that it directly serves.

    b. The MG in the MFSS is required to support ISDN PRI trunks.

    c. The MG in the MFSS support for CAS trunks is Conditional.

5. Figure 5.3.2-9, Functional Reference Model – MFSS, shows the MFSS supporting a single MG on a single ASLAN. A single MFSS can also support multiple MGs on multiple ASLANs, where those ASLANs are interconnected to form a MAN or COIN. In this arrangement, it is expected that the set of ASLANs forming the MAN or COIN can meet

the single-ASLAN performance requirements in UCR 2008, Section 5.3.1, Assured Services Local Area Network Infrastructure. In this case, the MFSS supports sessions between an MG on one ASLAN and an EI, MG, or EBC on another ASLAN, as long as both ASLANs are part of the same MAN or COIN.

Another way of stating this is that a single MFSS is able to support Media Gateways at multiple physical locations. In some voice deployments, an MFSS in one location will serve ASLANs and EIs at distant locations, where both locations are part of the same regional MAN or COIN. In these cases, each distant ASLAN may want to have its own gateway to the local PSTN. In these cases, the MFSS supports Media Gateways at multiple locations over MAN or COIN infrastructures that meet the ASLAN performance requirements in UCR 2008.

6. The MFSS and the LSC are not required to support an SG. Support for an SG is conditional for both the MFSS and the LSC. As a result, the MFSS and LSC CCAs are not required to interact with the SG. As a result, support for an SG-CCA interface is Conditional for both the MFSS and LSC. The SG-CCA interface is viewed as an internal unexposed interface within the MFSS or LSC, and can be based on proprietary protocols or on various Signaling Transport (SIGTRAN) Protocols.

7. The TDM side of the MFSS provides Tandem and EO functions. Tandem functions in the MFSS provide circuit-switched network functions that terminate CCS7, PRI, and CAS type TDM trunks. The EO functions terminate ISDN, and analog EIs. These End Office and Tandem functions can interact with the softswitch side of the MFSS's CCA, MG, and SG through industry-standard external interfaces (e.g., CCS7 signaling links and TDM media trunks, as shown in Figure 5.3.2-9, Functional Reference Model – MFSS), or through internal interfaces that use protocols that are specific to a supplier's solution.

8. The MFSS supports Global Location Service (GLS) functionality, and the LSC does not. The purpose of the GLS is to provide the CCA with information on call routing and called address translation for calls that are directed outside of the MFSS (where a called address is contained within the SIP URI in the form of a called number). For example, the CCA uses the routing information stored in the Global Location Server to

   a. Route outgoing calls from MFSS EIs to other MFSSs and LSCs, and
   b. Route incoming calls from LSCs and other MFSSs to other LSCs and other MFSSs.

   However, the MFSS still uses the routing information stored in its Local Location Server to route internal calls from one MFSS EI to another, to route internal calls from an MFSS EI to an MFSS MG (and vice versa), and to route incoming AS-SIP calls from another MFSS or LSC to local MFSS EIs.

9. The MFSS interactions with its EBC are different from the LSC interactions with their EBCs.

    a. In the LSC case, the EBC controls signaling streams between an LSC connected to an ASLAN and an MFSS whose separate ASLAN is connected to the DISN WAN. In this case, the EBC also controls media streams between LSC EIs and MGs connected to the ASLAN, and EIs and MGs on other LSCs whose separate ASLANs are connected to the DISN WAN. The LSC accesses the DISN WAN via the LSC EBC and an associated PE Router on the DISN WAN. As a result, it is possible for an LSC MG to direct a VoIP media stream (interworked from a TDM media stream from the TDM side of that MG) through an EBC to the DISN WAN, and through the DISN WAN to a remote EI or MG.

    b. In the MFSS case, the EBC controls signaling streams between the MFSS where the EBC is connected to the DISN WAN and the LSCs that it serves, which are connected to the DISN WAN via their own EBCs and PE Routers. The MFSS EBC also controls signaling streams between the MFSS with its EBC connected to the DISN WAN and other MFSSs that it communicates with (with their own EBCs connected to the DISN WAN). As a result, the MFSS EBC is responsible for boundary control for both MFSS-LSC signaling and MFSS-MFSS signaling.

    c. An LSC <u>within</u> an MFSS will serve a set of (MFSS-internal) LSC EIs and MGs. These LSC EIs and MGs will exchange media streams with EIs and MGs on other LSCs located elsewhere on the DISN WAN. In this case, the <u>MFSS</u> EBC also controls these media streams between the (MFSS-internal) LSC EIs and MGs connected to the MFSS ASLAN, and EIs and MGs on other LSCs whose separate ASLANs are connected to the DISN WAN.

5.3.2.8.2 Summary of MFSS Functions and Features

The MFSS provides functions similar to the current DSN switching system referred to as an MFS, plus functions specified for an LSC with additional features as required to serve as a network-level softswitch.

5.3.2.8.2.1 TDM Side End Office and Tandem Requirements

[Required: MFSS] The requirements for the TDM side of the MFSS are entirely the same as for the DSN MFS specified in UCR 2008, Section 5.2, Circuit-Switched Capabilities and Features.

The EO and Tandem functions allow the MFSS to support connectivity to existing TDM switches in DoD networks (continental United States (CONUS) and Global), allied and coalition networks, and the PSTN worldwide (CONUS and Global).

These functions allow the MFSS to connect via EO-based and Tandem-based TDM signaling links and TDM media trunks to DoD networks, allied and coalition networks, and PSTNs worldwide. These EO and Tandem functions extend the DoD CCS7, ISDN PRI, and CAS trunk capabilities for the MFSS CCA, MG, and SG.

In addition, the EO function of the MFSS supports both analog EIs and ISDN EIs (e.g., ISDN telephones served by ISDN BRIs, and ISDN PBXs served by ISDN PRIs). This allows the MFSS to support TDM users (analog and ISDN EIs) on its TDM EO side, and to separately support VoIP and Video users (AS-SIP and Proprietary VoIP/Video users) on its IP-based softswitch side.

5.3.2.8.2.2 Global Location Server

The Global Location Server provides global location services and supports call routing where the called address points to a global destination (outside of the MFSS) rather than a local destination (within the MFSS). A called address is contained within a SIP URI in the form of a called number. UCR 2008, Section 5.3.2.10.9, CCA Interactions with Global Location Service, describes how the CCA uses routing information stored in the Global Location Server to route calls between MFSS EIs, and:

- LSCs served by the MFSS
- Other MFSSs
- DoD TDM networks
- Allied TDM networks
- Coalition TDM networks
- PSTN (CONUS and Global)

However, the MFSS still uses the routing information stored in its Local Location Server to:

- Route internal calls from one MFSS EI to another, and
- Route incoming calls to local MFSS EIs from:
  - An LSC
  - Another MFSS
  - A DoD TDM network
  - An allied or coalition TDM network, or
  - The PSTN (CONUS and Global)

5.3.2.8.2.3 MFSS Signaling Interfaces

[Required: MFSS] The MFSS shall support PRI signaling for TDM communication with other systems.

[Required: MFSS] The TDM side of the MFSS shall support CCS7 signaling for communication with other TDM systems.

[Required: MFSS] The MFSS shall support AS-SIP signaling for IP communication with other MFSSs and LSCs.

[Required: MFSS] The MFSS shall provide internal signaling and media conversion for calls between the TDM side and softswitch side of the MFSS. The method used for internal interface is left up to the supplier as long as all MLPP requirements are met.

[Conditional: MFSS] The MFSS shall provide support for (and inclusion of) the SG. An SG supports CCS7 signaling. The condition here is that the interface between the TDM side and the softswitch side of the MFSS is considered internal to the MFSS product. The MFSS supplier may choose to include an SG as the internal interface between the TDM and softswitch sides in its MFSS product.

[Conditional: MFSS] The MFSS shall support CAS signaling as required by local implementations.

The MFSS supports the VoIP, Video, and CCS7 signaling interfaces shown in Table 5.3.2-5, MFSS Support for VoIP, Video, and CCS7 Signaling Interfaces.

5.3.2.8.2.4 SG and MG Requirements for Interactions between the TDM Side and Softswitch Side of the MFSS

[Required] The CCA/SG/MGC/MG complex in the softswitch side of the MFSS needs to interface and interact with the EO and Tandem functions in the TDM side of the MFSS. The interaction required to support intra-MFSS calls will be accomplished using the following requirements:

1. "MFSS internal connections" are used between the IP-based softswitch side and the TDM side of the MFSS to provide media conversion and signaling internal to the MFSS as an APL product SUT.

2. The MFSS will use one of the following MG/SG appliances for the internal MFSS connections:

Table 5.3.2-5. MFSS Support for VoIP, Video, and CCS7 Signaling Interfaces

FUNCTIONAL COMPONENT	VoIP AND VIDEO SIGNALING INTERFACES	VoIP AND VIDEO SIGNALING PROTOCOLS
CCA	CCA (MFSS) – to – CCA (LSC)	AS-SIP over IP
CCA	CCA (MFSS) – to – CCA (Other MFSS)	AS-SIP over IP
CCA	CCA (MFSS) – to – MFSS EI (details outside of the scope of this section)	AS-SIP and Proprietary VoIP over IP (details outside of the scope of this section)
CCA/MGC and MG	MFSS CCA (MGC) – to – MFSS MG	ITU-T H.248 over IP (used with DoD CCS7, ISDN PRI, and CAS trunks) **[Objective, not Required]**
CCA/MGC and MG	MFSS CCA (MGC) – to – MFSS MG	ISDN PRI over IP (North American National ISDN Version, used with ISDN PRI trunks only) **[Objective, not Required]**
CCA/MGC and MG	MFSS CCA (MGC) – to – MFSS MG	Proprietary Supplier Protocols (used with DoD CCS7, ISDN PRI, and CAS trunks)
CCA and SG (SG Conditional	MFSS CCA – to – MFSS SG	DoD CCS7 over IP (used with DoD CCS7 trunks)
CCA and SG (SG Conditional	MFSS CCA – to – MFSS SG	Proprietary Supplier Protocols (used with DoD CCS7 trunks)
CCA, SG, and EO (SG Conditional	MFSS CCA – to – MFSS SG – to – MFSS EO	CCS7 ISUP and TCAP
CCA, SG, and Tandem (SG Conditional	MFSS CCA – to – MFSS SG – to – MFSS Tandem	CCS7 ISUP and TCAP

LEGEND

AS-SIP	Assured Services Session Initiation Protocol	IP	Internet Protocol	MFSS	Multifunction Softswitch
CAS	Channel Associated Signaling	ISDN	Integrated Services Digital Network	MG	Media Gateway
CCA	Call Connection Agent	ISUP	ISDN User Part	MGC	Media Gateway Controller
CCS7	Common Channel Signaling No. 7	ITU-T	International Telecommunications Union – Telecommunication	PRI	Primary Rate Interface
DoD	Department of Defense	LSC	Local Session Controller	SG	Signaling Gateway
EI	End Instrument			TCAP	Transaction Capabilities Application Part
EO	End Office			VoIP	Voice over IP

a. **[Required]** The MFSS MG must support internal MG connections that interconnect the softswitch side of the MFSS with the EO and Tandem functions on the TDM side of the MFSS.

b. **[Required]** The MFSS MG shall interact with the MFSS MGC so that Internal MG connections between the softswitch and TDM sides of the MFSS support:

(1) Intra-MFSS calls between TDM EIs connected to the TDM side and EIs connected to the softswitch side of the MFSS.

(2) Incoming and outgoing calls to/from systems external to the MFSS that require conversion between TDM and IP.

[Conditional] When a DoD CCS7-based connection is used between the softswitch and TDM sides of the MFSS, the MFSS MG shall interact with the MFSS MGC so that DoD CCS7 signaling is used between the softswitch and TDM sides, and the CCS7 version of the MLPP feature operates correctly between the softswitch and TDM sides of the MFSS, for both VoIP-to-TDM calls and TDM-to-VoIP calls over this connection.

[Required] When a U.S. ISDN PRI-based connection is used between the softswitch and TDM sides of the MFSS, the MFSS MG shall interact with the MFSS MGC so that U.S. ISDN PRI signaling (National ISDN PRI signaling with the Precedence Level information element (IE) and related MLPP information elements included) is used between the softswitch and TDM sides, and the T1.619/T1.619a version of the ISDN PRI MLPP feature operates correctly between the softswitch and TDM sides of the MFSS, for both VoIP-to-TDM calls and TDM-to-VoIP calls over this trunk group.

[Conditional] When a U.S. CAS-based connection is used between the softswitch and TDM sides of the MFSS, the MFSS MG shall interact with the MFSS MGC so that

- U.S. CAS trunk signaling is used between the softswitch and TDM sides, and
- The DoD version of the CAS Trunk MLPP feature as specified in UCR 2008, Section 5.2, Circuit-Switched Capabilities and Features, operates correctly between the softswitch and TDM sides of the MFSS, for both VoIP-to-TDM calls and TDM-to-VoIP calls over this trunk group.

5.3.2.8.2.5 Requirements for External Connections between MFSS and Other Systems

Calls between the MFSS and a distant-end system will be either TDM-based or IP-based as follows:

1. The TDM EO or TDM Tandem component of the MFSS will connect to another MFSS, or EO using TDM-based trunks.

2. The softswitch side of an MFSS will connect to the softswitch side of a distant-end MFSS, or a distant-end (subtending) LSC using AS-SIP and IP transport.

5.3.2.8.2.6 Features of the Softswitch Side of the MFSS

The following feature requirements apply to the softswitch side of the MFSS:

1. **[Required]** The softswitch side of the MFSS shall meet all the requirements for MLPP, as appropriate for VoIP and Video over IP services, as specified in the UCR 2008, Section 5.2.2, Multilevel Precedence and Preemption.

2. **[Required]** The softswitch side of the MFSS shall support CND as specified in UCR 2008, Section 5.2.3.5.1.8.2, Calling Number Delivery.

3. **[Required]** The requirements for SCS functions (CCA, IWF, MG, MGC, and SG) and NM are provided in separate sections of this document as follows:

    a. Section 5.3.2.9, Call Connection Agent, including the CCA-associated IWF that apply to both the LSC and the MFSS

    b. Section 5.3.2.12, Media Gateway Requirements, including MG and MGC requirements

    c. Section 5.3.2.13, Signaling Gateway Requirements, including SG requirements

    d. Section 5.3.2.17, Management of Network Appliances, including network management requirements

5.3.2.8.2.7 ASAC Requirements for the MFSS Related to Voice and Video

The ASAC requirements are specified in UCR 2008, Section 5.3.2.2.2.3, ASAC – Open Loop.

5.3.2.8.3 Network Management Requirements for the MFSS

[Required] The network management requirements for the TDM side of the MFSS are specified in UCR 2008, Section 5.2.8, Network Management.

[Required] The network management requirements for the softswitch side of the MFSS are specified in UCR 2008, Section 5.3.2.17, Management of Network Appliances, Section 5.3.2.18, Network Management Requirements of Appliance Functions, and Section 5.3.2.19, Accounting Management.

5.3.2.8.3.1 Network Management System Interface

[Required: MFSS] The MFSS shall provide a single, common interface to the DISA NMS. The single interface shall provide access to MFSS features and functions for both the TDM and softswitch side of the MFSS.

[Required: MFSS] The MFSS to NMS interface shall be a 10/100 Mbps Ethernet connection as specified in UCR 2008, Section 5.3.2.4.4.

5.3.2.9 Call Connection Agent

5.3.2.9.1 Introduction

The purpose of this section is to provide Generic System Requirements for the CCA function in the following network appliances:

- LSC
- MFSS

Each of these appliances has a DISN-defined design that includes Session Control and Signaling functions. These functions include both a Signaling Protocol IWF and a Media Gateway Controller function.

The CCA described in the following requirements is part of the SCS functions, and includes both the IWF and the MGC. As a result, the scope of these CCA requirements covers the following areas:

1. Control of AS-SIP sessions within the network appliance, including:

    a. AS-SIP sessions from/to EIs served by an LSC or MFSS appliance (NOTE: Proprietary protocol sessions from/to LSC EIs and MFSS EIs are supported also.)

    b. AS-SIP sessions from/to LSCs served by an MFSS appliance

    c. AS-SIP sessions between MFSS appliances (where sessions span multiple MFSSs)

2. Support for the following PSTN and VoIP signaling protocols:

    a. AS-SIP

    b. DoD CCS7, including MLPP

c. ISDN PRI; (North American National ISDN Version), including MLPP

d. PSTN CAS, for Dual-Tone Multifrequency (DTMF) and Multifrequency (MF) trunks (North American Version)

e. Protocol interworking of the previous signaling protocols (for example, AS-SIP ⇔ DoD CCS7 interworking) through the CCA IWF

3. Control of MGs that link the network appliance with TDM network elements through the CCA MGC in:

   a. DoD networks
   b. Allied and coalition networks
   c. PSTN in CONUS
   d. PSTN Global (i.e., outside the continental United States (OCONUS))

4. CCA support for interactions with other network appliance functions, including:

   a. SG
   b. Admission control
   c. Service Control functions
      (1) Media servers
      (2) UFS
      (3) IA
      (4) Local Location Service (LLS)
   d. Appliance Management functions
   e. GLS (in the MFSS only)
   f. EBCs

5. CCA support for voice calls and video calls

6. CCA support for Voice and Video services features and capabilities

[Required: LSC, MFSS] A CCA in an MFSS or LSC shall be able to support multiple MGs on a single ASLAN.

[Required: LSC, MFSS] A CCA in an MFSS or LSC shall be able to support multiple MGs on multiple ASLANs, where those ASLANs are interconnected to form a MAN or COIN. In this arrangement, it is expected that the set of ASLANs forming the MAN or COIN will meet the single-ASLAN performance requirements in UCR 2008, Section 5.3.1, Assured Services Local Area Network Infrastructure. In this case, the LSC shall support sessions between an MG on one

ASLAN and an EI, MG, or EBC on another ASLAN, as long as both ASLANs are part of the same MAN or COIN.

[Required: LSC, MFSS] A CCA in an MFSS or LSC shall be able to support Media Gateways at multiple physical locations. In some deployments, an LSC in one location will serve ASLANs and EIs at distant locations, where both locations are part of the same regional MAN or COIN. In these cases, each distant ASLAN may want to have its own gateway to the local PSTN. In these cases, the LSC shall support Media Gateways at multiple locations over MAN or COIN infrastructures that meet the ASLAN performance requirements in UCR 2008.

5.3.2.9.2 Functional Overview of the CCA

Figure 5.3.2-10, CCA Relationships, illustrates the relationship between the CCA and other functional components. As indicated in the figure the IWF, MGC, and SG are contained within a CCA. However, it is permissible for the SG to be in an external network appliance.

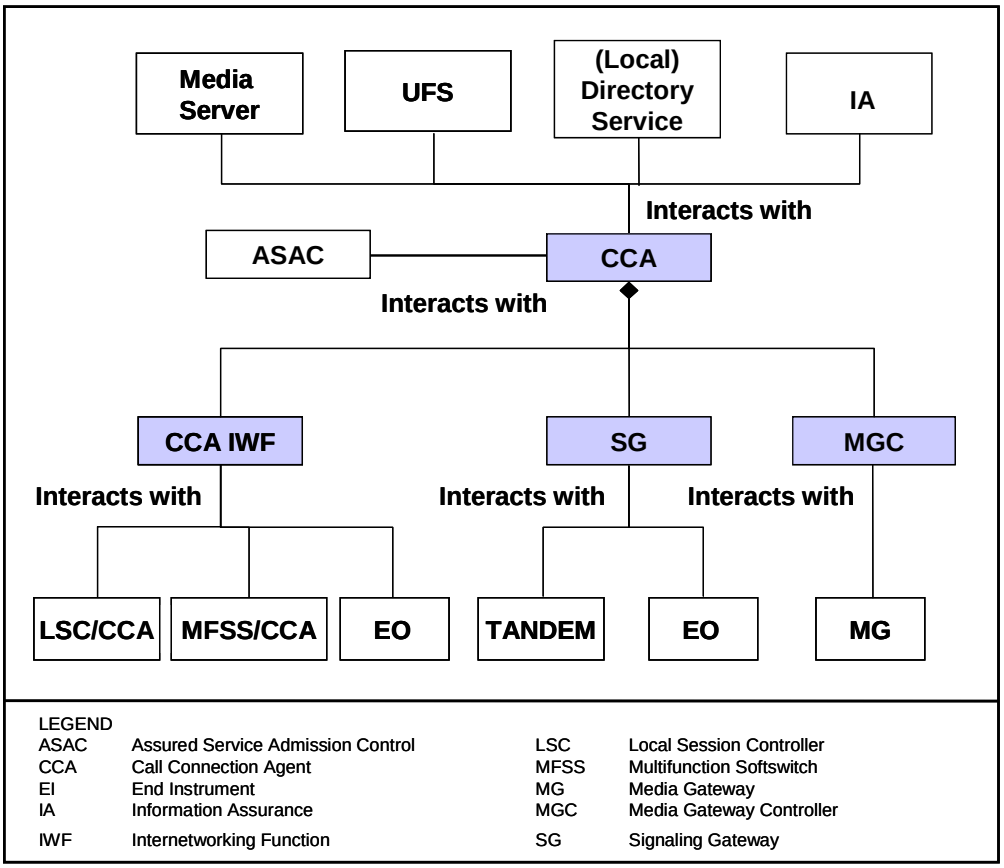


Figure 5.3.2-10. CCA Relationships

The role of a CCA is to provide session control for all VoIP sessions and Video over IP sessions that are originated by or terminated in the voice network. These VoIP and Video sessions can be established using SIP, a Proprietary VoIP protocol, AS-SIP, or some combination of these (e.g., SIP and AS-SIP on an EI/LSC/EBC/MFSS session). The CCA takes on the role of the SIP Back-to-Back User Agent (B2BUA) in the traditional SIP architecture.

In addition, the CCA takes on the role of a SIP Registrar for all EIs, MGs, and EBCs served by the LSC, allowing EIs, MGs, and EBCs to register their SIP URIs (Addresses of Record) and current IP addresses with the CCA. The CCA is responsible for maintaining a SIP-URI-to-IP-address "binding" for each EI, MG, and EBC that is active on the LSC at any moment in time.

In addition to acting as a SIP B2BUA, the CCA is responsible for providing call control and feature control for all VoIP and Video over IP network-based calls and features. All VoIP and Video over IP features that are provided to LSC EI end users, on either a per-call basis or an all-calls basis, are controlled by the CCA.

5.3.2.9.2.1 CCA IWF Component

The role of the IWF within the CCA is to

1. Support all the VoIP and TDM signaling protocols that the LSC supports for EIs, MGs, and EBCs, and

2. Interwork all these various signaling protocols with one another.

Specifically, this section requires the CCA IWF to support the following VoIP and TDM signaling protocols:

1. **[Required: LSC, MFSS]** AS-SIP.

2. **[Conditional: LSC]** Proprietary VoIP (for EIs, on the EI-LSC interface; this is conditional and may include supplier-specific SIP, supplier-specific H.323, and other supplier-proprietary protocols).

3. **[Conditional: LSC, MFSS]** DoD CCS7 including MLPP (for SG/MG trunks; North America Version Conditional; European or other Foreign PRI version Conditional when required by the DoD User).

4. **[Required: LSC, MFSS]** ISDN PRI, including MLPP (for MG trunks; North American version Required; European or other Foreign PRI version Conditional when required by the DoD user).

5. **[Conditional: LSC, MFSS]** CAS, including MLPP (for MG trunks; North American version Conditional; European or other Foreign CAS trunk version Conditional when required by the DoD user).

5.3.2.9.2.2 CCA MGC Component

The role of the MGC within the CCA is to:

1. Control all MGs within the LSC or MFSS.

2. Control all trunks (DoD CCS7, PRI, CAS) within each MG

    a. **[Required: LSC, MFSS]** Support for DoD ISDN trunks
    b. **[Conditional: LSC, MFSS]** Support for CAS trunks

3. Control all signaling and media streams on each trunk within each MG

4. Accept IP-encapsulated signaling streams from an SG or MG, and return IP-encapsulated signaling streams to the SG or MG accordingly.

    a. This approach is used for CCS7 signaling to/from an SG **[Conditional in both the MFSS and LSC Cases]**, and for PRI signaling to/from an MG.

5. Within the LSC, use either ITU-T H.248 or a supplier-proprietary protocol to accomplish these controls.

The MGC and the MG that it controls are considered Conditional – Tactical for the LSC. The SG is considered Conditional for the LSC.

5.3.2.9.2.3 SG Component

The role of the CCA with respect to the SG in the network appliance is to:

1. Control all SGs within the network appliance.

2. Control all signaling links (DoD CCS7) within each SG.

[Required: MFSS – Conditional: LSC] The CCA shall be responsible for controlling all the SGs within the MFSS and LSC. (This covers cases where there is a single SG within the network appliance, and cases that are more complex where there are multiple SGs within the network appliance.)

[Required: MFSS – Conditional: LSC] The CCA shall be responsible for controlling each signaling link within each SG within the MFSS or LSC.

[Required: MFSS – Conditional: LSC] The CCA shall be responsible for controlling the DoD CCS7 signaling stream(s) within each signaling link within each SG.

[Required: MFSS – Conditional: LSC] Within the network appliance (the MFSS and LSC), the CCA shall use either an Internet Engineering Task Force (IETF)-standard set of CCS7-over-IP protocols or a supplier-proprietary protocol to accomplish the above SG, signaling link, and signaling stream controls.

5.3.2.9.3 CCA Requirements Assumptions

The following assumptions were used to develop VoIP and Video over IP requirements for the CCA:

1. Definitions of terms can be found in UCR 2008, Appendix A, Section A2, Glossary and Terminology Description.

2. The network supports voice and video services and features. Support for other services, such as messaging and unified messaging, is not required in the Voice and Video network design in the FY2008 time frame.

3. The network consists of voice and video APL products that are supported over a converged IP transport network. The APL products include the LSC, MFSS, EBC, CE Router, and terrestrial transport products. Intersystem communication between these products and associated appliance functions is accomplished by VoIP and Video communication (e.g., use of AS-SIP signaling packets and SRTP media packets) over an underlying IP network layer and IP-based transport layer, such as UDP or TCP). For IOC, intersystem communication between these appliances can also be accomplished by voice and video communication over the existing DoD TDM network using DoD CCS7, PRI, or CAS signaling.

4. The LSC is assumed to be a local APL product located in a local domain (B/P/C/S).

5. The EBC functions are assumed to be external to the LSC and MFSS. The EBC functions are Session Border Controller (SBC)-type functions and firewall-type functions that are provided by network appliances.

6. The CCA requirements in this section support voice and video call control for originating, terminating, and tandem calls, as well as the following end-user features: Call Hold, Call

Waiting, Precedence Call Waiting, Call Forwarding, Call Transfer, Hotline Service, and Calling Party and Called Party ID (number only).

7. The CCA requirements in this section support MLPP.

8. The CCA requirements in this section assume that CCA call routing decisions are based on call routing data provided by the LLS and GLS (other functional components within the LSC and MFSS). How this routing data is established within these Location Servers and/or obtained at these Location Servers is beyond the scope of these CCA requirements.

9. The MFSS is assumed to support AS-SIP connectivity, for connections to other MFSSs and LSCs, and TDM connectivity, for connections to other MFSSs and DoD TDM switches. The TDM connectivity can use CCS7, PRI, or CAS signaling.

10. The LSC is assumed to include an MGC and an MG **[Required: Strategic – Conditional: Tactical]**, and an SG (Conditional). This means that the TDM trunk groups that terminate on the LSC MG can use PRI, CAS, or CCS7 signaling.

11. The MFSS supports end users on both the softswitch side (VoIP end users using VoIP end instruments (EIs)) and on the TDM side (traditional end users with traditional DoD telephones).

12. The MFSS also supports TDM trunk group and CCS7 signaling links on both the VoIP side (through the MGC, MG, and SG [SG Conditional]) and the TDM side (through the EO and Tandem Switch).

13. The VoIP signaling protocol used between the VoIP EI and the LSC, and between the VoIP EI and the LSC part of an MFSS, can be vendor-proprietary. The VoIP signaling protocol does not need to be AS-SIP between a VoIP EI and LSC, or between the VoIP EI and the LSC component of an MFSS, within the IOC time frame. However, the VoIP signaling protocol used between signaling appliances (i.e., LSC and MFSSs) is required to be AS-SIP in the IOC time frame.

14. The LSC and the MFSS will both use Location Services (Local or Global, as needed) to route calls to their intended destination. Location Services will be supported as an internal function of the LSC or MFSS, instead of an external function that the LSC or MFSS would have to access over an external interface using an industry-standard Location Services protocol.

15. It is assumed that route selections at the LSCs and the MFSS will be based on the originating call signaling type (i.e., either IP or TDM signaling). If the originating

signaling is IP-based, it is assumed that the call signaling will stay IP-based for as long as possible as the signaling transits the network. Similarly, if the originating call signaling is TDM-based, it is assumed that the call signaling will stay TDM-based for as long as possible as the signaling transits the network.

16. The LSC and the MFSS will use SIP URIs for addressing and routing, and will not use "tel" URIs for this purpose. See Table 5.3.2-6, An E.164 and a DSN Number, Expressed as a SIP URI and a tel: URI, for an example of an E.164 and a DSN number, expressed as a SIP URI and a tel URI.

Table 5.3.2-6. An E.164 and a DSN Number, Expressed as a SIP URI and a tel: URI

TELEPHONE NUMBER	TELEPHONE NUMBER AS SIP URI	TELEPHONE NUMBER AS tel URI
+17327582000 (an E.164 number in the United States)	sip:+17327582000@dsn.mil; user=phone	tel: +17327582000; user=phone
3144305353 (a DSN number at the Patch Barracks in Germany)	sip:3144305353; phone-context=dsn.mil @dsn.mil; user=phone (Support for the phone-context tag is an objective, and is not required for IOC)	tel: 3144305353; phone-context=dsn.mil; user=phone (Support for the phone-context tag is an objective, and is not required for IOC)

17. Tones and announcements that are provided to VoIP end users will be provided from an internal media server, which is a functional component of the LSC or MFSS. An external media server that is separate from the LSC or MFSS is not envisioned.

18. See UCR 2008, Section 5.3.2.2.2.2, Public Safety Features, for a description of 911 call handling.

19. In some cases, a function like an MGC or MG will be labeled as Conditional – Tactical in this section. In these cases, Conditional – Tactical means that normally this function is not used in a tactical environment, but may be used in that environment under certain conditions. When this function is used in that environment, the function should conform to the MGC requirements in this section. For example, an LSC deployed in one camp in a war zone overseas may not use an MGC or an MG, while another LSC deployed in another camp in the same zone may use both of them.

20. The CCA VoIP and Video over IP requirements in this section assume that all the functions within an individual appliance (i.e., LSC or MFSS) are provided by the same appliance supplier. Within a collection of network appliances, all the appliances may be provided by

the same supplier, or some appliances may be provided by one supplier and other appliances may be provided by other suppliers.

21. Interoperability between LSCs and MFSSs is the goal of the UCR 2008 and the CCA requirements in this section. Integration between the functions within an individual LSC or MFSS is the responsibility of the network appliance supplier.

22. The LSC supports MGC and MG functionality, so that LSCs can support access to DoD TDM networks, allied TDM networks, coalition partner TDM networks, and the local PSTN, when this access is needed in both strategic and tactical environments. In addition, the LSC supports MGC and MG functionality to enable TDM connectivity (i.e., PRI, CAS, and CCS7 trunks and signaling links) to interconnecting MFSSs when it is needed.

23. "Voice and Video Assured Services" supports VoIP, Voice band FoIP, Voice band Data MoIP, SCIP over IP, and Video over IP. The voice budgets used to manage end users' VoIP calls will collectively manage those users' VoIP calls, FoIP calls, MoIP calls, and SCIP over IP calls. The separate video budgets used to manage end users' Video over IP calls will manage those users' Video over IP calls <u>only</u>, and will not manage any VoIP, FoIP, MoIP, or SCIP over IP calls for those users. In short, VoIP budgets and Video over IP budgets are maintained and managed separately in Voice and Video Assured Services.

24. The LSCs and MFSSs providing Assured Services Voice and Video will support proprietary VoIP videophones (using the vendor's version of SIP or H.323) in the IOC time frame. The LSC and MFSS suppliers may support AS-SIP videophones in the IOC time frame, but are not required to. The LSC and MFSS suppliers are required to support protocol interworking between their videophones (Proprietary VoIP and AS-SIP) and the AS-SIP protocol used on network-side interfaces between LSCs and MFSSs (and between LSCs and between MFSSs) in the IOC time frame.

25. The VoIP signaling protocol used between the VoIP EI and the LSC (and between the VoIP EI and the LSC part of an MFSS) can be vendor-proprietary. The VoIP signaling protocol does not need to be AS-SIP between a VoIP EI and LSC (or between the VoIP EI and the LSC component of an MFSS) in the DoD IOC time frame. However, the VoIP signaling protocol used between signaling appliances (i.e., LSCs and MFSSs) is required to be AS-SIP in the IOC time frame.

5.3.2.9.4 Role of the CCA in Network Appliances

The role of the CCA is to provide session control for all VoIP sessions and Video over IP sessions that are originated by or terminated by EIs on the LSC. These VoIP and Video sessions can be established using either:

- **[Conditional]** AS-SIP or
- **[Conditional]** A Proprietary VoIP protocol

The CCA takes on the role of a SIP B2BUA in the traditional SIP architecture.

The CCA takes on the role of a SIP Registrar for all EIs, MGs, and EBCs served by the LSC, allowing EIs, MGs, and EBCs to register their SIP URIs (Addresses of Record) and current IP addresses with the CCA. The CCA is responsible for maintaining a SIP URI-to-IP-address "binding" for each EI, MG, and EBC that is active on the LSC at any time.

The CCA is responsible for providing call control and feature control for all VoIP and Video over IP calls and features that the LSC provides. All VoIP and Video over IP calls that are originated by or answered by LSC EI end users are controlled by the CCA. All VoIP and Video over IP features that are provided to LSC EI end users, on either a per-call basis, a per-feature-request basis, or an all-calls basis, are controlled by the CCA.

In the current DISN design for an LSC, the CCA includes an IWF and an MGC, and the MGC controls all the TDM interfaces served by the MG (DoD CCS7 trunks, ISDN PRI trunks, and CAS trunks (i.e., DTMF and MF)). This section reviews the role of the CCA in the LSC and MFSS reference models, and covers the role of the CCA, IWF, and MGC in each case.

5.3.2.9.5 CCA-IWF Signaling Protocol Support Requirements

This section describes the requirements for the CCA Signaling Protocol IWF to support the various VoIP and TDM signaling protocols used in the LSC and MFSS. In summary, the role of the IWF within the CCA is to support all the VoIP and TDM signaling protocols that are used by the EIs, MGs, and EBCs, and interwork all these various signaling protocols with one another.

5.3.2.9.5.1 CCA-IWF Support for AS-SIP

[Required: LSC, MFSS] The CCA IWF shall support the AS-SIP protocol consistent with the detailed AS-SIP protocol requirements in UCR 2008, Section 5.3.4, AS-SIP Generic System Specification.

[Required: LSC, MFSS] The CCA IWF shall use the AS-SIP protocol on LSC-MFSS and MFSS-MFSS sessions.

[Required: LSC, MFSS] When the CCA IWF uses the AS-SIP protocol over the Access Segment between the EBC and the DISN WAN, or over the DISN WAN itself, the CCA IWF shall secure the AS-SIP protocol using TLS, as described in UCR 2008, Section 5.4, Information Assurance Requirements.

5.3.2.9.5.2 CCA-IWF Support for DoD CCS7, via an SG

[Conditional: LSC, MFSS] The CCA IWF shall support the DoD CCS7 protocol, consistent with the detailed DoD CCS7 protocol requirements in the following DoD and ANSI documents:

- UCR 2008, Section 5.2.2, Multilevel Precedence and Preemption, including
  - UCR 2008, Section 5.2.2.4.3, Common Channel Signaling Number 7
  - UCR 2008, Section 5.2.2.9, MLPP CCS7
  - UCR 2008, Section 5.2.4.6, Common Channel Signaling Number 7
- ANSI T1.619-1992 (R2005)
- ANSI T1.619a-1994 (R1999)

[Conditional: LSC, MFSS] When used in the European Theater and in other OCONUS European Telecommunications Standards Institute (ETSI)-compliant countries, the CCA IWF shall support the ITU-T Q.735.3 MLPP extensions to the ITU-T CCS7 protocol, consistent with the UCR 2008 and ITU-T Recommendation Q.735.3, Stage 3 description for community of interest supplementary services using Signaling System No. 7: Multilevel precedence and preemption.

[Conditional: LSC, MFSS] The CCA IWF shall support reception of DoD CCS7 messages from the SG and transmission of DoD CCS7 messages to the SG, as described in this document. The CCA IWF shall support securing of DoD CCS7 messages to and from the SG, as described in UCR 2008, Section 5.4, Information Assurance Requirements.

[Conditional: LSC, MFSS] The CCA IWF shall be able to determine the DoD CCS7 signaling link that a CCS7 message was sent or received on (and the MG CCS7 trunk group associated with this signaling link), when processing a CCS7 message sent or received at the SG.

[Conditional: LSC, MFSS] The CCA IWF shall be able to support multiple DoD CCS7 signaling links at the SG, where each CCS7 signaling link is connected to a different CCS7 end point (i.e., to a different DoD Signaling Transfer Point (STP), a DoD TDM switch, another MFSS, or another LSC).

[Conditional: LSC, MFSS] The CCA IWF shall be able to differentiate between the individual DoD CCS7 signaling links at the SG. The CCA IWF shall know (as part of its configuration data) which DoD STP, DoD TDM switch, other MFSS, or other LSC each SG signaling link is connected to.

[Conditional: LSC, MFSS] In conjunction with the SG, the CCA IWF shall support DoD CCS7 signaling links to:

- TDM switches and STPs in the DoD TDM network
- MFSSs and LSCs in the DoD network
- TDM switches and STPs in allied and coalition partners (when those STPs support DoD CCS7)
- The TDM EO and Tandem switch components of the MFSS itself

[Conditional: LSC, MFSS] The CCA IWF shall be able to associate individual CCS7 link, ISDN User Part (ISUP), and Transaction Capabilities Application Part (TCAP) configuration data with each individual CCS7 link served by the SG and the CCA. The CCA IWF shall not require groups of CCS7 links served by the SG and the CCA to share "common" link, ISUP, and TCAP configuration data.

[Conditional: LSC, MFSS] As part of this CCS7 configuration data, the CCA IWF shall know the identity of the CCS7 device at the far end of each CCS7 signaling link. Specifically, the CCA IWF shall know the identity of each interconnected

- TDM switch and STP in the DoD TDM network
- MFSS and LSC in the DoD network
- TDM switch and STP in each allied and coalition partner
- TDM EO and Tandem switch component in the MFSS itself

5.3.2.9.5.3 CCA-IWF Support for PRI, via MG

[Required LSC, MFSS] The CCA IWF shall support the U.S./National ISDN version of the ISDN PRI protocol, consistent with the detailed ISDN PRI protocol requirements in the following DoD and ANSI documents:

1. UCR 2008, Section 5.2.9, Integrated Services Digital Network, including Table 5.2.9-4, PRI Access, Call Control, and Signaling, and Table 5.2.9-5, PRI Features.

    a. The "MFS" column in these tables shall apply to the MFSS.

    b. The "PBX1" and "PBX2" columns in these tables shall apply to the LSC.

2. UCR 2008, Section 5.2.2, Multilevel Precedence and Preemption, including

a. UCR 2008, Section 5.2.4.2, Line Signaling.

b. UCR 2008, Section 5.2.2.7, ISDN MLPP PRI.

3. ANSI T1.619-1992 (R2005).

4. ANSI T1.619a-1994 (R1999).

5. **[ETSI PRI: Required – Other Foreign PRIs: Conditional]** The appliance supplier (i.e., LSC or MFSS supplier) has the option of supporting one or more foreign versions of the ISDN PRI protocol on their product. As used here, the term "Foreign version of ISDN PRI protocol," means the version of the PRI protocol that is used in the PSTN of a foreign country.

   If an appliance supplier supports a foreign version of the ISDN PRI protocol on their product, the CCA IWF in that product shall support that foreign version of the ISDN PRI protocol consistent with the PRI protocol standards that are used in the PSTN of that foreign country.

Examples of these standards include:

1. ETSI standards on the use of ISDN PRI in European countries (and other countries that also support ETSI PRI standards)

2. Japanese Telecommunication Technology Committee (TTC) and South Korean Telecommunication Technology Association (TTA) standards on the use of ISDN PRI in Japan and South Korea, respectively

3. ITU-T standards on the use of ISDN PRI worldwide (in countries that only support ITU-T standards)

   NOTE: The ISDN-PRI/AS-SIP interworking requirements in this document only apply to the U.S. version of ISDN PRI. ISDN-PRI/AS-SIP interworking requirements for foreign versions of ISDN PRI (e.g., European, Japanese, South Korean) are outside of the scope of this document.

   NOTE: Support for ETSI PRI is required when the LSC or MFSS is used in the European Theater or in other OCONUS ETSI-compliant countries.

4. **[ETSI PRI: Required]** When used in the European Theater and in other OCONUS ETSI-compliant countries, the CCA IWF shall support the ITU-T Q.955.3 MLPP extensions to

the ITU-T ISDN PRI protocol, consistent with the UCR 2008 and the following ITU-T document:

- ITU-T Recommendation Q.955.3.

[Required: LSC, MFSS] The CCA IWF shall support reception of ISDN PRI messages from the MG and transmission of ISDN PRI messages to the MG.

[Required: LSC, MFSS] The CCA IWF shall be able to determine the ISDN PRI (and its D-Channel signaling link) that an incoming PRI message was received on, when processing an incoming PRI message from the MG.

[Required: LSC, MFSS] The CCA IWF shall be able to identify the ISDN PRI (and its D-Channel signaling link) that an outgoing PRI message will be sent on, when generating an outgoing PRI message to the MG.

[Required: LSC, MFSS] The CCA IWF shall be able to support multiple ISDN PRIs (and their D-Channel signaling links) at the MG, where each PRI is connected to a different PRI end point (e.g., to a different DoD PBX, DoD TDM switch, MFSS, LSC, PSTN PBX, or PSTN TDM switch).

[Required: LSC, MFSS] The CCA IWF shall be able to differentiate between the individual ISDN PRIs (and their D-Channel signaling links) at the MG. The CCA IWF shall know (as part of its configuration data) which DoD PBX, DoD TDM switch, MFSS, LSC, PSTN PBX, or PSTN TDM switch each ISDN PRI (and its D-Channel signaling link) is connected to.

[Required: LSC, MFSS] In conjunction with the MG, the CCA IWF shall support ISDN PRIs (and D-Channel signaling links) to:

- TDM PBXs and switches in the DoD network (This includes the TDM EO and Tandem components of the local MFSS, in the MFSS CCA/MG case.)
- MFSSs and LSCs in the DoD network
- TDM PBXs and switches in the U.S. PSTN
- TDM PBXs and switches in allied and coalition partner networks (when those networks support U.S. “National ISDN” PRI)

[Required: LSC, MFSS] The CCA IWF shall support the full set of ISDN MLPP requirements in ANSI T1.619 and ANSI T1.619A, including inclusion of the ANSI T1.619:

- Precedence level
- Cause
- Notification Indicator
- Signal
- Call Identity
- Information elements in ISDN PRI messages, on ISDN PRIs to:

  – TDM PBXs in the DoD TDM network

  – TDM switches in the DoD TDM network (This includes the TDM EO and Tandem components of the local MFSS, in the MFSS CCA/MG case.)

  – MFSSs in the DoD network

  – LSCs in the DoD network

[Required: LSC, MFSS] The CCA IWF shall not support any of the ISDN MLPP requirements in ANSI T1.619 and ANSI T1.619A, on ISDN PRIs to TDM PBXs and switches in the U.S. PSTN.

In other words, the MLPP feature and its associated ISDN PRI signaling shall be supported on ISDN PRIs from the CCA/MG to PBXs and switches in the DoD TDM network (or to appliances in the network), but shall not be supported on ISDN PRIs from the CCA/MG to PBXs and switches in the U.S. PSTN.

[Required: LSC, MFSS] On ISDN PRIs from the CCA/MG to TDM PBXs and switches in allied and coalition partners (where those networks support U.S. "National ISDN" PRI), the CCA IWF shall support a DoD-User-configurable per-PRI option that allows the PRI to support or not support the ANSI T1.619/619A PRI MLPP feature on calls to and from that PRI.

[ETSI PRI: Required – Other Foreign PRIs: Conditional] When the appliance supplier supports a foreign ISDN PRI on their product, consistent with the PRI protocol standards used in the PSTN of that foreign country, the CCA IWF (along with the MG) shall support ISDN PRIs and D-Channel signaling links to

- TDM PBXs and switches in the PSTN in that foreign country

- TDM PBXs and switches in allied and coalition partner networks (where those networks support the ISDN PRI used in the home country of the allied or coalition partner)

Support for ETSI PRI is required when the LSC or MFSS is used in the European Theater or in other OCONUS ETSI-compliant countries.

[Required: LSC, MFSS] The CCA IWF shall be able to associate individual PRI configuration data with each individual PRI served by the MG and the CCA. The CCA IWF shall not require groups of PRIs served by the MG and the CCA to share "common" PRI configuration data.

As part of this PRI configuration data, the CCA IWF shall know the identity of the PRI device at the far end of each PRI signaling link. Specifically, the CCA IWF shall know:

- The identity of each interconnected TDM PBX and TDM switch in the DoD TDM network (This includes the TDM EO and Tandem components of the local MFSS, in the MFSS CCA/MG case)

- The identity of each interconnected LSC and MFSS in the DoD network

- The identity of each interconnected TDM PBX and TDM switch in the U.S. PSTN

- The identity of each interconnected TDM PBX and TDM switch in each allied and coalition partner network (when that network supports U.S. "National ISDN" PRI)

[ETSI PRI: Required – Other Foreign PRIs: Conditional] When the appliance supplier supports a foreign ISDN PRI on their product, the CCA IWF shall know as part of PRI configuration data, the identity of the foreign PRI device at the far end of each foreign PRI. Specifically, the CCA IWF shall know

- The identity of each interconnected TDM PBX and TDM switch in the foreign PSTN
- The identity of each interconnected TDM PBX and TDM switch in each allied and coalition partner network (when that network supports the foreign ISDN PRI of the allied or coalition partner's home country)

- Support for ETSI PRI is required when the LSC or MFSS is used in the European Theater or in other OCONUS ETSI-compliant countries.

NOTE: These "foreign" ISDN PRI requirements are included to support DoD users in interconnecting their MFSSs and LSCs with the networks of foreign PSTNs, U.S. Allies, and U.S. Coalition Partners using ISDN PRIs. Detailed requirements for support of foreign ISDN PRI are outside the scope of this document.

5.3.2.9.5.4 CCA-IWF Support for CAS Trunks, via MG

[Conditional] The CCA IWF (with the MG) shall support the U.S. version of CAS trunks and trunk signaling, consistent with the CAS trunk and trunk signaling requirements in the following DoD documents:

1. DoD UCR 2008, Section 5.2.4, Signaling, including

    a. UCR 2008, Section 5.2.4.3, Trunk Supervisory Signaling
    b. UCR 2008, Section 5.2.4.4, Control Signaling
    c. UCR 2008, Section 5.2.4.5, Alerting Signals and Tones

2. DoD UCR 2008, Section 5.2.2, Multilevel Precedence and Preemption, including

    a. Section 5.2.2.4.1, Channel Associated Signaling

    b. Section 5.2.2.9, MLPP CCS7, CAS-to-CCS7 trunk interworking in a mixed media network.

[Conditional] The appliance supplier (i.e., LSC or MFSS supplier) has the option of supporting one or more foreign versions of CAS trunks and trunk signaling on their product. As used here, the term "foreign version of CAS trunks and trunk signaling," means the version of CAS trunks and trunk signaling <u>that is used in the PSTN of a foreign country</u>.

If an appliance supplier supports a foreign version of CAS trunks and trunk signaling on their product, the CCA IWF shall support the version of CAS trunks and trunk signaling <u>that is used in the PSTN of a foreign country</u>, consistent with the CAS trunk standards <u>that are used in the PSTN of that foreign country</u>. Examples of these standards include:

- ETSI standards on the use of CAS trunks in European countries (and other countries that also support ETSI CAS trunk standards)

- Japanese TTC and South Korean TTA standards on the use of CAS trunks in Japan and South Korea, respectively

- ITU-T standards on the use of CAS trunks worldwide (in countries that only support ITU-T standards)

NOTE: The CAS trunk/AS-SIP interworking requirements in this document only apply to the U.S. version of CAS trunks. The CAS trunk/AS-SIP interworking requirements for foreign

versions of CAS trunks (i.e., European, Japanese, South Korean) are outside the scope of this document.

[Conditional] The CCA IWF shall support reception of CAS signaling sequences (i.e., Supervisory, Control, and Alerting) from the MG, and transmission of CAS signaling sequences to the MG.

[Conditional] The CCA IWF shall be able to determine the MG CAS trunk and CAS trunk group that an incoming CAS signaling sequence was received on, when processing an incoming CAS signaling sequence from the MG.

[Conditional] The CCA IWF shall be able to identify the MG CAS trunk and CAS trunk group that an outgoing CAS signaling sequence will be sent on, when generating an outgoing CAS signaling sequence to the MG.

[Conditional] The CCA IWF shall be able to support multiple CAS trunk groups at the MG, where each CAS trunk group is connected to a different end point (e.g., to a different DoD PBX, DoD TDM switch, MFSS, LSC, PSTN PBX, or PSTN TDM switch).

[Conditional] The CCA IWF shall be able to differentiate between the individual CAS trunk groups at the MG. The CCA IWF shall know (as part of its configuration data) which DoD PBX, DoD TDM switch, MFSS, LSC, PSTN PBX, or PSTN TDM switch each CAS trunk group is connected to.

[Conditional] In conjunction with the MG, the CCA IWF shall support CAS trunk groups to

- TDM PBXs and switches in the DoD TDM network (This includes the TDM EO and Tandem components of the local MFSS, in the MFSS CCA/MG case.)

- MFSSs and LSCs in the DISN
- TDM PBXs and switches in the U.S. PSTN

- TDM PBXs and switches in allied and coalition networks (where those networks support U.S. CAS trunk groups)

[Conditional] The CCA IWF shall support the MLPP signaling requirements for CAS trunk groups in UCR 2008, Section 5.2.2.4.1, Channel Associated Signaling. This MLPP signaling support shall include the following four cases:

- Answered call, Trunk to be reused
- Unanswered call, Trunk to be reused

- Answered call, Trunk not to be reused
- Unanswered call, Trunk not to be reused

[Conditional] When the IWF is the appliance sending the preemption request over the CAS trunk group, the CCA IWF shall generate the measured supervisory signal (preemption signal) causing trunk circuit disconnect, with the following four variations:

- Answered call, Trunk to be reused
- Unanswered call, Trunk to be reused
- Answered call, Trunk not to be reused
- Unanswered call, Trunk not to be reused

[Conditional] When the IWF is the appliance receiving the preemption signal over the CAS trunk group, the CCA IWF shall be able to receive and act on the measured supervisory signal (preemption signal) causing trunk circuit disconnect, with the following four variations:

- Answered call, Trunk to be reused
- Unanswered call, Trunk to be reused
- Answered call, Trunk not to be reused
- Unanswered call, Trunk not to be reused

[Conditional] When the IWF is the appliance receiving the preemption request over the CAS trunk group, the CCA IWF shall generate the Preempt warning tone to the CCA-served party on the preempted call (e.g., a VoIP EI served by the CCA that is active on the preempted call).

[Conditional] When the IWF is the appliance receiving the preemption request over the CAS trunk group, the CCA IWF shall detect the Returned disconnect signal from the CCA-served party on the preempted call, and remove the Preempt warning tone from the party after this detection.

[Conditional] The CCA IWF shall support the CAS MLPP signaling as described earlier on CAS trunk groups to

- TDM PBXs and switches in the DoD TDM Network (This includes the TDM EO and Tandem components of the local MFSS, in the MFSS CCA/MG case.), and

- MFSSs and LSCs in the DISN

[Conditional] The CCA IWF shall not use the CAS MLPP signaling described earlier on CAS trunk groups to TDM PBXs and switches in the U.S. PSTN.

In other words, the MLPP feature and its associated CAS signaling shall be supported on CAS trunk groups from the CCA/MG to PBXs and switches in the DoD TDM network (or to appliances in the network), but shall not be supported on CAS trunk groups from the CCA/MG to PBXs and switches in the U.S. PSTN.

[Conditional] On CAS trunk groups from the CCA/MG to

- TDM PBXs and in allied and coalition partners (where those networks support U.S. CAS trunks)

- The CCA IWF shall support a DoD-User-configurable per-CAS-trunk group option that allows the CAS trunk group to either

  – Support the UCR 2008 CAS MLPP feature on calls to and from that trunk group, or

  – Not support the UCR 2008 CAS MLPP feature on calls to and from that trunk group.

When the "Support" option is configured, the CCA IWF shall support the CAS MLPP feature for allied and coalition partner calls on that trunk group.

When the "Not Support" option is configured, the CCA IWF shall not support the CAS MLPP feature for allied and coalition partner calls on that trunk group.

[Conditional] When the appliance supplier supports foreign CAS trunk groups on their product, the CCA IWF, along with the MG, shall support CAS trunk groups to

- TDM PBXs and switches in the PSTN in a foreign country, and
- TDM PBXs and switches in allied and coalition partner networks (where those networks support the CAS trunk groups used in the home country of the allied or coalition partner).

[Conditional] The CCA IWF shall be able to associate individual CAS trunk group configuration data with each individual CAS trunk group served by the MG and the CCA. The CCA IWF shall not require groups of CAS trunk groups served by the MG and the CCA to share "common" CAS trunk group configuration data.

[Conditional] As part of this CAS trunk group configuration data, the CCA IWF shall know the identity of the CAS device at the far end of each CAS trunk group. Specifically, the CCA IWF shall know

- The identity of each interconnected TDM PBX and switch in the TDM portion of the network (This includes the TDM EO and Tandem components of the local MFSS, in the MFSS CCA/MG case.)

- The identify of each interconnected MFSS and LSC in the DISN

- The identity of each interconnected TDM PBX and switch in the U.S. PSTN

- The identity of each interconnected TDM PBX and switch in each allied and coalition partner network (when that network supports U.S. CAS trunk groups)

[Conditional] When the appliance supplier supports foreign CAS trunk groups on their product, the CCA IWF shall know, as part of CAS trunk group configuration data, the identity of the foreign CAS device at the far end of each foreign CAS trunk group. Specifically, the CCA IWF shall know

- The identity of each interconnected TDM PBX and switch in the foreign PSTN

- The identity of each interconnected TDM switch in the foreign PSTN

- The identity of each interconnected TDM PBX and switch in each allied and coalition partner network (when that network supports the foreign CAS trunk group of the allied or coalition partner's home country)

NOTE: These "foreign" CAS trunk group requirements are included to support DoD users in interconnecting their MFSSs and LSCs with the networks of foreign PSTNs, U.S. Allies, and U.S. Coalition Partners using CAS trunk groups. Detailed requirements for support of foreign CAS trunk groups are outside the scope of this document.

5.3.2.9.5.5 CCA-IWF Support for EI Signaling Protocols

[Required: LSC, MFSS] The CCA IWF shall support supplier-proprietary Voice and Video EIs, and their associated proprietary EI signaling protocols. Proprietary EI signaling protocols, which may include a supplier's version of SIP or H.323, are permitted in IOC.

[Objective] It is desirable that the CCA IWF support the following Voice and Video EIs, and their associated EI signaling protocols

- Voice and Video SIP EIs

- Voice and Video H.323 EIs
- **[Required: FOC]** Voice and Video AS-SIP EIs

[Conditional] When the CCA IWF supports Voice and Video SIP EIs, the IWF shall support these EIs using the set of IETF SIP and Session Description Protocol (SDP) RFCs listed in UCR 2008, Section 5.3.4, AS-SIP Generic System Specification.

[Conditional] When the CCA IWF supports Voice and Video H.323 EIs, the IWF shall support these EIs using ITU-T Recommendation H.323, Packet-based multimedia communications systems, June 2006.

NOTE: An LSC or MFSS ASLAN may support two different types of Voice and Video H.323 EIs:

- H.323 EIs that are served by an H.323 Gatekeeper, which is completely separate from the CCA and its IWF, and

- H.323 EIs that are served by the CCA and its IWF (where the CCA IWF is effectively an H.323 Gatekeeper for these EIs).

In the first case, the H.323 EIs are completely independent of the CCA, MG, SG, and EBC. It is possible in this case for an H.323 EI on the local ASLAN to set up an H.323 Voice or Video call with another H.323 EI on a remote ASLAN (located elsewhere on the DISN WAN), without using any AS-SIP, and without affecting any of the AS-SIP Voice or Video budgets that are used at LSCs or MFSSs.

This first case is an “H.323 Overlay Network” case, and is outside the scope of this document.

In the second case, the H.323 EIs are dependent on the CCA, MG, SG, and EBC, for interworking with TDM voice networks, for interworking with AS-SIP, and for gaining access to the DISN WAN. When an H.323 EI on the local ASLAN makes an H.323 Voice or Video call to another H.323 EI on a remote ASLAN in this case, the “calling LSC” does H.323/AS-SIP protocol conversion, the called LSC does AS-SIP/H.323 protocol conversion, and the call is treated as an AS-SIP session (with resulting Voice or Video budget impacts) between the calling LSC, the called LSC, and any intermediate MFSSs.

This second case, while unusual, is an “H.323/AS-SIP Interworking” case, and is within the scope of this document, with one major qualification. The CCA and IWF’s use of AS-SIP in this interworking case is within the section’s scope. The details on how the supplier’s CCA and IWF perform the protocol interworking between EI H.323 and CCA AS-SIP are outside this section’s scope.

[Conditional] When the CCA IWF supports Voice and Video AS-SIP EIs, the IWF shall support these EIs using the set of AS-SIP protocol requirements in UCR 2008, Section 5.3.4, AS-SIP General System Specification (AS-SIP EIs are Required for FOC.)

5.3.2.9.5.6 CCA-IWF Support for VoIP and TDM Protocol Interworking

Per UCR 2008, Section 5.3.2.9.2.1, CCA IWF Component, the role of the IWF within the CCA is to support all the VoIP and TDM signaling protocols that the appliance supports for EIs, MGs, and EBCs, and interwork all these various signaling protocols with one another.

The requirements in this section support the IWF's interworking of the various VoIP and TDM signaling protocols together. Table 5.3.2-7, Full IWF Interworking Capabilities for VoIP and TDM Protocols, summarizes the various interworking capabilities that the appliance is required to support.

[Objective: FY10] This section covers the interworking of six VoIP and TDM "input" protocols (AS-SIP on EIs, Proprietary VoIP on EIs, AS-SIP on EBCs, DoD CCS7 on SGs, ISDN PRI on MGs, and CAS trunks on MGs) with six VoIP and TDM output protocols (also AS-SIP on EIs, Proprietary VoIP on EIs, AS-SIP on EBCs, DoD CCS7 on SGs, ISDN PRI on MGs, and CAS trunks on MGs).

Ruling out cases where the "input" and "output" protocol are the same, and combining cases where interworking between input protocol "A" and output protocol "B" also covers interworking between input protocol "B" and output protocol "A", this leaves 15 separate protocol interworking cases that need to be addressed. The number of cases is further complicated because

1. Depending on who they are connected to, ISDN PRIs can connect network appliances to either U.S. ISDN networks or foreign ISDN networks, and can either support or not support MLPP.

2. Depending on who they are connected to, CAS trunks can connect network appliances to U.S. TDM networks or foreign TDM networks, and can either support or not support MLPP.

3. An ISDN PRI or CAS trunk may be used to connect a network appliance to the U.S. PSTN, a foreign PSTN, a point in the worldwide DoD TDM network or DoD network, an allied TDM network, or a coalition partner TDM network.

Table 5.3.2-7. Full IWF Interworking Capabilities for VoIP and TDM Protocols

IWF INPUT PROTOCOL	IWF OUTPUT PROTOCOL					
	AS-SIP (TO AN EI)	AS-SIP (TO AN EBC)	PV	DOD CCS7	ISDN PRI	CAS
AS-SIP (from an EI)	*No interworking needed*	Required	Required if PV is supported	Conditional (for MFSS)	Required	Conditional
AS-SIP (from an EBC)	Required	*No interworking needed*	Required if PV is supported	Conditional (for MFSS)	Required	Conditional
PV	Required if PV is supported	Required if PV is supported	*No interworking needed*	Conditional if PV is supported	Required if PV is supported	Conditional
DoD CCS7	Conditional (for MFSS)	Conditional (for MFSS)	Conditional if PV is supported	*No interworking needed*	Conditional (for MFSS) (per UCR 2007)	Conditional
ISDN PRI	Required	Required	Required if PV is supported	Conditional (for MFSS) (per UCR 2007)	*No interworking needed*	Conditional
CAS	Conditional	Conditional	Conditional	Conditional	Conditional	*No interworking needed*

LEGEND:

AS-SIP	Assured Services Session Initiation Protocol	MFS	Multifunction Switch
CAS	Channel-Associated Signaling	MFSS	Multifunction Softswitch
CCS7	Common Channel Signaling No. 7	PBX	Private Branch Exchange
DoD	Department of Defense	PRI	Primary Rate Interface
EBC	Edge Boundary Controller	PV	Proprietary VoIP
EI	End Instrument	SG	Signaling Gateway
EO	End Office	UCR	Unified Capabilities Requirements
ISDN	Integrated Services Digital Network	TDM	Time-Division Multiplexing
IWF	Inter Working Function	VoIP	Voice over Internet Protocol
LSC	Local Session Controller		

As a result, this section addresses a wide variety of protocol interworking cases. All cases included are believed to be relevant to DoD networks worldwide.

In the following requirements, interworking is only required where the network appliance supplier supports both the AS-SIP protocol and the other protocol in the requirement.

[Required] When they are present in the network appliance, the CCA IWF shall interwork the protocols for the following cases (These cases shall include support for both Voice and Video EIs, unless noted otherwise.):

- AS-SIP protocol via AS-SIP EIs with the supplier's proprietary VoIP EI protocol

- **[Conditional: LSC, MFSS]** AS-SIP protocol via AS-SIP EIs with the DoD CCS7 protocol

- AS-SIP protocol via AS-SIP EIs with the U.S. ISDN PRI protocol

- **[Required: ETSI PRI – Conditional: Other Foreign PRIs]** AS-SIP protocol via AS-SIP EIs with the appropriate foreign ISDN PRI protocol

- **[Conditional]** AS-SIP protocol via AS-SIP EIs with the U.S. CAS trunk protocol

- **[Conditional]** AS-SIP protocol via AS-SIP EIs with the appropriate foreign CAS trunk protocol

[Required] When they are present in the network appliance, the CCA IWF shall interwork the protocols for the following cases (These cases shall include support for both VoIP and Video EIs, unless noted otherwise.):

- **[Conditional: LSC, MFSS]** Proprietary VoIP EI protocol with the DoD CCS7 protocol

- Proprietary VoIP EI protocol with the U.S. ISDN PRI protocol

- **[Required: ETSI PRI – Conditional: Other Foreign PRI]** Proprietary VoIP EI protocol with the appropriate foreign ISDN PRI protocol

- **[Conditional]** Proprietary VoIP EI protocol with the U.S. CAS trunk protocol
- **[Conditional]** Proprietary VoIP EI protocol with the appropriate foreign CAS trunk protocol

[Required] When they are present in the network appliance, the CCA IWF shall interwork the protocols for the following cases (These cases shall include both VoIP and Video EIs, unless noted otherwise.):

- AS-SIP protocol via EBCs with the supplier's Proprietary VoIP EI protocol

- **[Conditional: LSC, MFSS]** AS-SIP protocol via EBCs with the DoD CCS7 protocol

- AS-SIP protocol via EBCs with the U.S. ISDN PRI protocol

- **[Required: ETSI PRI – Conditional: Other Foreign PRI]** AS-SIP protocol via EBCs with the appropriate foreign ISDN PRI protocol

- **[Conditional]** AS-SIP protocol via EBCs with the U.S. CAS trunk protocol

- **[Conditional]** AS-SIP protocol via EBCs with the appropriate foreign CAS trunk protocol

5.3.2.10 CCA Interaction with Network Appliances and Functions

This section describes how the CCA interacts with network appliances and appliance functions. These other appliance functions include

- ASAC
- Service control functions
- NM (FCAPS and audit logs)
- Transport interface functions
- EBC (not part of the LSC but part of the local assured services domain)

5.3.2.10.1 CCA Interactions between the Softswitch and TDM Sides of the MFSS

The CCA/SG/MGC/MG complex in the MFSS must provide interoperability between the softswitch side and TDM side in the MFSS (using connections based on either CCS7, U.S. PRI, or U.S. CAS signaling at the discretion of the vendor). In this case, some high-level requirements for this interworking are needed. These high-level requirements are included in this section.

[Required] The MFSS CCA shall be able to support MG connections between the softswitch side of the MFSS and the EO and Tandem functions on the TDM side of the MFSS.

[Conditional] When a DoD CCS7 connection is used between the softswitch and TDM sides of the MFSS, the MFSS CCA shall control the MG function and its associated SG signaling link so that

1. DoD CCS7 signaling is used between the softswitch and TDM sides, and

2. The CCS7 version of the MLPP feature operates correctly between the softswitch and TDM sides of the MFSS, for both VoIP-to-TDM calls and TDM-to-VoIP calls over this trunk group.

[Required] When a U.S. ISDN PRI connection is used between the softswitch and TDM sides of the MFSS, the MFSS CCA shall control the MG function so that

1. U.S. ISDN PRI signaling (national ISDN PRI signaling, with the Precedence Level IE and related MLPP IEs included) is used between the softswitch and TDM sides, and

2. The ANSI T1.619/T1.619a version of the ISDN PRI MLPP feature operates correctly between the softswitch and TDM sides of the MFSS, for both VoIP-to-TDM calls and TDM-to-VoIP calls over this trunk group.

[Conditional] When a U.S. CAS connection is used between the softswitch and TDM sides of the MFSS, the MFSS CCA shall control the MG function so that

1. U.S. CAS trunk signaling is used between the softswitch and TDM sides, and

2. The UCR 2008 version of the CAS trunk MLPP feature operates correctly between the softswitch and TDM sides of the MFSS, for both VoIP-to-TDM calls and TDM-to-VoIP calls over this trunk group.

[Required] The MFSS CCA shall use MG connections between the softswitch and TDM sides of the MFSS to support

- TDM calls between the TDM EO/Tandem and IP EIs on the MFSS, allowing calls between EO lines and IP EIs, and calls between EO and Tandem trunks and MFSS EIs

- TDM calls between the TDM EO/Tandem and the EBC on the MFSS, allowing calls between EO lines and other appliances on the DISN WAN, and calls between EO and Tandem trunks and other appliances on the DISN WAN

- TDM calls between the TDM EO/Tandem and other MG trunk groups on the MFSS, allowing calls between EO lines and these trunk groups, and calls between EO and Tandem trunks and these trunk groups

5.3.2.10.2 CCA Support for Appliance Management Functions

Requirements for CCA support for Appliance Management functions are found in UCR 2008, Section 5.3.2.18.1, Management Requirements of the CCA Function.

5.3.2.10.3 CCA Interactions with Transport Interface Functions

The Transport Interface functions in an appliance provide interface and connectivity functions with the ASLAN and its IP packet transport network. High-level requirements for these functions are outlined within this section. The detailed implementation methods for these requirements are left up to each vendor. Examples of Transport Interface functions include:

- Network Layer functions: IP and IPSec
- Transport Layer functions: TCP, UDP, Stream Control Transmission Protocol (SCTP), TLS
- LAN protocols

The CCA interacts with Transport Interface functions by using them to communicate with EIs, the EBC, the MGs, and the SG over the ASLAN. The following appliance elements are all IP end points on the ASLAN:

- Each EI
- Each MG and SG (even though the MG or SG may be physically connected to the CCA over an internal proprietary interface, instead of being logically connected to the CCA over the ASLAN)
- The CCA/IWF/MGC itself
- The EBC (for LSC, EI, and MG communication with other LSCs, MFSSs, EIs, and MGs over the DISN WAN)

As an example, the CCA interacts with the LSC Transport Interface functions when it uses IP, TLS, UDP or TCP, and the native ASLAN protocols to exchange SIP signaling messages with EIs and the EBC over the ASLAN.

The MGs controlled by the CCA interact with the LSC Transport Interface functions when they use IP, UDP, and the native ASLAN protocols to route SRTP media streams to and from EIs, other LSC MGs, and the EBC over the ASLAN.

[Required] The CCA shall support assignment of the following items to itself:

- At least one CCA IP address,
- A CCA Fully Qualified Domain Name (FQDN) that maps to that IP Address, and
- A CCA SIP URI that uses that CCA FQDN as its domain name, and maps to the "SIP B2BUA" function within the CCA itself

[Required] The CCA shall support assignment of the following items to each SIP and AS-SIP EI on the Appliance LAN:

- At least one EI IP address,
- An EI FQDN that maps to that IP address, and
- An EI SIP URI that uses that EI FQDN as its domain name, and maps to the "SIP User Agent" function within the EI

[Required] The CCA shall support assignment of the following items to each MG on the Appliance LAN:

- At least one MG IP address,
- An MG FQDN that maps to that IP address, and
- An MG SIP URI that uses that MG FQDN as its domain name, and maps to the "RTS Signaling and Media End Point" function within the MG.

[Required: MFSS – Conditional: LSC] The CCA shall support assignment of the following items to each SG on the Appliance LAN:

- At least one SG IP address,
- An SG FQDN that maps to that IP address, and
- An SG SIP URI that uses that SG FQDN as its domain name, and maps to the "RTS Signaling End Point" function within the SG.

[Required] The CCA shall support assignment of the following items to the EBC:

- At least one EBC IP address,
- An EBC FQDN that maps to that IP address, and
- An EBC SIP URI that uses that EBC FQDN as its domain name, and maps to the "SIP B2BUA" function within the EBC.

5.3.2.10.4 CCA Interactions with the EBC

The EBC provides SBC and firewall capabilities for the ASLAN, the EIs, and the IP-based components of the LSC, including the CCA/IWF/MGC and the MGs.

The CCA interacts with the EBC by directing AS-SIP signaling packets to it (for signaling messages destined for an MFSS) and by accepting AS-SIP signaling packets from it (for signaling messages directed to the LSC from an MFSS).

The LSC EIs and MGs, which are controlled by the CCA, interact with the EBC by directing SRTP media streams to it (for call media destined for EIs and MGs on other LSCs) and by accepting SRTP media streams from it (for call media directed to the LSC EIs and MGs from EIs and MGs on other LSCs).

The AS-SIP signaling packets exchanged between the LSC and an MFSS must pass through the EBC. The SRTP media streams exchanged between LSC EIs/MGs and EIs/MGs on other LSCs must also pass through the EBC.

The CCA in the MFSS and LSC needs to interact with AS-SIP functions in the EBC, which

- Mediates AS-SIP signaling between an LSC and an MFSS, and between two MFSSs
- Supports SBC functions, such as Network Address Translation (NAT) and Network Address and Port Translation (NAPT), and
- Supports IP firewall functions.

High-level CCA requirements are needed for interacting with an EBC. These requirements are as follows:

1. **[Required]** When directing VoIP Sessions to other network appliances providing voice and video services across the DISN, the CCA shall direct these VoIP Sessions to the EBC, so that the EBC can process them before directing them to the network appliances on the DISN WAN.

2. **[Required]** The CCA shall direct VoIP sessions to other network appliances through the EBC in the following cases:

    a. When the CCA is part of an LSC and is directing VoIP sessions to an MFSS on the DISN WAN, which is the "parent" MFSS for that LSC

    b. When the CCA is part of an MFSS and is directing VoIP sessions to an LSC on the DISN WAN, which is a "child" LSC for that MFSS

    c. When the CCA is part of an MFSS and is directing VoIP sessions to another MFSS on the DISN WAN

3. **[Required]** When accepting VoIP sessions from other network appliances on the DISN, the CCA shall accept these VoIP sessions from the EBC, because that the EBC relays them from the network appliances on the DISN WAN.

4. **[Required]** The CCA shall accept VoIP sessions from other network appliances through the EBC in the following cases:

    a. When the CCA is part of an LSC and is accepting VoIP Sessions from an MFSS on the DISN WAN, which is the "parent" MFSS for that LSC

    b. When the CCA is part of an MFSS and is accepting VoIP sessions from an LSC on the DISN WAN, which is a "child" LSC for that MFSS

    c. When the CCA is part of an MFSS and is accepting VoIP sessions from another MFSS on the DISN WAN

5.3.2.10.5 CCA Support for Admission Control

The CCA interacts with the ASAC component of the LSC and MFSS to perform specific functions related to ASAC, such as counting internal, outgoing, and incoming calls, managing separate call budgets for VoIP and Video over IP calls, and providing preemption.

Requirements for ASAC are handled in two categories: CAC and ASAC. CAC is defined as follows:

> "A process in which a call is accepted or denied entry (blocked) to a network based on the network's ability to provide resources to support the quality of service (QoS) requirements for the call."

Call Admission Control is also referred to as Session Admission Control (SAC), because in the network appliances a VoIP call is also a SIP Voice session, and a Video call is also a SIP Video session. SAC is limited as follows:

> "In the IOC, SAC is typically limited to managing the pre-populated session budgets for each Assured Service (voice and video)."

Assured Services Admission Control includes CAC/SAC (and its support for call counting, voice call budgets, and video call budgets). In addition, ASAC includes capabilities for handling calls differently based on their precedence level (e.g., DSN ROUTINE, PRIORITY, IMMEDIATE, FLASH, or FLASH OVERRIDE), and for having calls of a higher precedence level preempt calls of a lower precedence level.

Two different levels of ASAC are LSC-Level ASAC (supported in the LSC and the MFSS) and WAN-Level ASAC (supported in the MFSS only). The LSC and MFSS are responsible for maintaining:

- VoIP session budgets
- VoIP session counts
- TDM session budgets
- TDM session counts
- VSU budgets
- VSU counts

[Required] The LSC and MFSS CCA shall meet all the requirements in UCR 2008, Section 5.3.2.2.2.3, ASAC – Open Loop.

[Required] The LSC and MFSS CCA shall meet all the requirements in UCR 2008, Section 5.3.4.10, Precedence and Preemption.

[Required] The LSC and MFSS CCA shall meet all the requirements in UCR 2008, Section 5.3.4.11, Policing of Call Count Thresholds.

5.3.2.10.6 CCA Support for UFS

The UFS Server is responsible for providing features and services to VoIP and Video EIs on an LSC or MFSS, where the CCA alone cannot provide the feature or service. In this section, no distinction is made between "features" and "services," and all features and services, such as Call Hold, Call Waiting, Precedence Call Waiting, Call Transfer, Call Forwarding, Hotline Service, and Calling Party and Called Party ID (number only), are called features. Examples of features that may require the use of a UFS Server are voice mail services, services that use TCAP queries

and responses over CCS7 signaling links, such as toll-free 800/888 number services and calling name delivery services, and services that require screening of calling party numbers on incoming calls (e.g., block calls to this VoIP EI from these numbers) and screening of called party numbers on outgoing calls (e.g., block calls from this VoIP EI to these numbers).

The CCA interacts with UFS by relaying end user requests for feature and service invocation to the UFS, and relaying UFS responses, such as text displays and message waiting indicators, back to EIs and end users. The CCA may relay feature information from the UFS to the EI and end user without a corresponding feature request from the EI or the end user. (Examples of this are the UFS text message that tells an EI that a call waiting call is available and the UFS indicator that tells an EI that there is a message waiting for that EI.)

[Required] The CCA within a network appliance shall support the operation of the following features and capabilities as listed in Table 5.3.2-2, Assured Services System Features and Capabilities:

1. **[Required]** The CCA shall generate a redirecting number each time it forwards a VoIP or Video Session request as part of a Call Forwarding feature.

2. The CCA supports the ability to direct VoIP and Video Sessions and session requests to the UFS Server, so that the UFS Server can apply an Appliance VoIP or Video feature, when use of that feature is required by the calling party, required by the called party, or required by the appliance itself.

The interface and protocols used to interconnect the CCA with the UFS Server are internal to the network appliance, and are therefore supplier-specific.

5.3.2.10.7 CCA Support for Information Assurance

The IA function within the appliance ensures that end users, EIs, MGs, SGs, and EBCs that use the appliance are all properly authenticated and authorized by the appliance. The IA function ensures that Voice and Video signaling streams and media streams that traverse the appliance and its ASLAN are properly encrypted (using SIP/TLS and SRTP, respectively).

[Required] The CCA shall relay received SIP and TLS authentication credentials and encryption key information from sending end systems (i.e., users, EIs, and EBCs) to the IA function, to support the IA function's user, EI and EBC authentication capabilities, and its EI and EBC signaling stream encryption capabilities.

[Required: MG – Conditional: SG] The CCA MGC shall relay received H.248 and IPSec (or proprietary-protocol-equivalent) authentication credentials and encryption key information from

sending end systems (i.e., MGs and SGs) to the IA function, to support the IA function's MG and SG authentication capabilities, and its MG and SG signaling stream encryption capabilities.

[Required] The CCA shall relay received SRTP encryption key information from sending end systems (i.e., EIs, MGs, and EBCs) to the IA function, to support the IA function's EI, MG, and EBC media stream encryption capabilities.

[Required] The CCA shall relay authentication credentials received in a SIP or AS-SIP REGISTER message from an EI or EBC to the IA function, so that the IA function can validate those credentials and allow that EI or EBC to register with the appliance.

[Conditional] The CCA MGC shall relay authentication credentials received with an H.248 message in an IPSec packet from an MG to the IA function, so that the IA function can validate those credentials and allow that MG to register with the appliance.

[Conditional] The CCA MGC shall relay authentication credentials received in an IPSec packet from an SG to the IA function, so that the IA function can validate those credentials and allow that SG to register with the appliance.

[Required] The CCA shall relay TLS encryption key information received from an EI to the IA function, so that the IA function can verify that this encryption key information can be used on the resulting signaling stream for the resulting Voice or Video Session from that EI.

[Required] The CCA shall relay TLS encryption key information received from an EBC to the IA function, so that the IA function can verify that this encryption key information can be used on the resulting signaling stream for the resulting Voice or Video Session from that EBC.

[Required] The CCA shall relay SRTP encryption key information received in a SIP or AS-SIP INVITE message from an EI to the IA function, so that the IA function can verify that this encryption key information can be used on the resulting media stream for the resulting Voice or Video Session from that EI.

[Required] The CCA shall relay SRTP encryption key information received in an AS-SIP INVITE message from an EBC to the IA function, so that the IA function can verify that this encryption key information can be used on the resulting media stream for the resulting Voice or Video Session from that EBC.

[Conditional] The CCA shall relay SRTP encryption key information received in an H.248 message in an IPSec packet from an MG to the IA function, so that the IA function can verify that this encryption key information can be used on the resulting media stream for the resulting Voice Session from that MG.

[Required] The CCA within the appliance shall support all of the IA Appliance requirements in UCR 2008, Section 5.4, Information Assurance Requirements, that involve the appliance's SCS functions and the appliance's MGC.

The interface and protocols used to interconnect the CCA with the IA function are internal to the appliance, and are therefore supplier-specific.

5.3.2.10.8 CCA Interactions with Local Location Service

The LLS Server provides information on called address translation in response to call routing queries from the CCA. The CCA sends call routing queries to the LLS Server for both outgoing calls from appliance EIs (i.e., LSC and MFSS) and incoming calls to appliance EIs (i.e., LSC and MFSS).

The CCA uses the information returned by the LLS Server to

- Route internal calls from one appliance EI to another,
- Route outgoing calls from an appliance EI to another appliance (via an EBC or an Appliance MG), or to a TDM network (via an Appliance MG), and
- Route incoming calls from another appliance (via an EBC or an Appliance MG), or from a TDM network (via an Appliance MG), to an LSC EI.

The interface and protocols used to interconnect the CCA with the LLS Server are internal to the appliance, and are therefore supplier-specific.

5.3.2.10.9 CCA Interactions with Global Location Service

Like the LLS Server, the Global Location Server provides information on call routing in response to call routing queries from the CCA. The CCA sends call routing queries to the Global Location Server for calls <u>where the CCA determines that the call's destination lies outside of the MFSS</u>.

Call routing/addressing will involve two basic scenarios: MFSS internal calls or external calls.

1. MFSS internal calls are defined as local calls within the MFSS. These calls are any combination of calls among and between IP instruments and TDM instruments served by either the TDM side or softswitch side of the MFSS. Calls between the TDM and softswitch sides of the MFSS are routed over internal, proprietary connections requiring an internal MG.

2. External calls are defined as calls to/from the MFSS and other distant-end systems and networks, including other MFSSs, DSN EOs, PBXs, and the PSTN. Calls to or from TDM-based distant-end systems will route through the TDM side of the MFSS; calls to IP-based distant-end systems (i.e., LSCs, MFSS) will route through the softswitch side of the MFSS using IP-bearer and AS-SIP signaling.

The CCA may determine call routing based on an analysis of the called address (for example, by finding that this address did not contain a PSTN escape code as a prefix, and by finding that the first six digits of this called address (i.e., the NPA-NXX in the DoD dialing plan) pointed to a location in the DoD network outside of the MFSS). The CCA may make this determination based on a previous call routing response from the MFSS's LLS that indicated, "This address is not assigned to any EI or MG on the MFSS."

As in the LLS Server case, the query from the CCA to the Global Location Server identifies the called address for the call in question (which may be embedded within a SIP URI, e.g., sip: +17327582000@dsn.mil; user=phone, or sip: 3144305353@dsn.mil; user=phone). The response from the Global Location Server identifies either:

- A remote IP address that points to the next appliance (i.e., an LSC or an MFSS) that the call should be routed to, or

- The local IP address of an MFSS MG trunk group that the call should be routed to. (This case applies when the MG TG connects to a TDM destination outside the MFSS, which can be on the DoD TDM network, an allied or coalition partner TDM network, or on the PSTN (CONUS and Global)).

5.3.2.10.10 CCA Interactions with End Instrument(s)

The CCA in the MFSS or LSC needs to interact with VoIP EIs served by that MFSS or LSC. The VoIP interface between the EI and the MFSS, or LSC, is left up to the network appliance supplier in FY2008. Detailed requirements for this VoIP interface are not included in this section.

However, the following high-level requirements on VoIP EIs do apply and are part of the CCA requirements for the MFSS or LSC:

1. **[Required]** The CCA shall support supplier-proprietary Voice and Video EIs, using EI-CCA protocols that are proprietary to the LSC or MFSS supplier.

2. **[Objective]** It is desirable that the CCA support the following Voice and Video EIs, and their associated EI signaling protocols:

    - SIP Voice and Video EIs
    - H.323 Voice and Video EIs
    - **[Required: FY12]** AS-SIP Voice and Video EIs

[Objective] When the CCA IWF supports H.323 Voice and Video EIs, the IWF shall support these EIs using ITU-T Recommendation H.323, Packet-based multimedia communications systems, June 2006.

NOTE: An LSC or MFSS ASLAN may support two different types of H.323 EIs:

1. "H.323 Overlay Network": H.323 EIs that are served by an H.323 Gatekeeper, which is completely separate from the CCA, and

2. "H.323/AS-SIP Interworking": H.323 EIs that are served by the CCA (where the CCA is effectively an H.323 Gatekeeper for these EIs).

The first case is outside the scope of this section.

The second case is within the scope of this section, with one qualification. The CCA's use of AS-SIP in this case is within the section's scope, but the details on how the supplier's CCA performs the protocol interworking between EI H.323 and CCA AS-SIP are outside this section's scope.

[Conditional] When the CCA IWF supports AS-SIP Voice and Video EIs, the IWF shall support these EIs using the set of AS-SIP protocol requirements in UCR 2008, Section 5.3.4, AS-SIP General System Specification.

5.3.2.10.11 CCA Support for Assured Services Voice and Video

[Required] The Appliance CCA (i.e., LSC or MFSS) shall support both assured Voice and Video services. The CCA shall support both assured Voice and assured Video sessions, and shall support these sessions from both VoIP EIs and Video EIs, as described in UCR 2008, Section 5.3.2.10.10, CCA Interactions with End Instrument(s).

[Required] The Appliance CCA shall support common procedures and protocol for VoIP and Video session control, with the following clarifications and exceptions:

1. The CCA is required to be able to support "single-rate" TDM video (i.e., 64 kbps TDM video calls) at MG trunk groups that are controlled by the CCA.

2. The CCA is not required to be able to support "multi-rate" TDM video (i.e., Nx64 kbps TDM video calls, where N runs from 2 to 24) at MG trunk groups that are controlled by the CCA.

The CCA is not required to support protocol interworking between TDM video calls and

- IP video sessions that originate from or terminate on local Video EIs that are served by the CCA, or

- IP video sessions that originate from or terminate on remote Video EIs, that reach the CCA via the EBC, the DISN WAN, and remote appliances.

[Required] The Appliance CCA shall support common procedures and protocol for feature control, for the features and capabilities given in Table 5.3.2-2, Assured Services System Features and Capabilities.

[Required] On calls to and from Proprietary VoIP and Proprietary Video EIs, the CCA shall use the appropriate parameters within the appliance supplier's Proprietary protocol messages to differentiate Proprietary VoIP sessions from Proprietary Video sessions.

[Conditional] When H.323 EIs are supported, on calls to and from H.323 EIs, the CCA shall use the appropriate parameters within the H.323 protocol messages to differentiate H.323 VoIP sessions from H.323 Video sessions.

[Conditional] When AS-SIP EIs are supported, on calls to and from AS-SIP EIs, the CCA shall use the SDP message bodies in AS-SIP INVITE, UPDATE, REFER, and ACK messages, as well as the SDP message bodies in AS-SIP 200 OK responses and earlier 1xx provisional responses, to differentiate AS-SIP Voice sessions from AS-SIP Video sessions. (NOTE: Support for AS-SIP EIs is Required for FY12.)

The CCA's use of these SDP bodies for VoIP and Video differentiation shall follow the detailed SDP requirements for VoIP and Video in UCR 2008, Section 5.3.4, AS-SIP Requirements.

[Required] The CCA shall track VoIP sessions against corresponding Appliance VoIP budgets, and shall **separately track** Video sessions against corresponding Video budgets. The CCA shall

maintain the Appliance's VoIP budgets separate from the Appliance's Video budget. The CCA shall perform this separate tracking of Appliance VoIP and Video calls and budgets consistent with the CAC/SAC requirements in UCR 2008, Section 5.3.2.10.5, CCA Support for Admission Control.

[Required] As part of LSC-Level ASAC and WAN-Level ASAC, the CCA shall support MLPP for both VoIP sessions and Video sessions, consistent with the ASAC/MLPP requirements in UCR 2008, Section 5.3.2.10.5, CCA Support for Admission Control.

[Required] The CCA shall allow an individual EI (Proprietary, H.323, or AS-SIP) to support both VoIP and Video sessions. The CCA shall allow an individual EI to have both VoIP and Video sessions active at the same time.

[Required] The CCA shall support the routing of both VoIP and Video session requests from LSCs to MFSSs, from MFSSs to LSCs, and from MFSSs to MFSSs, using AS-SIP. The CCA shall direct outgoing VoIP and Video session requests to EBCs, and shall accept incoming VoIP and Video session requests from EBCs, consistent with this LSC-to-MFSS routing, MFSS-to-LSC routing, and MFSS-to-MFSS routing.

5.3.2.10.12 CCA Interactions with Service Control Functions

[Required] The CCA shall support the ability to remove VoIP and Video sessions and session requests from the media server, so that the CCA can continue with necessary session processing once the media server has completed its functions. Examples include the following:

1. Removing a calling VoIP EI from the media server after dial tone has been applied and then removed, or once in-band audible ringing has been applied and then removed (for a local EI-to-EI call).

2. Removing a called VoIP EI from the media server after a Call Preemption tone or announcement has been applied and then removed.

The interface and protocols used to interconnect the CCA with the media server are internal to the LSC and MFSS, and are therefore supplier-specific.

The media server function provides tones and announcements that the LSC "plays out" to local and remote end users on VoIP and Video calls. In addition, the media server may provide audio and video messages, or "clips," that the LSC can "play" to local and remote users on Video calls.

NOTE: It is possible that some tones and announcements may be generated locally by the end user's EI, based on commands from the LSC to the EI that mandate the "play" of the tones or

announcements. (An example of this is the use of an LSC command that instructs an EI to "play" dial tone to a calling end user, and then to automatically halt "playing" dial tone upon receipt of the first keypad digit from that end user.) In these cases, the use of a separate media server to provide tones and announcements to end user EIs is up to the LSC vendor.

The media server stores these tones, announcements, audio clips, and video clips locally, and "plays them out" to either local or remote end users in response to corresponding requests from the CCA. As part of this "play out" process, the media server may prompt the end users for information (e.g., entry of keypad digits, or vocal answers to media server questions). In this case, the media server collects that information and responds to the CCA indicating what the collected information was, or what action the CCA should take based on the collected information.

The CCA is responsible for asking the media server to "play out" tones, announcements, audio clips, and video clips, and for ensuring that the media from the media server is directed to the correct end user. In addition, the CCA is responsible for capturing collected information from the media server, such as the series of keypad digits entered by an end user in response to a media server prompt, and using that information appropriately for call processing or feature processing.

5.3.2.11 CCA Interworking between AS-SIP and DoD CCS7

5.3.2.11.1 Purpose and Scope

This section provides basic requirements for interworking call setup and release signaling between a DoD network using the AS-SIP and a network using DoD CCS7. The interworking is performed at a node with CCA (SIP/CCS7 IWF) functionality that processes/interworks incoming CCS7 messages to outgoing AS-SIP messages, and similarly, incoming AS-SIP messages to outgoing CCS7 messages.
All requirements in this section are [Conditional: LSC, MFSS], unless otherwise indicated. This condition is illustrated in Figure 5.3.2-9, Functional Reference Model – MFSS

The requirements in this section are defined in terms of functionality at a SIP/CCS7 IWF as follows:

- UCR 2008, Section 5.3.2.11.4, Interworking for a Call Originating in an AS-SIP Network toward an ISUP Network, reviews the protocols that are interworked at the SIP/CCS7 IWF, their scope and their relationship to national standards and requirements documents.

- UCR 2008, Section 5.3.2.11.4.1.3.6.2, Generic Address, discusses the general principles of interworking between the protocols and provides an overview of the design and functionality required at the SIP/SCCS7 IWF.

- UCR 2008, Section 5.3.2.11.5, Interworking for a Call Originating in an ISUP Network toward an AS-SIP Network, provides detailed interworking requirements for a call that is initiated from an AS-SIP network toward a CCS7 network.

- UCR 2008, Section 5.3.2.11.5.1.3, Coding of SDP Media Description Lines from USI, provides detailed interworking requirements for a call that is initiated from a CCS7 network toward an AS-SIP network.

- UCR 2008, Section 5.3.2.12.9, MG Support for DoD CCS7 Trunks, defines conditions for connection of the bearer (voice) path through the MG, including the playing of tones and announcements by the SIP/CCS7 IWF toward the CCS7 network.

- UCR 2008, Section 5.3.2.11.5.3, Expiration of T_{OIW2} and Sending Early ACM, provides the requirements for the T_{OIW2} timer, which controls the sending of an early CCS7 Address Complete Message (ACM) message.

5.3.2.11.2 Background

This section applies to network nodes that meet the requirements for support of the DSN CCS7 and AS-SIP protocols as given in UCR 2008, Section 5.3.2.9.5, CCA-IWF Signaling Protocol Support Requirements. In addition, operation of MLPP functionality at the SIP/CCS7 IWF is aligned with the specification of that functionality in ANSI T1.619 and ANSI T1.619a. The functionality described in this section is aligned with that functionality specified in ANSI T1.679.
It is assumed that the SIP/CCS7 IWF does not perform number portability queries for enabling service provider portability. The SSIP/CCS7 IWF does, however, map number portability-related information elements, retaining any knowledge of a prior number portability query performed to support service provider portability. Though not a requirement, the SIP/CCS7 IWF may support SIP and CCS7 signaling to enable service portability and geographic portability.

Every call at the SIP/CCS7 IWF will have an assigned MLPP priority level and domain assigned when the call was originated or when it entered the DoD network.

5.3.2.11.3 General Considerations

[Conditional] The following rules apply to the handling of unrecognized ISUP information:

1. Assuming that no ISUP encapsulation is used, the SIP/CCS7 IWF shall act as a Type A exchange for the purposes of ISUP Compatibility procedures.

2. Only the procedures, methods, and elements of information (i.e., messages, parameters, indicators, headers) relevant to interworking are described. Therefore, the procedures, methods, and elements of information that are of local significance (i.e., only relevant to one of the signaling systems: AS-SIP or ISUP) are not interworked.

3. The SIP/CCS7 IWF combined with an ISUP exchange or an MG shall provide interworking between the bearer network connections into the AS-SIP and ISUP networks.

4. Before sending any information into the AS-SIP network, the SIP/CCS7 IWF shall consult its local trust policy (e.g., for authentication and authorization) to determine if the subsequent node to which the outgoing message is directed is trusted to receive that information. If the adjacent SIP node is not trusted to receive that information, the SIP/CCS7 IWF shall take appropriate action (e.g., omit the information, provide another value, or release the call).

5. Before accepting any information from the AS-SIP network, the SIP/CCS7 IWF shall consult its local trust policy (e.g., for authentication and authorization) to determine whether the node from which the incoming message came is trusted to originate or pass on that information. If the adjacent SIP node is not trusted to provide that information, the SIP/CCS7 IWF shall take appropriate action (e.g., ignore the information, use a default value, or release the call).

[Conditional] The SIP/CCS7 IWF shall establish a one-to-one relationship between each AS-SIP Dialog and the corresponding ISUP call/bearer control instance so that the SIP/CCS7 IWF interworks all the signaling information associated with a given call.
[Conditional] For calls where AS-SIP-to-CCS7 interworking is required, when an AS-SIP message is received for that call, the SIP/CCS7 IWF shall construct an appropriate ISUP message for that call using the information received within the SIP message's header fields and SDP body, if present.

UCR 2008, Section 5.3.2.11.4, Interworking for a Call Originating in an AS-SIP Network toward an ISUP Network, and Section 5.3.2.11.4.1.3.6.2, Generic Address, provide the interworking specifications for AS-SIP and ISUP networks.

5.3.2.11.4 Interworking for a Call Originating in an AS-SIP Network toward an ISUP Network

This section describes the interworking requirements for a call originating in an AS-SIP network toward an ISUP network.

5.3.2.11.4.1 Sending of IAM

If an AS-SIP INVITE request is received and the INVITE request cannot be associated with an existing call, the interworking procedures depend on whether the INVITE request contains an SDP Offer. UCR 2008, Section 5.3.2.11.4.1.1, INVITE Request Received without an SDP Offer, provides detailed interworking procedures for the case when an SDP Offer is not contained. UCR 2008, Section 5.3.2.11.4.1.2, INVITE Request Received with an SDP Offer, provides detailed interworking procedures for the case when an SDP Offer is contained.

[Conditional] If an AS-SIP INVITE is received, the Initial Address Message (IAM) resulting from the interworking procedures in UCR 2008, Section 5.3.2.11.4.1.1, INVITE Request Received without an SDP Offer, and Section 5.3.2.11.4.1.2, INVITE Request Received with an SDP Offer as applicable, shall be sent into the CCS7 network. The IAM parameters shall be coded as specified in UCR 2008, Section 5.3.2.11.4.1.3, IAM Parameters.

If an INVITE request is received that does not have enough digits to route to the CCS7 network, normal SIP procedures apply and the INVITE request is not interworked.

5.3.2.11.4.1.1 INVITE Request Received without an SDP Offer

[Conditional] Upon receipt of an INVITE request without an SDP Offer, if the INVITE request indicates support for reliable provisional responses, then an SDP Offer including media description shall be sent backward into the AS-SIP network within the first reliable non-failure provisional response (1xx > 100]:

1. If SIP preconditions are not in use, the IAM shall be sent into the CCS7 network upon receipt of the SDP Answer with media description.

2. If SIP preconditions are in use, the IAM shall be sent into the CCS7 network by continuing on to the procedures in UCR 2008, Section 5.3.2.11.4.1.2.2, Received INVITE Request with Preconditions.

[Conditional] Upon receipt of an INVITE request without an SDP Offer, if the INVITE request indicates reliable provisional responses are not supported, then the IAM shall be sent immediately into the CCS7 network.

5.3.2.11.4.1.2 INVITE Request Received with an SDP Offer

The following subparagraphs describe an INVITE request with an SDP Offer with or without preconditions.

5.3.2.11.4.1.2.1 Received INVITE Request without Preconditions

[Conditional] Upon receipt of an INVITE request with an SDP Offer, if SIP preconditions are not in use, then the IAM shall be sent immediately into the CCS7 network.

5.3.2.11.4.1.2.2 Received INVITE Request with Preconditions

[Conditional] Upon receipt of an INVITE request with an SDP Offer, if SIP preconditions are in use, then:

1. If outgoing CCS7 signaling supports the use of the Continuity Check procedure, the IAM shall be sent immediately into the CCS7 network. The Continuity Check Indicator in the Nature of Connection Indicators parameter shall be set to "continuity check performed on previous circuit," or "continuity check required on this circuit." The latter setting shall be used if the continuity check is to be performed on the outgoing circuit.

2. If outgoing ISUP signaling on the subsequent network does not support the use of the continuity check procedure, sending of the IAM shall be deferred until all preconditions have been met.

In all cases, UCR 2008, Section 5.3.2.11.4.1.3, IAM Parameters, gives specific details related to the population of specific parameters of the IAM. Table 5.3.2-8, IAM Parameters Mapped from an INVITE Request, lists the parameters within the IAM message that are interworked from the INVITE message and the associated sections that describe the specific interworking procedures.

5.3.2.11.4.1.3 IAM Parameters

Table 5.3.2-8 indicates the IAM parameters that interwork from INVITE.

Table 5.3.2-8. IAM Parameters Mapped from an INVITE Request

PARAMETER	SECTION
Called Party Number	5.3.2.11.4.1.3.1
Calling Party's Category	5.3.2.11.4.1.3.2
Nature of Connection Indicators	5.3.2.11.4.1.3.3
Forward Call Indicators	5.3.2.11.4.1.3.4
User Service Information	5.3.2.11.4.1.3.5
Calling Party Number	5.3.2.11.4.1.3.6.1
Generic Address	5.3.2.11.4.1.3.6.2
Hop Counter	5.3.2.11.4.1.3.7
Transit Network Selection[1]	5.3.2.11.4.1.3.8
Precedence	5.3.2.11.4.1.3.9

NOTES:
1. The Transit Network Selection parameter is not applicable in the DoD network. See UCR 2008, Section 5.3.2.11.4.1.3.8, Transit Network Selection.
- The Charge Number parameter may also be included in the IAM as a network option when AS-SIP is used.

LEGEND
AS-SIP Assured Services Session Initiation Protocol IAM Initial Address Message

5.3.2.11.4.1.3.1 Called Party Number (Required)

In the Request-URI, the incoming INVITE request will contain a sip(s): URI with:

- The user=phone parameter and
- The userinfo part of that URI is an E.164 number encoded as specified by the telephone-subscriber rule of RFC 3966.

To generate the outgoing IAM, the SIP/CCS7 IWF shall use the following principles:

1. If the routing number field is not present in the userinfo component of the Request-URI, then the geographical telephone number field contained in the userinfo component of the Request-URI shall be mapped to the Called Party Number parameter of the IAM.

2. If the routing number field is present in the userinfo component of the Request-URI, the routing number field contained in the userinfo component of the Request-URI shall be mapped to the Called Party Number parameter of the IAM. For the mapping of the geographical telephone number field contained in the userinfo component of the Request-URI, refer to Table 5.3.2-9, Mapping of INVITE Request-URI to IAM Called Party Number.

[Conditional] The SIP/CCS7 IWF shall map the information contained in the userinfo component of the Request-URI to the Called Party Number parameter of the IAM message. Table 5.3.2-9 summarizes this mapping.

Table 5.3.2-9. Mapping of INVITE Request-URI to IAM Called Party Number

INVITE REQUEST-URI	IAM CALLED PARTY NUMBER	CONDITIONS
Geographical number in userinfo	Address Signal	If the routing number field is not present in the userinfo component
Routing number in userinfo (following "rn=")	Address Signal	If the routing number field is present in the userinfo component
LEGEND IAM Initial Address Message URI Universal Resource Identifier		

5.3.2.11.4.1.3.2 Calling Party's Category (Required)

[Conditional] If the incoming INVITE request uses AS-SIP, the default coding of the Calling Party's Category field shall be 0 (binary 0000 0000," "Calling party's category unknown").

Other codes such as "ordinary subscriber," "NS/EP call," or "emergency service call" may be used in the Calling Party's Category parameter based on the interworking configuration and on additional information received in the SIP INVITE request.

5.3.2.11.4.1.3.3 Nature of Connection Indicators (Required)

[Conditional] The Nature of Connection indicators parameter in the outgoing IAM shall be set as shown in Table 5.3.2-10.

Table 5.3.2-10. Nature of Connection Indicators Parameter

BITS	NATURE OF CONNECTION INDICATORS PARAMETER
AB	Satellite indicator
DC	Continuity check indicator (ISUP)
E	Outgoing echo control device
LEGEND ISDN Integrated Services Digital Network ISUP ISDN User Part	

Other Nature of Connection Indicators shall use the values specified in ANSI T1.113.3.
The codes in Table 5.3.2-11, Coding of the Nature of Connection Indicators Parameter, shall be used as the default in the Nature of Connection Indicators parameter field.

Table 5.3.2-11. Coding of the Nature of Connection Indicators Parameter

BITS	CODES	MEANING	CONDITIONS
AB	01	One satellite circuit in the connection	If AS-SIP is not used.
DC*	00	Continuity check not required	Without pending precondition request (all profiles).
	10	Continuity check performed on a previous circuit	With pending precondition request (all profiles).
E	1	Outgoing echo control device included	Use of this value assumes that the DoD network supports echo control.
* The SIP/CCS7 IWF creates COT, as required. See UCR 2008, Section 5.3.2.13.4.2, SG and CCA Interactions.			

LEGEND
AS-SIP-T Assured Services Session Initiation Protocol for Telephones
CCA Call Connection Agent
DoD Department of Defense
IWF Interworking Function
SG Signaling Gateway
SIP Session Initiation Protocol

5.3.2.11.4.1.3.4 Forward Call Indicators (Required)

[Conditional] The Forward Call Indicators (FCI) parameter and its default values in the outgoing IAM shall be set as shown in Table 5.3.2-12.

Table 5.3.2-12. Forward Call Indicators Parameter

BITS	INDICATORS IN FCI PARAMETER	DEFAULT CODE	MEANING
D	Interworking indicator	1	Interworking encountered
F	ISUP indicator	0	ISUP not used all the way
HG	ISUP preference indicator	01	ISUP not required all the way
I	ISDN access indicator	0	Originating access non-ISDN
M	Ported number translation indicator	See Table 5.3.2-8, IAM Parameters Mapped from an INVITE Request	

LEGEND
FCI Forward Call Indicator
IAM Initial Address Message
ISDN Integrated Services Digital Network
ISUP ISDN User Part

Other Forward Call Indicators should follow ANSI T1.113. The appropriate values of the FCI are determined based on analysis of various parameters (i.e., signaling, internal states, or configurations) at the SIP/CCS7 IWF.

The value of the M bit is set depending on whether an NP Database Dip Indicator (npdi) parameter is present in the userinfo component of the Request-URI, as shown in Table 5.3.2-13, Bit M in the FCI Parameter.

Table 5.3.2-13. Bit M in the FCI Parameter

BIT	CODE	MEANING	CONDITIONS
M	0	Number not translated	LNP dip not performed (npdi not present)
M	1	Number translated	LNP dip performed (npdi present)
LEGEND LNP Local Number Portability npdi NP Database Dip Indicator NP Number Portability			

5.3.2.11.4.1.3.5 User Service Information (Required) and Higher Layer Compatibility Information Element within Access Transport Parameter (Optional)

[Conditional] If the incoming INVITE request uses AS-SIP, either:

1. The User Service Information (USI) parameter is set to 3.1 kilohertz (kHz) audio and transcoding is applied when required or

2. If SDP is received from the remote peer before the IAM is sent and if transcoding is not supported by the SIP/CCS7 IWF, then the USI parameter shall be derived from SDP, as described in Table 4/T1.679 of ANSI T1.679. Otherwise, they shall be set in accordance with local policy.

Table 4/T1.679 in ANSI T1.679 reflects the following considerations:

1. The SDP Media Description Part received by the SIP/CCS7 IWF should indicate only one media stream.

2. Only the “m=”, “b=”, and “a=” lines of the SDP Media Description Part are considered to interwork with the IAM USI and High Layer Compatibility (HLC) parameters.

3. The first subfield (i.e., <media>) of the “m=“ line will indicate one of the currently defined values: “audio”, “video”, “application”, “data”, “image”, or “control”.

5.3.2.11.4.1.3.6 Calling Line Identification Parameters

Table 5.3.2-14, Mapping of SIP From/P-Asserted-Identity/Privacy headers to ISUP CLI Parameters, summarizes the cases for mapping from the SIP INVITE header fields to the ISUP Calling Line Identification (CLI) parameters.

Table 5.3.2-14. Mapping of SIP From/P-Asserted-Identity/Privacy Headers to ISUP CLI Parameters

HAS A "P-ASSERTED -IDENTITY" HEADER FIELD CONTAINING A URI[1] WITH AN IDENTITY IN THE FORMAT "+CC"+"NDC"+ "SN" BEEN RECEIVED?	HAS A "FROM" HEADER FIELD[2] CONTAINING A URI WITH AN IDENTITY IN THE FORMAT "+CC"+"NDC"+ "SN" BEEN RECEIVED?	CALLING PARTY NUMBER PARAMETER ADDRESS SIGNALS	CALLING PARTY NUMBER PARAMETER APRI	GENERIC ADDRESS (SUPPLEMENTAL USER PROVIDES CALLING ADDRESS – NOT SCREENED) ADDRESS SIGNALS	GENERIC ADDRESS PARA-METER APRI
No	No	Network option to either include a network-provided E.164 number (see Table 5.3.2-15) or omit the Address Signals.	If a Privacy header field was received, set APRI as indicated in Table 5.3.2-16; otherwise, Network option to set APRI to "presentation restricted" or "presentation allowed."	Parameter not included	Not applicable
No	Yes	Network option to either include a network-provided E.164 number (see Table 5.3.2-15) or omit the Address Signals.	If a Privacy header field was received, set APRI as indicated in Table 5.3.2-16; otherwise, Network option to set APRI to "presentation restricted" or "presentation allowed."	Network option either to omit the parameter (if CgPN has been omitted) or derive from the "From" header (see Table 5.3.2-16)[3].	(See Table 5.3.2-17)
Yes	No	Derive from P-Asserted-Identity (see Table 5.3.2-15).	APRI = "presentation restricted" or "presentation allowed" depending on SIP Privacy header (see Table 5.3.2-16).	Not included	Not applicable

HAS A "P-ASSERTED -IDENTITY" HEADER FIELD CONTAINING A URI[1] WITH AN IDENTITY IN THE FORMAT "+CC"+"NDC"+ "SN" BEEN RECEIVED?	HAS A "FROM" HEADER FIELD[2] CONTAINING A URI WITH AN IDENTITY IN THE FORMAT "+CC"+"NDC"+ "SN" BEEN RECEIVED?	CALLING PARTY NUMBER PARAMETER ADDRESS SIGNALS	CALLING PARTY NUMBER PARAMETER APRI	GENERIC ADDRESS (SUPPLEMENTAL USER PROVIDES CALLING ADDRESS – NOT SCREENED) ADDRESS SIGNALS	GENERIC ADDRESS PARA-METER APRI
NOTES 1. It is possible that the P-Asserted-Identity header field includes both a tel: URI and a sip: URI. The handling of this case is for further study. 2. The "From" header may contain an "Anonymous URI." An Anonymous URI includes information that does not point to the calling party. RFC 3261 recommends that the display-name component contain "Anonymous." RFC 3323 recommends that the Anonymous URI itself have the value anonymous@anonymous.invalid. 3. This mapping effectively gives the equivalent of Special Arrangement (Network Option) to *all* SIP UACs with access to the SIP/CCS7 IWF.					
LEGEND APRI Address Presentation Restricted Indicator CgPN Calling Party Number IWF Interworking Function RFC Request for Comments			SIP Session Initiation Protocol UAC User Agent Client URI Universel Resource Identifier		

5.3.2.11.4.1.3.6.1 Calling Party Number

Table 5.3.2-15, Setting of the Network-Provided ISUP CgPN Parameter with a CLI, provides details for when the Calling Party Number (CgPN) is given a network-provided value.

Table 5.3.2-15. Setting of the Network-Provided ISUP CgPN Parameter with a CLI

ISUP CgPN PARAMETER FIELD	VALUE
Screening Indicator	*"network provided"*
Number Plan Indicator	ISDN/Telephony (E.164)
Address Presentation Restricted Indicator	Presentation allowed/restricted (see Table 5.3.2.-14)
Nature of Address Indicator	If next ISUP node is located in the same country, set to "national (significant) number"; otherwise, set to "International number."
Address signals	If NOA is "*national (significant) number*," no country code should be included. If NOA is "*international number*," then the country code of the network-provided number should be included.
LEGEND CgPN Calling Party Number ISDN Integrated Services Digital Network	ISUP ISDN User Part NOA Nature of Address

Table 5.3.2-16, Mapping of P-Asserted-Identity and Privacy Headers to the ISUP CgPN Parameter, provides details for CgPN mapping in other cases.

Table 5.3.2-16. Mapping of P-Asserted-Identity and Privacy Headers to the ISUP CgPN Parameter

SOURCE SIP HEADER FIELD & COMPONENT	SOURCE COMPONENT VALUE	CgPN PARAMETER FIELD	DERIVED VALUE OF PARAMETER FIELD
–	–	Numbering Plan Indicator	"*ISDN (Telephony) numbering plan (Recommendation E.164)*"
P-Asserted-Identity header field, appropriate global number portion of the URI, assumed to be in the form of "+" CC+NDC+SN[1]	CC	Nature of Address Indicator	If CC is equal to the country code of the country where the SIP/CCS7 IWF is located AND the next ISUP node is located in the same country, then set to "*national (significant) number*"; otherwise, set to "*International number*"
Privacy, priv-value component[2]	Privacy header field absent	APRI	"*presentation allowed*"
	"*none*"		"*presentation allowed*"
	"*header*"		"*presentation restricted*"
	"*user*"		"*presentation restricted*"
	"*id*"		"*presentation restricted*"
–	–	Screening Indicator	"*network provided*"
P-Asserted-Identity header field, appropriate global number portion of the URI, assumed to be in the form of "+" CC+NDC+SN[1]	CC, NDC, SN	Address Signals	If NOA is "*National (Significant) number*," then set to NDC + SN. If NOA is "*International number*," then set to CC+NDC+SN.

NOTES
1. It is possible that the P-Asserted-Identity header field includes both a tel: URI and a sip: URI. The handling of this case is for further study.
2. It is possible to receive two priv-values, one of which is "*none*," the other "*id.*" In this case, APRI shall be set to "*presentation restricted*."

LEGEND

APRI	Address Presentation Restricted Indicator	NOA	Nature of Address
CgPN	Calling Party Number	SIP	Session Initiation Protocol
ISDN	Integrated Services Digital Network	URI	Universal Resource Indicator
ISUP	ISDN User Part		
IWF	Interworking Function		

Table 5.3.2-17, Mapping of SIP From Header Field to ISUP Generic Address Parameter, provides details for mapping to a Generic Address, when this is possible.

[Conditional] The SIP/CCS7 IWF shall apply the mappings shown in Table 5.3.2-14, Table 5.3.2-15, Table 5.3.2-16, and Table 5.3.2-17 when generating the ISUP CLI parameter. If any

discrepancy occurs in privacy settings during the alignment process, the strongest privacy shall be used.

5.3.2.11.4.1.3.6.2 Generic Address

[Objective] The SIP/CCS7 IWF shall map the SIP From header field to the ISUP Generic Address parameter for supplemental CgPN, as shown in Table 5.3.2-17.

Table 5.3.2-17. Mapping of SIP From Header Field to ISUP Generic Address (Supplemental Calling Party Number Parameter)

SOURCE SIP HEADER FIELD	SOURCE COMPONENT VALUE	GENERIC ADDRESS PARAMETER FIELD	DERIVED VALUE OF PARAMETER FIELD
– component	–	Type of Address	" supplemental user provided calling address – not screened "
From, userinfo component of URI assumed to be in the form of "+"CC+NDC+SN	CC	Nature of Address Indicator	If CC is equal to the country code of the country where I-IWU is located AND the next ISUP node is located in the same country, then set to "national (significant) number"; otherwise, set to "International number"
–	–	Numbering Plan Indicator	"ISDN (Telephony) numbering plan (Recommendation E.164)"
–	–	APRI	Use same setting as for CgPN.
From, userinfo component assumed to be in the form of "+"CC+NDC+SN	CC, NDC, SN	Address Signals	If NOA is "national (significant) number" then set to NDC + SN. If NOA is "International number," then set to CC+NDC+SN.

NOTE
The "Geographical telephone number" in the userinfo component, refers to the initial telephone number (immediately following "sip:") in the Request-URI.

LEGEND

APRI	Address Presentation Restricted Indicator	NOA	Nature of Address
I-IWU	Incoming Interworking Unit	SIP	Session Initiation Protocol
ISDN	Integrated Services Digital Network	URI	Universal Resource Identifier
ISUP	ISDN User Part		
IWF	Interworking Function		

[Conditional] In the presence of the routing number and npdi fields in the userinfo component of the Request-URI, the geographical telephone number field contained in the userinfo component of the Request-URI shall be mapped to the GAP of the IAM. The coding of the GAP set by the SIP/CCS7 IWF is as specified in Table 5.3.2-18, Mapping of SIP Request-URI to ISUP Generic Address (Ported Number) Parameter.

Table 5.3.2-18. Mapping of SIP Request-URI to ISUP Generic Address (Ported Number) Parameter

SOURCE SIP HEADER FIELD & COMPONENT	SOURCE COMPONENT VALUE	GENERIC ADDRESS PARAMETER FIELD	DERIVED VALUE OF PARAMETER FIELD
–	–	Type of Address	"ported number "
– "+" CC+NDC+SN	–	Nature of Address Indicator	*"national (significant) number"*
–	–	Numbering Plan Indicator	"*ISDN (Telephony) numbering plan (Recommendation E.164)*"
Geographical number in userinfo component	"+CC""NDC""SN" from the URI	Address Signal	Set to the "NDC" + "SN"

5.3.2.11.4.1.3.7 Hop Counter

[Conditional] If the incoming INVITE request uses AS-SIP, the Hop Counter parameter shall be set to an integer equal to the value from the Max-Forwards header field value divided by a factor (F), rounded down. The value of F shall be derived by the SIP/CCS7 IWF using the following principles:

1. The Hop Counter parameter for a given message shall never increase and shall decrease by at least one with each successive visit to an SIP/CCS7 IWF, regardless of intervening interworking. The same is true for Max-Forwards in the SIP domain.

2. The initial and successively mapped values of Max-Forwards should be large enough to accommodate the maximum number of hops that might be expected of a validly routed call.

3. The factor used to map from Max-Forwards to Hop Counter for a given call will depend on call origin and call destination, and will be provisioned at the SIP/CCS7 IWF based on network topology, trust domain rules, and bilateral agreement.

5.3.2.11.4.1.3.8 Transit Network Selection

The DSN is the only transit network visible to the SIP/CCS7 IWF. Therefore, the SIP/CCS7 IWF does not expect to receive a Transit Network Selection parameter, and interworking for this parameter is not specified here.

5.3.2.11.4.1.3.9 Precedence

The modeling of the SIP/CCS7 IWF assumes that preemption of a call will occur at a node in the AS-SIP network or in the CCS7 network. The role of the SIP/CCS7 IWF is limited to interworking the signaling that indicates the relative priority of the calling party.

NOTE: If the SIP/CCS7 IWF controls the bearer path, it may perform preemption as described in UCR 2008, Section 5.3.2.11.3, General Considerations.

[Conditional] If the incoming INVITE request uses AS-SIP, the Resource-Priority Header (RPH) shall be used to derive the Precedence parameter, as shown in UCR 2008, Section 5.3.2.11.4, Interworking for a Call Originating in an AS-SIP Network toward an ISUP Network, or Section 7.1.1.2.1 of ANSI T1.619a) in the outgoing IAM as follows:

1. The Network Domain in the RPH is expected to be "dsn." However, the Network Identity in the Precedence parameter shall be coded as "0000" (corresponding to the dsn domain), independent of the received Network Domain.

2. The six-character Precedence Domain in the RPH shall be converted to binary to populate the MLPP Service Domain in the Precedence parameter.

3. If the received Network Domain in the RPH is "dsn," then the SIP/CCS7 IWF shall map the received decimal value in the r-priority field in the RPH to the Precedence Level in the Precedence parameter. Some elements of this table are specified in Table 5.3.2-19, Mapping of RPH r-priority Field to IAM Precedence Level.

Table 5.3.2-19. Mapping of RPH r-priority Field to IAM Precedence Level

RECEIVED DECIMAL VALUE IN r-priority FIELD IN RPH	CALL PRIORITY	PRECEDENCE LEVEL IN IAM
0	ROUTINE	0 1 0 0
2	PRIORITY	0 0 1 1
4	IMMEDIATE	0 0 1 0
6	FLASH	0 0 0 1
8	FLASH OVERRIDE	0 0 0 0
LEGEND IAM Initial Address Message RPH Resource Priority Header		

4. If the received Network Domain is not "dsn", the Precedence Level in the Precedence parameter shall be coded as 0100 ("routine").

[Conditional] For an incoming AS-SIP, the Precedence Level in the outgoing IAM shall be derived as follows:

[Objective] Network Domains other than "dsn" may be configured as valid domains in the SIP/CCS7 IWF. When the SIP/CCS7 IWF receives the AS-SIP message, it is an objective that the IWF check whether the Network Domain is recognized.

If the Network Domain is recognized, then the IWF shall map the Network Domain to the appropriate Network Identity in the Precedence parameter according to configuration data, and shall translate the value of the r-priority field in the RPH to the Precedence Level bits in the Precedence parameter. The six-character Precedence Domain in the RPH shall be converted to binary to populate the MLPP Service Domain in the Precedence parameter.

If the Network Domain is not recognized, then the IWF shall populate the Precedence parameter according to configuration data.

5.3.2.11.4.2 Sending of COT

[Conditional] When the preconditions on the incoming AS-SIP side have been met and any continuity tests on the outgoing CCS7 side have been completed successfully, the SIP/CCS7 IWF shall send the COT message coded as "Continuity check successful."

5.3.2.11.4.3 ACM Received

Table 5.3.2-20, Message Sent to AS-SIP Network upon Receipt of ACM from the CCS7 Network, provides a summary of how the ACM message is interworked by the SIP/CCS7 IWF to be sent into an AS-SIP network.

Table 5.3.2-20. Message Sent to AS-SIP Network upon Receipt of ACM from the CCS7 Network

MESSAGE SENT TO AS-SIP NETWORK	ACM RECEIVED FROM CCS7 NETWORK: BCI PARAMETER, CALLED PARTY'S STATUS INDICATOR
183 Session Progress	00 – No indication
180 Ringing	01 – Subscriber free

LEGEND

ACM	Address Complete Message	BCI	Backwards Call Indicator	CCS7	Common Channel Signaling No. 7
AS-SIP	Assured Services Session Initiation Protocol				

[Conditional] On receipt of the ACM, the backward SIP response sent by the SIP/CCS7 IWF depends on the value of the Called Party's Status Indicator in the Backwards Call Indicator (BCI) parameter of the ACM, as follows:

1. If the BCI (Called Party's Status Indicator) is set to "subscriber free," then a 180 Ringing SIP response shall be sent.

2. If the BCI (Called Party's Status Indicator) is set to "no indication" or any value other than "subscriber-free," and if ISUP encapsulation is not used (i.e., interworking with an AS-SIP network), the ACM shall not be interworked.

NOTE: A backward path is available as soon as the IAM is sent and the appropriate SDP is received from the calling end.

NOTE: When the ACM is not interworked, protection against indefinite prolongation of the call is provided by timers specified in ANSI T1.113.

5.3.2.11.4.4 Call Progress Message Received

[Conditional] A Call Progress Message (CPG) with an event indicator of "progress" or "in-band information" shall not be interworked with AS-SIP. A CPG with event indicator of "alerting" shall be interworked with AS-SIP, as shown in Table 5.3.2-21, Receipt of CPG at the SIP/CCS7 IWF.

Table 5.3.2-21. Receipt of CPG at the SIP/CCS7 IWF

MESSAGE SENT TO THE AS-SIP NETWORK	CPG EVENT INFORMATION PARAMETER RECEIVED EVENT INDICATOR RECEIVED	
180 Ringing	000 0001	(alerting)
Not interworked	000 0010 000 0011	(progress) or (in-band information or an appropriate pattern is now available)
LEGEND AS-SIP Assured Services Session Initiation Protocol	CPG Call Progress Message	

5.3.2.11.4.5 Answer Message Received

[Conditional] On receipt of an Answer message (ANM), the SIP/CCS7 IWF shall send a 200 OK INVITE request to the AS-SIP network. If no offer was received in the initial INVITE request, and reliable provisional responses were not supported, the 200 OK INVITE request shall include an SDP Offer consistent with the USI used on the CCS7 side.

5.3.2.11.4.6 Confusion Message Received

[Conditional] A received Confusion message shall be discarded by the SIP/CCS7 IWF.

5.3.2.11.4.7 Circuit (CIC) Query Response Message Received

[Conditional] After sending a Circuit (CIC) Query Message, the SIP/CCS7 IWF expects to receive a Circuit (CIC) Query Response Message. The SIP/CCS7 IWF shall process the Circuit (CIC) Query Response Message as described in ANSI T1.113.4, clause 2.8.2A. The ISUP procedures may result in the release of a call.

5.3.2.11.4.8 Pass Along Message Received

On receipt of a Pass Along Message (PAM), the actions taken toward the CCS7 network are based on the contents of the PAM.

[Conditional] A received PAM shall be discarded by the SIP/CCS7 IWF.

5.3.2.11.4.9 Through Connection

Through connection of bearer path is applicable only to an SIP/CCS7 IWF that controls the bearer path.

[Conditional] Through connection at the SIP/CCS7 IWF shall follow the ANSI T1.113 through connection procedures for the originating exchange.

5.3.2.11.4.10 Suspend Message, Network Initiated Received

[Conditional] If the SIP/CCS7 IWF is the controlling exchange for the Suspend procedure, the actions taken toward the CCS7 network upon receipt of the Suspend message (SUS) shall be as described in ANSI T1.113, Clause 2.5.1.3. The SUS is not interworked and no action is taken toward the AS-SIP network.

5.3.2.11.4.11 Resume Message, Network Initiated Received

[Conditional] If the SIP/CCS7 IWF is the controlling exchange for the Resume procedure, the actions taken toward the CCS7 network upon receipt of the Resume message (RES) shall be as described in ANSI T1.113, Clause 2.4.2c. The RES is not interworked and no action is taken toward the AS-SIP network.

5.3.2.11.4.12 Release Procedures

5.3.2.11.4.12.1 Receipt of BYE or CANCEL

[Conditional] On receipt of an AS-SIP BYE or CANCEL message, the SIP/CCS7 IWF shall send an ISUP Release message (REL).

[Conditional] If AS-SIP is being used, then if the Reason header field is included in the BYE or CANCEL message, then the cause value may be mapped to the ISUP cause value field in the ISUP REL message, as shown in Table 5.3.2-22, Mapping of AS-SIP Reason Header Fields into Cause Indicators Parameter, depending on local policy. Table 5.3.2-23, Coding of Cause Value If Not Taken from the Reason Header Field, shows the coding of the cause value in the REL message if it is not available from the Reason header field. In all cases, the Location field shall be set to "network beyond interworking point."

Table 5.3.2-22. Mapping of AS-SIP Reason Header Fields into Cause Indicators Parameter

COMPONENT OF AS-SIP REASON HEADER FIELD	COMPONENT VALUE	ISUP PARAMETER/FIELD	VALUE
protocol	"Q.850"	Coding standard	ITU-T Standard
protocol	"ANSI"	Coding standard	ANSI Standard
protocol-cause	"cause = XX" (Note)	Cause Value	"XX" (Note)
		Location	Network beyond interworking point
NOTE: "XX" is the cause value as defined in ITU-T Recommendation Q.850 or ANSI T1.113, depending on the value of the coding standard.			

Table 5.3.2-23. Coding of Cause Value If Not Taken from the Reason Header Field

AS-SIP MESSAGE	REL CAUSE INDICATORS PARAMETER
BYE	Cause Value No. 16 (normal clearing)
CANCEL	Cause Value No. 31 (normal unspecified)
LEGEND AS-SIP Assured Services Session Initiation Protocol	REL Release Message

5.3.2.11.4.12.2 REL Message Received

[Conditional] On receipt of an ISUP REL message, if the SIP/CCS7 IWF is capable of bearer control, it immediately requests the disconnection of the internal bearer path. When the ISUP circuit is available for reselection, an ISUP RLC is returned to the CCS7 network.

[Conditional] Depending on local policy, containing the received (ITU-T Recommendation Q.850 or ANSI T1.113) cause value of the REL message may be added to the AS-SIP final response or BYE message that is sent. The mapping of the Cause Indicators parameter to the Reason header field shall be as shown in Table 5.3.2-24, Mapping of Cause Indicators Parameter into AS-SIP Reason Header Fields.

Table 5.3.2-24. Mapping of Cause Indicators Parameter into AS-SIP Reason Header Fields

CAUSE INDICATIONS PARAMETER FIELD	VALUE OF PARAMETER FIELD	COMPONENT OF AS-SIP REASON HEADER FIELD	COMPONENT VALUE
Coding standard	ITU-T Standard	protocol	"Q.850"
Coding standard	ANSI Standard	protocol	"ANSI"
Cause Value	"XX"[1]	protocol-cause	"cause= XX"[1]
		reason-text	Should be filled with the definition text as given in ITU-T Q.850 or ANSI T1.113[2]

NOTES
1. "XX" is the cause value as defined in ITU-T Recommendation Q.850 or ANSI T1.113.
2. Because the Cause Indications parameter does not include the definition text as defined in ITU-T Recommendation Q.850 or ANSI T1.113, this is based on provisioning in the SIP/CCS7 IWF.

LEGEND
ANSI American National Standards Institute
AS-SIP Assured Services Session Initiation Protocol
ITU-T Internal Telecommunication Union – Telecommunications

[Conditional] On receipt of a REL message before receiving an ANM, the SIP/CCS7 IWF shall send the appropriate SIP status-code in an AS-SIP final response, as shown in Table 5.3.2-25, Receipt of the REL Message. The ISUP cause codes not appearing in the table shall have the same mapping as the appropriate ANSI T1.113 class defaults.

Table 5.3.2-25. Receipt of the REL Message

AS-SIP MESSAGE	REL CAUSE INDICATORS PARAMETER
Cause Values with Coding Standard Field Set to 00 (ITU-T Standard)[1]	
404 Not Found	Cause Value No. 1 (unallocated (unassigned) number)
500 Server Internal Error	Cause Value No. 2 (no route to network)
500 Server Internal Error	Cause Value No. 3 (no route to destination)
500 Server Internal Error	Cause Value No. 4 (send special information tone)
No Mapping (No procedure specified for this cause value in U.S. networks)	Cause Value No. 5 (misdialed trunk prefix) (No procedures specified for this cause value in U.S. networks.)
See UCR 2008, Section 5.3.4, AS-SIP Generic System Specification, which references RFCs 4411 & 3326	Cause Value No. 8 (Preemption-circuit is not to be reused.)

AS-SIP MESSAGE	REL CAUSE INDICATORS PARAMETER
See UCR 2008, Section 5.3.4, AS-SIP Generic System Specification, which references RFCs 4411 &3326	Cause Value No. 9 (Preemption-circuit is reserved for reuse.)
486 Busy Here	Cause Value No. 17 (user busy)
480 Temporarily Unavailable	Cause Value No. 18 (no user responding)
480 Temporarily Unavailable	Cause Value No. 19 (no answer from the user)
480 Temporarily Unavailable	Cause Value No. 20 (subscriber absent)
480 Temporarily Unavailable	Cause Value No. 21 (call rejected)
410 Gone	Cause Value No. 22 (number changed)
No Mapping (due to redirection procedures)	Cause Value No. 23 (redirect to a new destination)
502 Bad Gateway	Cause Value No. 27 (destination out of order)
484 Address Incomplete	Cause Value No. 28 (invalid number format (address incomplete))
500 Server Internal Error	Cause Value No. 29 (facility rejected)
480 Temporarily Unavailable	Cause Value No. 31 (normal unspecified) (Class default)
480 Temporarily Unavailable	Cause Value in the Class 010 (resource unavailable, Cause Value No. 34)
500 Server Internal Error	Cause Value in the Class 010 (resource unavailable, Cause Value Nos. 38-47) (47 is class default)
500 Server Internal Error	Cause Value No. 50 (requested facility not subscribed)
500 Server Internal Error	Cause Value No. 57 (bearer capability not authorized)
500 Server Internal Error	Cause Value No. 58 (bearer capability not presently available)
500 Server Internal Error	Cause Value No. 63 (service option not available, unspecified) (Class default)
500 Server Internal Error	Cause Value in the Class 100 (service or option not implemented Cause Value Nos. 65-79) (79 is class default)
500 Server Internal Error	Cause Value No. 88 (incompatible destination)
404 Not Found	Cause Value No. 91 (invalid transit network selection)
500 Server Internal Error	Cause Value No. 95 (invalid message) (Class default)
500 Server Internal Error	Cause Value No. 97 (message type non-existent or not implemented)
500 Server Internal Error	Cause Value No. 99 (information element/parameter non-existent or not implemented)
480 Temporarily Unavailable	Cause Value No. 102 (recovery on timer expiry)
500 Server Internal Error	Cause Value No. 103 (parameter non-existent or not implemented, passed on)
500 Server Internal Error	Cause Value No. 110 (message with unrecognized parameter, discarded)
500 Server Internal Error	Cause Value No. 111 (protocol error, unspecified) (Class default)
480 Temporarily Unavailable	Cause Value No. 127 (interworking unspecified) (Class default)
Cause Values with Coding Standard Field Set to 01 (ANSI Standard) [1]	
404 Not Found	Cause Value No. 23 (unallocated destination number)
500 Server Internal Error	Cause Value No. 24 (unknown business group)

AS-SIP MESSAGE	REL CAUSE INDICATORS PARAMETER
500 Server Internal Error	Cause Value No. 25 (exchange routing error)
404 Not Found[1]	Cause Value No. 26 (misrouted call to a ported number)
No Mapping (No procedure specified for this cause value in U.S. networks)	Cause Value No. 27 (NP QoR – number not found) (No procedures are specified for this cause value in U.S. networks.)
Not Applicable	Cause Value in the Class 010 (resource unavailable, Cause Value Nos. 45 & 46) NOTE: Cause Value No. 45 is superseded by Cause Values 8 and 9 in codeset 0; Cause Value No. 46 is in codeset.
500 Server Internal Error	Cause Value in the Class 011 (service or option not available, Cause Value Nos. 51 & 54)

NOTE
1. The Coding Standard field in the Cause Indicators parameter in the received REL message may be set to either "ITU-T Standard" or "ANSI Standard." This table is separated into two sections pertaining to each of these values of the Coding Standard field.

LEGEND

ANSI	American National Standards Institute	ITU-T	International Telecommunication Union – Telecommunications	QoR	Query on Release
				REL	Release Message
AS-SIP	Assured Services Session Initiation Protocol	NP	Number Portability	RFC	Request for Comment

[Conditional] On receipt of a REL message after receiving an ANM, the SIP/CCS7 IWF shall send a BYE message.

5.3.2.11.4.12.3 Autonomous REL at SIP/CCS7 IWF

Table 5.3.2-26, Autonomous REL Message at SIP/CCS7 IWF, shows the trigger events at the SIP/CCS7 IWF and the release initiated by the SIP/CCS7 IWF when the call is traversing from AS-SIP to ISUP.

[Conditional] If an automatic repeat attempt initiated by the SIP/CCS7 IWF is not successful (because the call is not routable), the SIP/CCS7 IWF shall send a 480 Temporarily Unavailable response to the AS-SIP side. No actions on the ISUP side are required.

[Conditional] If, after answer, ISUP procedures result in an autonomous REL message from the SIP/CCS7 IWF, then a BYE message shall be sent on the AS-SIP side.

[Conditional] If the SIP/CCS7 IWF receives unrecognized backward ISUP signaling information and determines that the call needs to be released based on the coding, the SIP/CCS7 IWF shall send a 500 Internal Server Error response on the AS-SIP side. Depending on local policy a Reason header field containing the (ITU-T Q.850 or ANSI) cause value of the REL message sent by the SIP/CCS7 IWF may be added to the AS-SIP message (BYE or final response) sent by the AS-SIP side of the SIP/CCS7 IWF.

Table 5.3.2-26. Autonomous Release at SIP/CCS7 IWF

AS-SIP SIDE	TRIGGER EVENT	REL ON THE CCS7 SIDE CAUSE PARAMETER
484 Address Incomplete	Determination that insufficient digits received	Not applicable
480 Temporarily Unavailable	Congestion at the SIP/CCS7 IWF	Not applicable
BYE	ISUP procedures result in release after answer	According to ISUP procedures
500 Server Internal Error	Call release due to the ISUP compatibility procedure (Note 1)	According to ISUP procedures
484 Address Incomplete	Call release due to expiry of T_7 within the ISUP procedures	According to ISUP procedures
480 Temporarily Unavailable	Other ISUP procedures result in release before answer	According to ISUP procedures

LEGEND

AS-SIP	Assured Services Session Initiation Protocol	ISDN	Integrated Services Digital Network	REL	Release Message
		ISUP	ISDN User Part	SIP	Session Initiation Protocol
CCS7	Common Channel Signaling No. 7	IWF	Interworking Function	SS7	Signaling System No. 7

5.3.2.11.4.12.4 Reset Circuit, Circuit Group Reset, or Circuit Group Blocking Message Received

Table 5.3.2-27, Receipt of RSC, GRS, or CGB Messages, shows the AS-SIP message sent by the SIP/CCS7 IWF upon receipt of an ISUP Reset Circuit message (RSC), Circuit Group Reset message (GRS), or Circuit Group Blocking message (CGB) with the Circuit Group Supervision Message Type Indicator coded as "hardware failure oriented," when at least one backward ISUP message relating to the call has already been received. The SIP/CCS7 IWF sends BYE message if it has already received an ACK message for the 200 OK INVITE request it had sent. If it has sent a 200 OK INVITE request but has not received an ACK message for the 200 OK INVITE request, then the SIP/CCS7 IWF shall wait until it receives the ACK message for the 200 OK INVITE request before sending the BYE message. Otherwise, it sends a 500 Server Internal Error response. On receipt of a GRS or CGB, one AS-SIP message is sent for each call association. Therefore, multiple AS-SIP messages may be sent on receipt of a single GRS or CGB message.

[Conditional] The SIP/CCS7 IWF shall process received a CCS7 RSC, GRS, or CGB as shown in Table 5.3.2-27, Receipt of RSC, GRS, or CGB Messages.

Table 5.3.2-27. Receipt of RSC, GRS, or CGB Messages

MESSAGE SENT TO AS-SIP NETWORK	MESSAGE RECEIVED FROM ISUP
500 Server Internal Error or BYE	RSC
500 Server Internal Error or BYE	GRS
500 Server Internal Error or BYE	CGB with the Circuit Group Supervision Message Type indicator coded "*hardware failure oriented*"

LEGEND
CGB Circuit Group Blocking Message
GRS Circuit Group Reset Message
ISDN Integrated Services Digital Network
ISUP ISDN User Part
RSC Reset Circuit Message

5.3.2.11.5 Interworking for a Call Originating in an ISUP Network toward an AS-SIP Network

This section describes the interworking requirements for a call originating in an ISUP network toward an AS-SIP network.

5.3.2.11.5.1 Sending of INVITE

[Conditional] After performing the normal ISUP handling for a received IAM and choosing to route the call to the AS-SIP network, the procedures at the SIP/CCS7 IWF will depend on whether preconditions are used in the AS-SIP network:

1. Procedures to send an INVITE request without precondition upon receipt of an ISUP IAM are given in UCR 2008, Section 5.3.2.11.5.1.1, Sending INVITE without Precondition for a Received ISUP IAM.

2. Procedures to send an INVITE request with precondition upon receipt of an ISUP IAM are given in UCR 2008, Section 5.3.2.11.5.1.2, Sending INVITE with Precondition for a Received ISUP IAM.

3. Coding of the IAM received and the INVITE request sent by the SIP/CCS7 IWF are specified in UCR 2008, Sections 5.3.2.11.5.1.3 through 5.3.2.11.5.1.7.

4. Timer (T_{OIW2}) is started when the INVITE request is sent.

5. If timer (T_{OIW2}) expires, an early ACM is sent to the CCS7 network. See UCR 2008, Section 5.3.2.11.5.3, Expiration of T_{OIW2} and Sending Early ACM.

5.3.2.11.5.1.1 Sending INVITE without Precondition for a Received ISUP IAM

Normal outgoing AS-SIP procedures for when an INVITE request is sent apply with the following clarifications and exceptions:

1. **[Conditional]** An INVITE request shall be sent immediately when an ISUP IAM is received and the Continuity Check Indicator in the Nature of Connection Indicators parameter in the IAM is set to indicate "continuity check not required."

2. **[Conditional]** Sending of the INVITE request shall be delayed if the Continuity Check Indicator in the Nature of Connection Indicators parameter in the IAM is set to indicate either "continuity check required on this circuit" or "continuity check performed on previous circuit." The INVITE request shall be sent on receipt of the Continuity message with the Continuity Indicators parameter set to "continuity check successful." The INVITE request shall not be sent if the Continuity message is received with the Continuity Indicators parameter set to "continuity check failed" or the ISUP timer T8 expires.

5.3.2.11.5.1.2 Sending INVITE with Precondition for a Received ISUP IAM

[Conditional] An INVITE request with precondition shall be sent on receipt of an ISUP IAM. Incoming ISUP procedures apply, with the following clarifications and exceptions as to when a confirmation of the precondition being met is sent:

NOTE: Configured procedures may delay the INVITE request until local resources have been reserved on the outgoing bearer path.

1. **[Conditional]** The SIP/CCS7 IWF initiates the precondition signaling procedure using the SDP Offer in the INVITE request. The precondition signaling is concluded upon sending (within an SDP Offer-Answer exchange) the confirmation of a precondition being met. The SDP Offer or SDP Answer carrying the confirmation of a precondition being met shall be sent when:

    a. If the Continuity Check Indicator in the Nature of Connection Indicators parameter in the incoming IAM is set to indicate either "continuity check required on this circuit" or "continuity check performed on previous circuit," the Continuity message with the Continuity Indicators parameter set to "continuity check successful" shall be received.

    b. The requested preconditions are met in the SIP network.

NOTE: As a network option, the signaling of a precondition being met may only occur within the SDP Offer in an UPDATE message.

2. **[Conditional]** A CANCEL or BYE message shall be sent if the Continuity message is received with the Continuity Indicators parameter set to "continuity check failed" or if ISUP timer T8 expires.

3. **[Conditional]** The REL message with Cause Value No. 47 (resource unavailable, unspecified) shall be sent by the SIP/CCS7 IWF to the ISUP network, and a CANCEL or BYE message shall be sent to the AS-SIP network if internal resource reservation was unsuccessful.

Table 5.3.2-28, Mapping of IAM Information to an INVITE Message, provides a summary of how the header fields within the outgoing INVITE message are populated. When the coding of the received Calling Party Category (CPC) is "NS/EP call" or "emergency service call," additional information may be sent in the INVITE request.

Table 5.3.2-28. Mapping of IAM Information to an INVITE Message

IAM	INVITE	REFERENCE
Called Party Number	Request-URI	5.3.2.11.5.1.4
	To	5.3.2.11.5.1.4
Calling Party Number	P-Asserted-Identity	5.3.2.11.5.1.5
	Privacy	5.3.2.11.5.1.5
	From	5.3.2.11.5.1.5
GAP (Supplemental User Provided Calling Address)	From	5.3.2.11.5.1.5
GAP (Ported Number)	Request-URI	5.3.2.11.5.1.4
FCI (ported Number Translation Indicator)	Request-URI	5.3.2.11.5.1.4
Hop Counter	Max-Forwards	5.3.2.11.5.1.6
USI	Message Body (application/SDP)	5.3.2.11.5.1.3
Precedence	Resource Priority Header	5.3.2.11.5.1.7

LEGEND
FCI Forward Call Indicator; SDP Session Description Protocol; USI User Service Information
IAM Initial Address Message; URI Universal Resource Indicator

5.3.2.11.5.1.3 Coding of SDP Media Description Lines from USI

[Conditional] The USI parameter (if present) in the IAM indicates user-requested bearer service characteristics. The USI codes shall be mapped to the AS-SIP SDP information. ANSI T1.113.3

provides an exhaustive list of the available codes in the USI. In principle, any combination of those codes can be mapped into any SDP information as long as transcoding is available.

[Conditional] The SIP/CCS7 IWF, as a network option, may also encode the SDP for the Adaptive Multi-Rate (AMR) codec, which is specified in RFC 3267.

[Conditional] If ITU-T Recommendation G.711 encoding may be used, then the SIP/CCS7 IWF shall send an SDP Offer with both "G.711 μ-law" and "G.711 A-law" included in the media description, and "G.711 μ-law" shall take precedence over "G.711 A-law."

[Conditional] If transcoding is not available at the SIP/CCS7 IWF, the SIP/CCS7 IWF shall use the mapping relations in Table 5.3.2-29, Coding of SDP Media Description Lines from USI: ISUP to AS-SIP, from USI codes to SDP media description lines.

Table 5.3.2-29. Coding of SDP Media Description Lines from USI: ISUP to AS-SIP

USI PARA-METER	USI PARA-METER	USI PARA-METER	USI PARA-METER	HLC IE IN ATP	M= LINE			B= LINE	A= LINE
Information Transfer Rate	Rate Multi-plier	Informa-tion Transport Capability	User Informa-tion Layer 1 Protocol Indicator	High Layer Characteris-tics Identifica-tion	<media>	<transport>	<fmt-list>	<modifier>: <bandwidth-value>	rtpmap:<dynamic -PT> <encoding name>/<clock rate>[/encoding parameters>
speech		Speech	G.711 μ-law	"Ignore"	audio	RTP/AVP	0 (& possibly 8)[1]	AS:64	rtpmap:0 PCMU/8000(& possibly rtpmap:8 PCMA/8000)[1]
speech		Speech	G.711 μ-law	"Ignore"	audio	RTP/AVP	Dynamic PT (& possibly a 2nd Dy-namic PT)	AS:64	rtpmap:<dynamic -PT> PCMU/8000(and possibly rtpmap:8 PCMA/8000)[1]
3.1 kHz audio		3.1 kHz audio	G.711 μ-law	Telephony or "HLC absent"	audio	RTP/AVP	0	AS:64	rtpmap:0 PCMU/8000
3.1 kHz audio		3.1 kHz audio		Facsimile Group 2/3	image	udptl	t38	AS:64	Based on T.38
3.1 kHz audio		3.1 kHz audio		Facsimile Group 2/3	image	tcptl	t38	AS:64	Based on T.38
64 kbps unrestricted		Unrestrict-ed digital informa-tion with tone/ann	N/A	"Ignore"	audio	RTP/AVP	9	AS:64	rtpmap:9 G.722/8000
64 kbps unrestricted		Unrestrict-ed dig. Informa-tion	N/A	"Ignore"	audio	RTP/AVP	Dynamic PT	AS:64	rtpmap:<dynamic -PT> CLEARMODE/8 000[2]
2 x 64 kbps unrestricted	2	Unrestrict-ed dig. Informa-tion	N/A	"Ignore"	[3]	[3]	[3]	[3]	[3]

USI PARA-METER	USI PARA-METER	USI PARA-METER	USI PARA-METER	HLC IE IN ATP	M= LINE			B= LINE	A= LINE
384 kbps unrestricted		Unrestrict-ed dig. Informa-tion	N/A	"Ignore"	[3]	[3]	[3]	[3]	[3]

NOTES:
1. Both PCMA and PCMU required under the conditions stated in UCR 2008, Section 5.3.2.5.1.3.
2. CLEARMODE has not yet been standardized.
3. No standard is defined at this time.

5.3.2.11.5.1.4 Request-URI and To Header Field

The Called Party Number parameter of the IAM contains the forward address information to derive the userinfo component of the INVITE Request-URI. The SIP/CCS7 IWF follows existing ISUP procedures to select the outgoing route.

[Conditional] If a new Called Party Number parameter is derived for the outgoing route, then the newly derived Called Party Number parameter shall be mapped into the userinfo component of the INVITE Request-URI.

For a basic call, the address information contained in the Called Party Number parameter is considered as the identification of the called party. Therefore, this information is used to derive the addr-spec component of the To header field.

If the Request-URI or the To header field contains a sip: URI, it shall include the "user=phone" URI parameter.

It is assumed that the SIP/CCS7 IWF does not perform number portability queries. It does, however, map number portability-related information elements.

[Conditional] When the Called Party Number parameter is included in the received IAM (and the GAP for the ported number is not present), the mapping of this parameter and of the FCI Ported Number Indicator to the Request-URI shall be as shown in Table 5.3.2-30, Mapping of Called Party Number and FCI Ported Number Translation Indicator.

Table 5.3.2-30. Mapping of Called Party Number and FCI Ported Number Translation Indicator

ISUP PARAMETER/ FIELD	VALUE	SIP COMPONENT	VALUE
Called Party Number	Digits	Request-URI	userinfo
Address Signal	Either NCD + SN (national number) or CC + NCD + SN (international number)	userinfo's geographical number	If national number, prepend +CC to Address signal digits, as in: "+CC" "NCD" "SN". If international number, prepend "+".
FCI	Ported Number Translation Indicator	userinfo's npdi parameter	If Ported Number Translation Indicator is equal to "1," append ";npdi" to userinfo.
LEGEND FCI Forward Call Indicator npdi NP Database Dip Indicator SIP Session Initiation Protocol NP Number Portability			

[Conditional] When the Generic Address (ported number) and Called Party Number parameters are both included in the received IAM, the mapping of these parameters and of the FCI ported number indicator to the Request-URI shall be as shown in Table 5.3.2-31, Mapping of Generic Address (Ported) and Called Party Number (When Both are Included), and FCI Ported Number to Request-URI.

NOTE: The ISUP Transit Network Selection parameter is not expected to be received at the SIP/CCS7 IWF. Therefore, this document does not specify interworking of the parameter.

Table 5.3.2-31. Mapping of Generic Address (Ported) and Called Party Number (When Both are Included), and FCI Ported Number to Request-URI

ISUP PARAMETER/ FIELD	VALUE	SIP COMPONENT	VALUE
Generic Address Type of Number	"ported number"	Request-URI	userinfo
Address Signal	Since NOA is "*National (Significant) number,"* then the format of the address signals is NCD + SN	userinfo's geographical number	Add +CC to Address Signal digits, as in: "+CC" "NCD" "SN"
FCI	Ported Number Translation Indicator	userinfo's npdi parameter	";npdi" is added to userinfo
Called Party Number Address Signal	Since NOA is "*National (Significant) number,"* then the format of the address signals is NCD + SN	userinfo's routing number	";rn=routing number" is added to userinfo, with +CC being prefixed to Address Signal's NCD+SN

LEGEND

FCI	Forward Call Indicator	ISUP	ISDN User Part	npdi	NP Database Dip Indicator
ISDN	Integrated Services Digital Network	NOA	Nature of Address	SIP	Session Initiation Protocol
		NP	Number Portability		

5.3.2.11.5.1.5 P-Asserted-Identity, From, and Privacy Header Fields

[Conditional] The SIP/CCS7 IWF shall follow the mapping in Table 5.3.2-32, ISUP CLI Parameters to AS-SIP Header Fields, when mapping from the ISUP Calling Party Number and Generic Address parameters to the AS-SIP P-Asserted-Identity, From, and Privacy header fields in the INVITE message.

Table 5.3.2-32. ISUP CLI Parameters to AS-SIP Header Fields

Has a CgPN Parameter with Complete E.164 Number, with Screening Indicator = UPPS or NP[1], and with APRI = "Presentation Allowed" or "Presentation Restricted" Been Received?	Has a Generic Address (Supplemental User Provide Calling Address – Not Screened) with a Complete E.164 Number, and with APRI = "Presentation Allowed" Been Received?	P-Asserted-Identity Header Field	From Header Field: display-name (Optional) and addr-spec	Privacy Header Field
No	No	Header field not included	Unavailable@Hostportion	Header field not included
No[2]	Yes	Header field not included	display-name derived from Generic Address (supplemental calling address) if possible. addr-spec derived from Generic Address (supplemental calling address) address signals or uses network-provided value	Header field not included
Yes[1]	No	Derived from CgPN parameter address signals (see Table 5.3.2-34).	If APRI = "allowed," display-name derived from CgPN if possible. If APRI = "restricted," display-name is "Anonymous." If APRI = "allowed," addr-spec is derived from CgPN parameter address signals (see Table 5.3.2-35) or uses network-provided value. If APRI = "restricted," addr-spec is set to the "Anonymous URI."[4]	If CgPN parameter APRI = "restricted," then priv-value =; "id." For other APRI settings, Privacy header is not included or if included, "id" is not included (see Table 5.3.2-36).

Has a CgPN Parameter with Complete E.164 Number, with Screening Indicator = UPPS or NP[1], and with APRI = "Presentation Allowed" or "Presentation Restricted" Been Received?	Has a Generic Address (Supplemental User Provide Calling Address – Not Screened) with a Complete E.164 Number, and with APRI = "Presentation Allowed" Been Received?	P-Asserted-Identity Header Field	From Header Field: display-name (Optional) and addr-spec	Privacy Header Field
Yes[1]	No	Derived from CgPN parameter address signals (see Table 5.3.2-34).	display-name may be derived from Generic Address[3] addr-spec is derived from Generic Address address signals (see Table 5.3.2-33).	If CgPN parameter APRI = "restricted," then priv-value =; "id". For other APRI settings, Privacy header is not included or if included, "id" is not included (see Table 5.3.2-36).

NOTES
1. A network-provided CLI in the CgPN parameter may occur on a call from an analog access line. Therefore, in order to allow the "display" of this network-provided CLI, it must be mapped into the AS-SIP From header. It is also considered suitable to map into the P-Asserted-Identity header.
2. This combination of CgPN and supplemental calling address is an error case, but is shown here to ensure consistent mapping across different implementations.
3. It may be possible to derive the Display name from the Generic Address parameter.
4. The From header may contain an "Anonymous URI," which would not point to the calling party. RFC 3261 recommends that the display-name component contain "Anonymous." Anonymous URI itself has the value "anonymous@anonymous.invalid."

LEGEND

APRI	Address Presentation Restricted Indicator	CgPN	Calling Party Number	RFC	Request for Comment
		CLI	Calling Line Identification	UPPS	
AS-SIP	Assured Services Session Initiation Protocol	NP	Number Portability	URI	Universal Resource Identifier

[Objective] The SIP/CCS7 IWF shall follow the detailed mapping in Table 5.3.2-33, Mapping of GAP (Supplemental User Provided Calling Address) to AS-SIP From Headers Fields, when mapping from the ISUP Generic Address parameter to the AS-SIP From header field.

Table 5.3.2-33. Mapping of GAP (Supplemental User Provided Calling Address) to AS-SIP From Header Fields

ISUP PARAMETER/ FIELD	VALUE	AS-SIP COMPONENT	VALUE
Generic Address Number Qualifier Indicator	"supplemental user provided calling address – not screened"	From header field	display-name (optional) and addr-spec
Nature of Address Indicator	"national (significant) number"	addr-spec	Add CC (of the country where the SIP/CCS7 IWF is located) to GAP address signals then map to AS-SIP URI.
	"International number"		Map complete GAP address signals to AS-SIP URI
Address Signal	If NOA is "National (Significant) number," then the format of the address signal is NDC + SN. If NOA is "International number," then the format of the address signal is CC + NDC + SN.	display-name	display-name shall be mapped from address signal, if possible, and if network policy allows it.
		addr-spec	"+CC" "NDC" "SN" mapped to the appropriate global number portion of URI scheme used

LEGEND					
AS-SIP	Assured Services Session Initiation Protocol	ISUP	ISDN User Part	SIP	Session Initiation Protocol
ISDN	Integrated Services Digital Network	IWF	Interworking Function	URI	Universal Resource Identifier
		NOA	Nature of Address		

[Conditional] The SIP/CCS7 IWF shall follow the detailed mapping in Table 5.3.2-34, Mapping of Calling Party Number Parameter to AS-SIP P-Asserted-Identity Header Fields, when mapping from the ISUP Calling Party Number parameter to the AS-SIP P-Asserted-Identity.

Table 5.3.2-34. Mapping of CgPN Parameter to AS-SIP P-Asserted-Identity Header Fields

ISUP PARAMETER/ FIELD	VALUE	SIP COMPONENT	VALUE
Calling Party Number		P-Asserted-Identity header field	display-name (optional) and addr-spec
Nature of Address Indicator	"national (significant) number"	addr-spec	Add CC (of the country where the SIP/CCS7 IWF is located) to CgPN address signals, then map to URI.
	"international number"		Map complete CgPN address signals to URI.
Address Signal	If NOA is "national (significant) number," then the format of the address signals is NDC + SN. If NOA is "international number," then the format of the address signals is CC + NDC + SN.	display-name	display-name shall be mapped from address signal, if possible, and if network policy allows it.
		addr-spec	"+CC" "NDC" "SN" mapped to the appropriate global number portion of URI scheme used

LEGEND
CgPN Calling Party Number
NOA Nature of Address
SIP Session Initiation Protocol
SS7 Signaling System No. 7
URI Universal Resource Identifier

[Conditional] The SIP/CCS7 IWF shall follow the detailed mapping in Table 5.3.2-35, Mapping of ISUP CgPN Parameter to AS-SIP from Header Fields, when mapping from the ISUP CgPN parameter to the AS-SIP From header field.

Table 5.3.2-35. Mapping of ISUP CgPN Parameter to AS-SIP From Header Fields

ISUP PARAMETER/ FIELD	VALUE	SIP COMPONENT	VALUE
Calling Party Number		From header field	display-name (optional) and addr-spec
Nature of Address Indicator	"national (significant) number"	addr-spec	Add CC (of the country where the SIP/CCS7 IWF is located) to CgPN address signals, then map to user portion of URI scheme used.
	"international number"		Map complete CgPN address signals to map to user portion of URI scheme used.
Address Signal	If NOA is "national (significant) number," then the format of the address signals is NDC + SN. If NOA is "international number," then the format of the address signals is CC + NDC + SN.	display-name	display-name shall be mapped from Address Signal, if possible and network policy allows it.
		addr-spec	"+CC" "NDC" "SN" mapped to user portion of URI scheme used

LEGEND					
CgPN	Calling Party Number	SIP	Session Initiation Protocol	URI	Universal Resource Identifier
NOA	Nature of Address	SS7	Signaling System No. 7		

[Conditional] The SIP/CCS7 IWF shall follow the detailed mapping in Table 5.3.2-36, Mapping of ISUP APRIs into AS-SIP Privacy Header Fields, when mapping from the ISUP Address Presentation Restricted Indicator (APRI) subfield of the Calling Party Number parameter to the AS-SIP Privacy header field.

[Conditional] If the From or the P-Asserted-Identity header field is sent with a sip: URI, it shall include the "user=phone" URI parameter.

5.3.2.11.5.1.6 Hop Counter (Max-Forwards)

[Conditional] If the outgoing INVITE message uses AS-SIP, then the Max-Forwards header field value from the Hop Counter value shall be set to an integer equal to the received Hop Counter value multiplied by a factor (F) rounded down. The value of F should be derived by the SIP/CCS7 IWF using the following principles:

Table 5.3.2-36. Mapping of ISUP APRIs into AS-SIP Privacy Header Fields

ISUP PARAMETER/ FIELD	VALUE	SIP COMPONENT	VALUE
Calling Party Number		Privacy header field	priv-value
APRI	"presentation restricted"	priv-value	"id," but only included if the P-Asserted-Identity header is included in the AS-SIP INVITE request
	"presentation allowed"	priv-value	Omit Privacy header or Privacy header without "id" if other privacy service is needed.
NOTE When CgPN parameter is received, P-Asserted-Identity header is always derived from it as shown in Table 5.3.2-34..			
LEGEND APRI Address Presentation Restricted Indicator AS-SIP Assured Services Session Initiation Protocol CgPN Calling Party Number ISDN Integrated Services Digital Network ISUP ISDN User Part			

1. The Max-Forwards header field for a given message shall never increase and shall decrease by at least one with each successive visit to an SIP/CCS7 IWF, regardless of intervening interworking. The same is true for the Hop Counter value in the ISUP domain.

2. The initial and successively mapped values of the Max-Forwards header field should be large enough to accommodate the maximum number of hops that might be expected of a validly routed call.

Since the value of F must take into account the topology of the networks that are traversed, it will depend on call origin and destination, and will be provisioned at the SIP/CCS7 IWF based on network topology, trust domain rules, and bilateral agreement.

5.3.2.11.5.1.7 Precedence

The modeling of the SIP/CCS7 IWF assumes that preemption of a call will occur at a node either in the AS-SIP network or in the CCS7 network. The role of the SIP/CCS7 IWF is limited to interworking the signaling that indicates the relative priority of the calling party.

NOTE: If the SIP/CCS7 IWF controls the bearer path, it may perform preemption as described in UCR 2008, Section 5.3.2.10.5, CCA Support for Admission Control.

[Conditional] The SIP/CCS7 IWF shall populate the RPH in the outgoing AS-SIP INVITE message as follows:

1. If the Network Identity (NI) in the received Precedence parameter is "0000," corresponding to "dsn," the Network Domain in the RPH shall be coded as "dsn."

2. If the NI in the received Precedence parameter is not "0000," corresponding to "dsn," then the Network Domain in the RPH shall be coded as "dsn."

3. The binary MLPP Service Domain in the received Precedence parameter shall be converted to six characters (0-F, one character per half-octet) and shall be used to populate the Precedence Domain in the RPH.

4. If the NI in the received Precedence parameter is "0000," then the r-priority field in the RPH shall be populated as shown in Table 5.3.2-37, Mapping of IAM Precedence Level to RPH Precedence Subfield.

5. If the NI in the received Precedence parameter is not "0000," then the r-priority field in the RPH shall be coded as 0 ("Routine").

Table 5.3.2-37. Mapping of IAM Precedence Level to RPH Precedence Subfield

ISUP PARAMETER/ FIELD	VALUE	SIP COMPONENT	VALUE
Calling Party Number		Privacy header field	priv-value
	"presentation restricted"	priv-value	"id," but only included if the P-Asserted-Identity header is included in the AS-SIP INVITE message
	"presentation allowed"	priv-value	Omit Privacy header or Privacy header without "id" if other privacy service is needed

LEGEND					
AS-SIP	Assured Services Session Initiation Protocol	ISDN	Integrated Services Digital Network	ISUP	ISDN User Part
				SIP	Session Initiation Protocol

5.3.2.11.5.2 18X Response Received

[Conditional]

UCR 2008, Section 5.3.2.11.5.2.1, Receipt of 180 Ringing, describes procedures on receipt of a 180 Ringing message.

UCR 2008, Section 5.3.2.11.5.2.2, Receipt of 183 Session Progress, describes procedures on receipt of a 183 Session Progress message.

Local ISUP procedures may generate a backward early ACM (no indication) based on timer expiry. Those procedures are independent of these AS-SIP interworking procedures.

5.3.2.11.5.2.1 Receipt of 180 Ringing

[Conditional] On receipt of a 180 Ringing message, timer T_{OIW2} (if running) is stopped. If a 180 Ringing message is received, the SIP/CCS7 IWF shall send either the ACM (if no ACM has previously been sent for this call) or a CPG message (if an ACM has been sent previously for this call).

5.3.2.11.5.2.1.1 Setting for ACM BCIs

[Conditional] Table 5.3.2-38, Indicators in the BCI Parameter, and Table 5.3.2-39, Default BCIs Values, list the bits of the BCI parameters that are set by the SIP/CCS7 IWF when an ACM is sent. Other BCI parameters are set according to ISUP procedures.

Table 5.3.2-38. Indicators in the BCI Parameter

BITS	INDICATORS IN BCI PARAMETER
DC	Called Party's Status Indicator
I	Interworking Indicator
K	ISUP Indicator
M	ISDN Access Indicator

Table 5.3.2-39. Default BCIs Values

PARAMETER	BITS	CODES	MEANING
Interworking Indicator	I	1	Interworking Encountered
ISUP Indicator	K	0	ISUP/BICC not used all the way
ISDN Access Indicator	M	0	Terminating Access Non-ISDN

LEGEND					
BCI	Backward Call Indicator	ISDN	Integrated Services Digital Network	ISUP	ISDN User Part
BICC	Bearer-Independent Call Control				

5.3.2.11.5.2.1.2 Settings for Event Information in CPG

[Conditional] On receipt of a 180 Ringing message, the SIP/CCS7 IWF shall send a CCS7 CPG message with the Event Indicator bits G F E D C B A set “alerting” (0 0 0 0 0 0 1) in the Event Information parameter.

5.3.2.11.5.2.2 Receipt of 183 Session Progress

[Conditional] On receipt of an AS-SIP 183 Session Progress message, no ISUP message is sent backward and ISUP procedures shall continue.

5.3.2.11.5.3 Expiration of T_{OIW2} and Sending Early ACM

[Conditional] When timer T_{OIW2} expires, the SIP/CCS7 IWF shall return an ACM to the CCS7 network. In the case that the Continuity Check is performed, the SIP/CCS7 IWF shall withhold sending an ACM until a successful continuity indication has been received.

[Conditional] When returning an ACM to the CCS7 network, the SIP/CCS7 IWF shall return an awaiting answer indication (e.g., ringing tone) toward the calling party.

[Conditional] The Called Party's Status Indicator (Bit DC) of the BCI parameter in the ACM shall be set to "no indication." The other BCI indicators shall be set as described in UCR 2008, Section 5.3.2.11.5.2.1.1, Setting for ACM BCIs.

5.3.2.11.5.4 Circuit (CIC) Query Response Message Received

[Conditional: SIP/CCS7 IWF]

After sending a Circuit (CIC) Query message, the SIP/CCS7 IWF expects to receive a Circuit (CIC) Query Response message.

[Conditional] The SIP/CCS7 IWF shall process the Circuit (CIC) Query Response message as described in ANSI T1.113.4, clause 2.8.2A. If the ISUP procedures result into release of a call, appropriate actions shall be taken on the AS-SIP side.

5.3.2.11.5.5 200 OK INVITE Received

[Conditional] On receipt of a 200 OK INVITE message, the SIP/CCS7 IWF shall stop Timer T_{OIW2} if it is running.

[Conditional] If the 200 OK INVITE message uses AS-SIP, the SIP/CCS7 IWF shall:

1. Send an ANM as determined by ISUP procedures. If an ANM is sent as the first backward message on the CCS7 side, the BCI parameter shall be coded with the Called Party's Status Indicator (Bits DC) set to "no indication," and the other BCI parameter indicators shall be set as described in UCR 2008, Section 5.3.2.11.5.2.1.1, Setting for ACM BCIs.

2. Stop any existing "awaiting answer indication" (e.g., ringing tone).

5.3.2.11.5.6 Through Connection, Tones and Announcements

Through connection of bearer path is applicable only to a SIP/CCS7 IWF that controls the bearer path.

[Conditional] For AS-SIP, through connection at the SIP/CCS7 IWF shall follow the ANSI T1.113.4 procedures for the destination exchange if this functionality is not available at the adjacent AS-SIP node. If the adjacent AS-SIP node does support the ANSI T1.113.4 procedures for through connection at a destination exchange, the SIP/CCS7 IWF shall follow the following procedures:

1. Through connection of the bearer path shall be completed dependent on whether preconditions are in use on the AS-SIP side of the call.

2. The bearer path shall be connected in both directions on completion of the bearer setup on the AS-SIP side. This event is indicated by the receipt of an SDP Answer acceptable to the SIP/CCS7 IWF, and an indication that all mandatory preconditions (if any) have been met.

3. The bearer path shall be connected in the forward direction no later than on receipt of a 200 OK INVITE message.

[Conditional] For AS-SIP, the following conditions shall result in a ringing tone being played from the SIP/CCS7 IWF:

- 180 Ringing received, and
- ISUP procedures indicate that ringing tone can be applied, and
- The local arrangements assign the role of destination exchange to the SIP/CCS7 IWF rather than the associated AS-SIP entity.

Ringing tone or a progress announcement may already be playing as a result of T_{OIW2} expiry. See UCR 2008, Section 5.3.2.11.5.3, Expiration of T_{OIW2} and Sending Early ACM.

[Conditional] In the case of ringing tones being played as a result of T_{OIW2} expiry, no additional ringing tone shall be played.

NOTE: If the associated AS-SIP entity performs the functions of the destination exchange, other tones or announcements may be received from the AS-SIP network.

5.3.2.11.5.7 Release Procedures

5.3.2.11.5.7.1 Receipt of Forward REL

[Conditional] Upon receipt of an ISUP REL message:

1. If a REL message is received before the INVITE request has been sent, the SIP/CCS7 IWF shall take no action on the AS-SIP side other than to terminate local procedures, if any, that are in progress.

2. If a REL message is received before any response has been received to the INVITE request, the SIP/CCS7 IWF shall hold the REL message until an AS-SIP response has been received. At that point, it shall take appropriate release actions.

3. If a REL message is received before a response has been received that establishes a confirmed dialog or early dialog, the SIP/CCS7 IWF shall send a CANCEL request. If the SIP/CCS7 IWF subsequently receives a 200 OK INVITE request, then it shall send an ACK message for the 200 OK INVITE request, and subsequently, send a BYE request after the ACK message has been sent.

4. If a REL message is received at the SIP/CCS7 IWF after a response has been received that establishes a confirmed dialog or early dialog, the SIP/CCS7 IWF shall send a BYE request. For cases in which no encapsulation is used, for an early dialog only, CANCEL may be used instead.

5. If a REL message is received after the 200 OK INVITE request, but before the outgoing side of the SIP/CCS7 IWF has sent the ACK message, then the SIP/CCS7 IWF shall send the ACK message before sending a BYE request.

NOTE: Depending on local policy, a Reason header field containing the received (ITU-T Q.850 or ANSI) cause value of the REL message may be added to the CANCEL or BYE request. If the Coding standard field of the Cause Indicators parameter is set to “ANSI Standard,” the Protocol parameter of the Reason header is set to “ANSI,” and if the Coding standard is set to “ITU-T Standard,” the Protocol parameter is set to “Q.850.” The mapping of the Cause Indicators parameter to the Reason header is shown in Table 5.3.2-27, Receipt of RSC, GRS, or CGB Messages.

5.3.2.11.5.7.2 Receipt of Backward BYE

[Conditional] On receipt of an AS-SIP BYE request, the SIP/CCS7 IWF shall send a CCS7 REL message.

[Conditional] For the AS-SIP case, if a Reason header with a Protocol parameter set to either "Q.850" or "ANSI" is included in the BYE request, then the appropriate cause value may be mapped to the cause value field in the REL message depending on the local policy. The mapping of the Reason header to the Cause Indicators parameter is shown in Table 5.3.2-22, Mapping of AS-SIP Reason Header Fields into Cause Indicators Parameter (see UCR 2008, Section 5.3.2.11.4.12.1, Receipt of BYE or CANCEL). In case a value is not available from the Reason header field, the Cause Indicators parameter shall be encoded as "normal clearing" (Cause Value No. 16).

5.3.2.11.5.7.3 Autonomous REL at the SIP/CCS7 IWF

Table 5.3.2-40, Autonomous REL at SIP/CCS7 IWF, shows the trigger events at the SIP/CCS7 IWF and the release initiated by the SIP/CCS7 IWF when the call is traversing from ISUP to AS-SIP.

Table 5.3.2-40. Autonomous REL at SIP/CCS7 IWF

REL ON THE CCS7 SIDE CAUSE PARAMETER	TRIGGER EVENT	AS-SIP SIDE
As determined by ISUP procedure	COT received with the Continuity Indicators parameter set to "continuity check failed" or the ISUP timer T8 expires	Send CANCEL or BYE request according to the rule described in Section 5.3.2.11.5.7.1.
REL message with Cause Value No. 47 (resource unavailable, unspecified)	Internal resource reservation unsuccessful	As determined by AS-SIP procedure
As determined by ISUP procedure	ISUP procedures result in generation of autonomous REL message on the ISUP side.	Send CANCEL or BYE request, according to the rule described in Section 5.3.2.11.5.7.1.
Depending on the AS-SIP release reason	AS-SIP procedures result in a decision to release the call	As determined by AS-SIP procedure

LEGEND
AS-SIP Assured Services Session Initiation Protocol
CCS7 Common Channel Signaling No. 7
ISDN Integrated Services Digital Network
ISUP ISDN User Part
REL Release

[Conditional] If, after answer, ISUP procedures result in autonomous REL message from the SIP/CCS7 IWF, then a BYE request shall be sent on the AS-SIP side.

5.3.2.11.5.7.4 Reset Circuit, Circuit Group Reset, or Circuit Group Blocking Message Received

Table 5.3.2-41, Receipt of RSC, GRS, or CGB Messages, shows the message sent by the SIP/CCS7 IWF upon receipt of an ISUP RSC message, GRS message, or CGB message with the Circuit Group Supervision Message Type Indicator coded as "hardware failure oriented." On

receipt of a GRS or CGB message, one AS-SIP message is sent for each call association. Therefore, multiple AS-SIP messages may be sent on receipt of a single GRS or CGB message.

Table 5.3.2-41. Receipt of RSC, GRS, or CGB Messages

MESSAGE RECEIVED FROM ISUP	MESSAGE SENT TO AS-SIP NETWORK:
RSC	CANCEL or BYE
GRS	CANCEL or BYE
CGB with the Circuit Group Supervision Message Type Indicator coded *"hardware failure oriented"*	CANCEL or BYE
LEGEND AS-SIP Assured Services Session Initiation Protocol CGB Circuit Group Blocking Message GRS Circuit Group Reset Message	ISDN Integrated Services Digital Network ISUP ISDN User Part RSC Reset Circuit Message

[Conditional] The SIP/CCS7 IWF shall process received CCS7 RSC, GRS, or CGB message as shown in Table 5.3.2-41, Receipt of RSC, GRS, or CGB Messages. The SIP/CCS7 IWF shall send a CANCEL or BYE message according to the rule described in UCR 2008, Section 5.3.2.11.5.7.1, Receipt of Forward REL.

Depending on local policy, a Reason header field containing the (ITU-T Q.850 or ANSI) Cause Value of the REL message sent by the SIP/CCS7 IWF may be added to the AS-SIP message (BYE or CANCEL).

5.3.2.11.5.7.5 3XX, 4XX, 5XX, or 6XX Response INVITE Received

[Conditional] The SIP/CCS7 IWF shall handle receipt of a 3XX Redirection message, if received in a response as part of a valid dialog, according to the AS-SIP protocol, resulting in invocation of the local routing function.

The remainder of this section applies only to the 4XX, 5XX, and 6XX response cases.

[Conditional] If a Reason header is included in a received 4XX, 5XX, or 6XX message, then the SIP/CCS7 IWF shall map the cause value of the Reason header to the ISUP Cause Value field in the CCS7 REL message. The mapping of the Reason header to the Cause Indicators parameter shall be as shown in Table 5.3.2-23, Mapping of Cause Indicators Parameter into AS-SIP Reason Header Fields.

[Conditional] If no Reason header is included in a received 4XX, 5XX, or 6XX message, then the SIP/CCS7 IWF shall use the mapping of the status code to cause value on receipt of a 4XX,

5XX, or 6XX final response to the INVITE request into the AS-SIP network side, as shown in Table 5.3.2-42, Mapping of 4XX, 5XX, or 6XX to REL Message.

Table 5.3.2-42. Mapping of 4XX, 5XX, or 6XX to REL Message

REL (CAUSE CODE)	4XX/5XX/6XX SIP MESSAGE	REMARKS
127 Interworking	400 Bad Request	
127 Interworking	401 Unauthorized	Note 1
127 Interworking	402 Payment Required	
127 Interworking	403 Forbidden	
1 Unallocated number	404 Not Found	
127 Interworking	405 Method Not Allowed	
127 Interworking	406 Not Acceptable	
127 Interworking	407 Proxy Authentication Required	Note 1
127 Interworking	408 Request Timeout	
22 Number changed (without diagnostic)	410 Gone	
127 Interworking	413 Request Entity Too Long	Note 1
127 Interworking	414 Request-URI Too Long	Note 1
127 Interworking	415 Unsupported Media Type	Note 1
127 Interworking	416 Unsupported URI Scheme	Note 1
127 Interworking	420 Bad Extension	Note 1
127 Interworking	421 Extension Required	Note 1
127 Interworking	423 Interval Too Brief	
20 Subscriber absent	480 Temporarily Unavailable	
127 Interworking	481 Call/Transaction Does Not Exist	
127 Interworking	482 Loop Detected	
127 Interworking	483 Too Many Hops	
28 Invalid Number format	484 Address Incomplete	Note 1
127 Interworking	485 Ambiguous	
17 User busy	486 Busy Here	
127 Interworking or no mapping (Note 3)	487 Request Terminated	Note 2
127 Interworking	488 Not Acceptable Here	
No mapping.	491 Request Pending	Note 2
127 Interworking	493 Undecipherable	
127 Interworking	500 Server Internal Error	
127 Interworking	501 Not Implemented	
127 Interworking	502 Bad Gateway	
127 Interworking	503 Service Unavailable	Note 1
127 Interworking	504 Server Timeout	
127 Interworking	505 Version Not Supported	Note 1
127 Interworking	513 Message Too Large	Note 1
127 Interworking	580 Precondition Failure	Note 1
17 User busy	600 Busy Everywhere	
21 Call rejected	603 Decline	
1 Unallocated number	604 Does Not Exist Anywhere	

REL (CAUSE CODE)	4XX/5XX/6XX SIP MESSAGE	REMARKS
127 Interworking	606 Not Acceptable	

NOTES
1. This response may be handled entirely on the AS-SIP side; if so, it is not interworked.

2. This response does not terminate an AS-SIP dialog, but only a specific transaction within it.

3 No mapping if the SIP/CCS7 IWF previously issued a CANCEL request for the INVITE.
.

LEGEND

AS-SIP	Assured Services Session Initiation Protocol	REL	Release
CCS7	Common Channel Signaling No. 7	SIP	Session Initiation Protocol
ISDN	Integrated Services Digital Network	SS7	Signaling System No. 7
ISUP	ISDN User Part	URI	Universal Resource Identifier
IWF	Interworking Function		

[Conditional] When the response to the INVITE request results in the sending of a REL message with a Cause Code No. 127, Interworking, the Location field shall be set to "network beyond interworking point."

In all cases where AS-SIP itself or this section specifies additional AS-SIP behavior related to the receipt of a particular INVITE response, these procedures should be followed in preference to the immediate sending of a REL message to the CCS7 network.

[Conditional] If there are no AS-SIP procedures associated with this response, the REL message shall be sent to the CCS7 network immediately.

It is possible that receipt of certain 4XX, 5XX, and 6XX responses to an INVITE request will not result in any REL message being sent to the CCS7 network. For example, if a 401 Unauthorized response is received and the SIP/CCS7 IWF successfully initiates a new INVITE request containing the correct credentials, the call will proceed.

If no further reference is given in the Remarks column, then this means that the AS-SIP response is interworked to a CCS7 REL message sent on the ISUP side of the SIP/CCS7 IWF with the cause value indicated within the table. In cases where further reference is indicated, the behavior of the SIP/CCS7 IWF is described within the referred-to clause. However, Table 5.3.2-43, Interworking Timer, indicates the "eventual" behavior of the SIP/CCS7 IWF in the case that further measures taken on the AS-SIP side of the call (to try to sustain the call) fail, resulting in the requirement to send a REL message into the CCS7 network with the cause value indicated.

5.3.2.11.6 Interworking Timer

The SIP/CCS7 IWF requires one timer that is specific to its interworking functionality. Table 5.3.2-43, Interworking Timer, summarizes the timer T_{OIW2}. The value of T_{OIW2} is set between 4 and 14 seconds (with a default value of 4 seconds). The timer is started when an INVITE

request is sent (unless an ACM has already been sent for this call). The timer is stopped on receipt of any of the following messages:

- 180 Ringing
- 183 Session Progress with an encapsulated ACM
- 200 OK INVITE

Table 5.3.2-43. Interworking Timer

TIME-OUT VALUE	CAUSE FOR INITIATION	NORMAL TERMINATION	AT EXPIRY
4-14 seconds (default of 4 seconds)	Sending of INVITE request unless the ACM has already been sent	On reception of 180 Ringing, 183 Session Progress with encapsulated ACM or 200 OK INVITE request	Send early ACM. For AS-SIP case, send the awaiting answer indication (e.g., ring tone) or appropriate progress announcement to the calling party.
LEGEND ACM Address Complete Message AS-SIP Assured Services Session Initiation Protocol			

[Conditional] The SIP/CCS7 IWF shall initiate the timer when an INVITE request is sent unless an ACM has already been sent for this call.

[Conditional] At the expiry of the timer, the SIP/CCS7 IWF shall send an early ACM into the CCS7 network.

[Conditional] For the AS-SIP case only, the SIP/CCS7 IWF shall send the awaiting answer indication (e.g., ring tone) or appropriate progress announcement to the calling party.

5.3.2.12 Media Gateway Requirements

5.3.2.12.1 Introduction

The purpose of this section is to provide generic system requirements for the MG function in the following network appliances:

- LSC
- MFSS

The LSC and MFSS have defined designs that include an MGC function and one or more MG functions.

The scope of these MG requirements covers the following areas:

1. Physical interfaces and protocols supported on the TDM side of the MG

    a. DoD CCS7 trunks (The TDM media trunks terminate on the MG, the TDM signaling links terminate on the separate SG, which is discussed in UCR 2008, Section 5.3.2.13, Signaling Gateway Requirements.)

    b. ISDN PRI trunks (The TDM media (B channels) channels and the TDM signaling channels (D channels) both terminate on the MG.)

    c. CAS trunks (Both DTMF and MF; the TDM channel that carries both the media and the signaling terminates on the MG.)

2. VoIP interfaces and protocols supported on the IP side of the MG

    a. Interface to the IP router network and the LAN (ASLAN, LANs internal to a UC product) that the network appliance is connected to

    b. VoIP protocol stacks, supporting IP, IPSec, UDP, TCP, SCTP, and SRTP.

    c. Secure VoIP media streams, packetized using IP, UDP, and SRTP, in accordance with UCR 2008, Section 5.4, Information Assurance Requirements

    d. Secure VoIP signaling messages, packetized using IPSec, and UDP or TCP or SCTP, in accordance with UCR 2008, Section 5.4, Information Assurance Requirements

        (1) H.248 signaling messages, for MGC control of DoD CCS7, ISDN PRI, and CAS trunks (if the supplier supports H.248)

        (2) ISDN PRI signaling messages, for MGC control of ISDN PRI trunks

3. Support for the following VoIP codecs, at a minimum, on the IP side of the MG:

    a. ITU-T Recommendation G.711 (uncompressed voice, both North American (μ-law and International A-law))

    b. ITU-T Recommendation G.723.1

    c. ITU-T Recommendation G.729

4. Support for FoIP on the IP side of the MG

5. Support for voiceband MoIP on the IP side of the MG

   The following terms define "Modem over IP" traffic, as used in the UCR 2008. The terms are listed here to clarify that SCIP over IP streams are a subset of all possible modem relay streams. For the purposes of the UCR 2008, the term SCIP over IP can be considered synonymous with the transmission of SCIP over V.150.1 Modem Relay. These terms also appear in Appendix A, Definitions, Abbreviations and Acronyms, and References.

   a. Modem over IP. The transport of modem data across an IP network, via either modem relay or voice band data (modem pass-through) techniques.

   b. Modem Relay. A subset of Modem over IP in which modem termination is used at gateways, thereby allowing only the baseband data to reach the packet network.

   c. Voice band Data (Modem Pass-Through). A subset of Modem over IP in which modem signals are transmitted over the voice channel of a packet network.

   d. SCIP over IP. The transport of SCIP information over an IP network. SCIP traffic can be transmitted over an IP network in many ways, but currently, the U.S. Government requires SCIP devices to support transmission of SCIP on IP networks via V.150.1 modem relay.

6. Support for SCIP over IP on the IP side of the MG

   As noted above, SCIP over IP streams are a subset of all possible modem relay streams. For the purposes of the UCR 2008, the term SCIP over IP is synonymous with the transmission of SCIP over V.150.1 Modem Relay. For SCIP over IP calls, the MG supports V.150.1 Modem Relay traffic in accordance with ITU V.150.1 and NSA document SCIP 216 on the IP side of the MG.

7. Support for 64 kbps unrestricted digital information (clear channel) ISDN over IP on the IP side of the MG

5.3.2.12.2 Overview of the MG and MGC Functions

Media Gateway is a generic term for a Trunk Gateway (TG) and for an Access Gateway (AG). Thus, MG requirements apply to TGs and to AGs.

Figure 5.3.2-11, MGC – MG Layered Interface, illustrates the relationship between the MGC, a component of the CCA, and a generic MG.

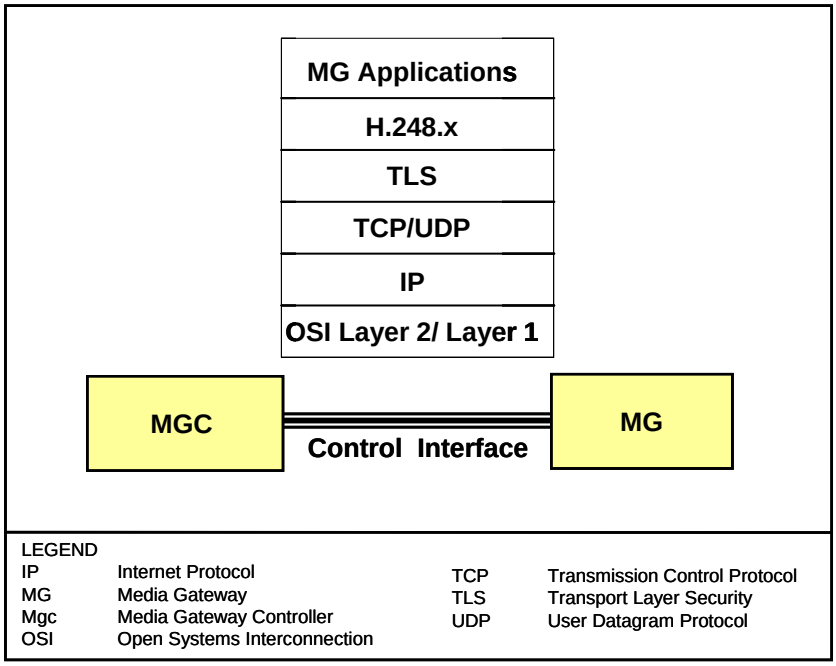


Figure 5.3.2-11. MGC – MG Layered Interface

Figure 5.3.2-12, MG Trunk Function, illustrates the MG trunk function.

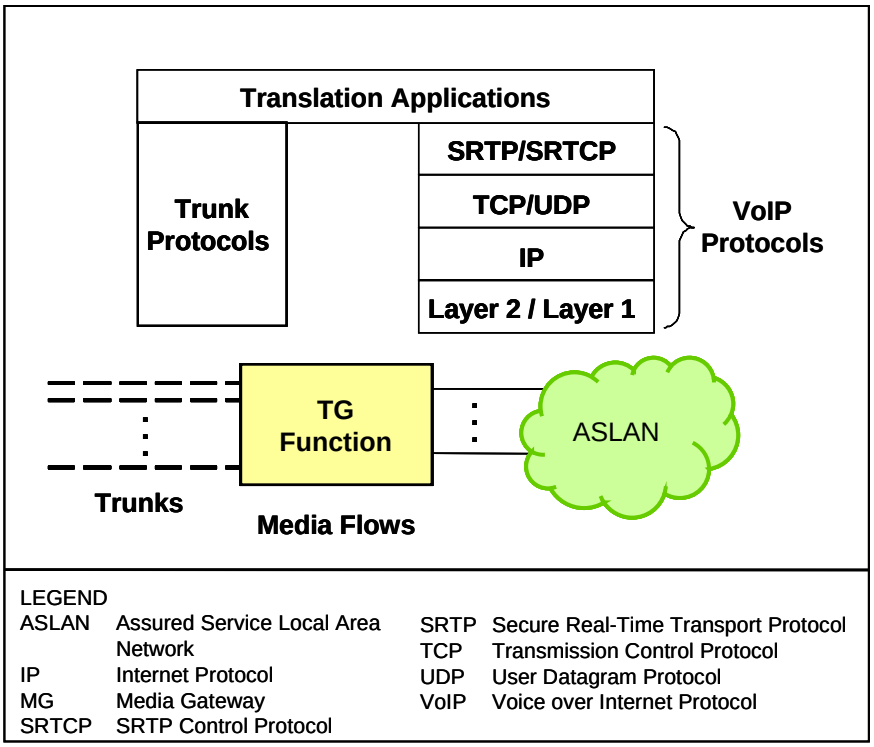


Figure 5.3.2-12. MG Trunk Function

5.3.2.12.2.1 Primary Trunk Functions and Interfaces

An MG may support a trunk side interface to circuit-switched telephone networks. It terminates circuit-switched trunks in the circuit-switched networks and packet flows in the DISN Core network and, as such, provides functions such as media translation. The MG has the capability to set up and manage media flows through the Core network when instructed by the CCA. It is associated with a specific CCA that provides it with the necessary call control instructions.

5.3.2.12.2.2 Primary Access Functions and Interfaces

An MG may support line-side and trunk-side interfaces to the voice network end users. Traditional telephones and PBXs, currently used in the PSTN, as well as ISDNBRI telephones, ISDN BRI terminals, and ISDN-capable PBXs using PRIs, can access the DISN Core network through the MG. The MG provides functions, such as packetization and echo control, for its end users' information streams, and is associated with a specific CCA that provides the necessary call control and service control instructions. On receiving the appropriate commands from its CCA, the MG provides Call Control functions, such as audible ringing and power ringing, as well as Service Control functions. The MG also is capable of setting up transport connections through the DISN Core network when instructed to do so by the CCA (see Figure 5.3.2-13, MG Primary Access Functions and Interfaces).

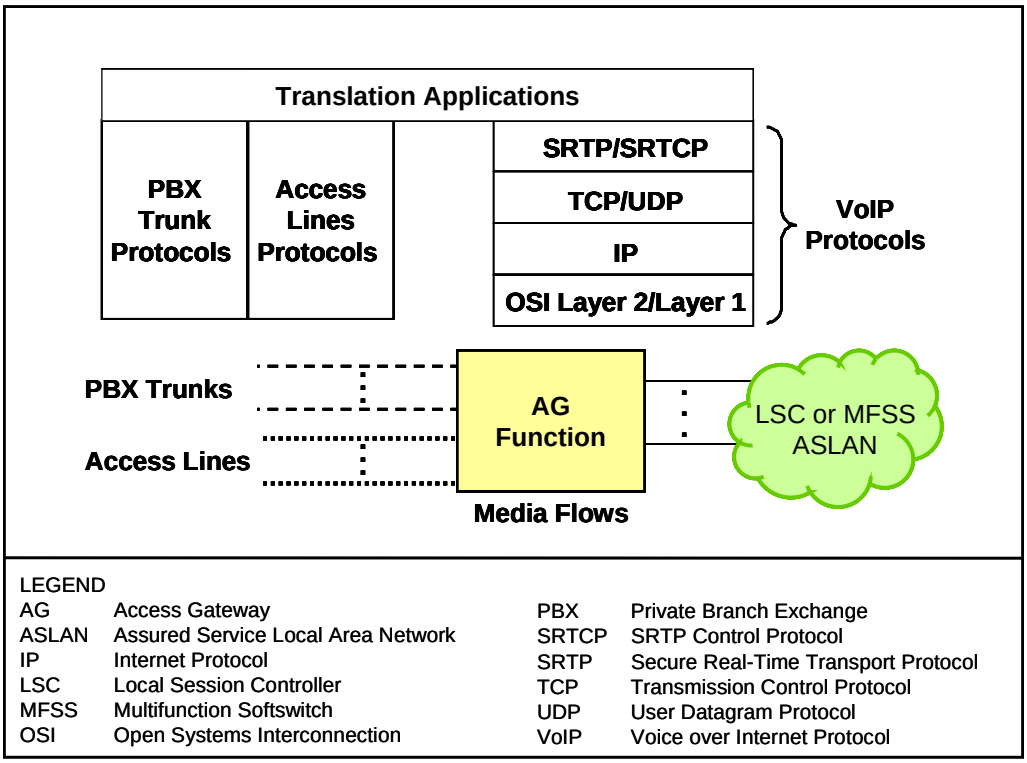


Figure 5.3.2-13. MG Primary Access Functions and Interfaces

5.3.2.12.2.3 MGC Functions

The requirements in this section allow for two options for the Gateway Control Protocol in the MGC and the MG as follows:

1. An industry-standard Gateway Control Protocol, using an open interface between the MGC and the MG. This protocol assumes MG-to-MGC communication over IP and the LAN that the appliance is connected to. This LAN is the ASLAN for the LSC and MFSS. (In some cases, this LAN may be the Internal LAN of the UC product, where the UC product also contains the LSC or the MFSS. In these cases, the Internal LAN of the UC product is not an ASLAN.)

   The industry-standard Gateway Control Protocol used in these requirements is ITU-T Recommendation H.248.1.

2. A supplier-specific Gateway Control Protocol, using a closed (supplier-proprietary) interface between the MGC and the MG. This supplier-specific protocol may use MGC-to-MG communication over IP and the LAN that the appliance is connected to (ASLAN or Internal LAN for the UC product), or it may use separate physical, data link, and network layer interfaces that are also proprietary to the supplier.

   The MGC function is part of the CCA function in the LSC and MFSS, which in turn is part of the SCS functions in these appliances. The MG function is a standalone appliance function in the LSC and MFSS, and is not part of any other appliance function.

The role of the MGC within an LSC and MFSS is to:

1. Control all MGs within the LSC and MFSS.

2. Control all trunks (e.g., DoD CCS7, PRI, or CAS) within each MG.

3. Control all signaling and media streams on each trunk within each MG.

4. Accept IP-encapsulated signaling streams from an SG or MG, and return IP-encapsulated signaling streams to the SG or MG accordingly.

5. The MGC and the MG that it controls are considered Conditional – Tactical for the LSC, and Required for the MFSS.

5.3.2.12.3 Role of the MG in Appliances

The MG provides circuit-switched trunk termination for DoD CCS7, PRI, and CAS trunks, and TDM/VoIP interworking. The MG is controlled by the MGC. The protocol that the MGC uses to control the MG can be ITU-T H.248 (specifically, H.248.1) or a proprietary protocol chosen by the LSC supplier.

5.3.2.12.3.1 Role of the MG in the LSC

Figure 5.3.2-14, Functional Reference Model – LSC, illustrates the reference model for the LSC, including the VoIP MG and MGC.

The roles of the MG within the LSC are as follows:

1. The MG terminates all TDM trunks that interconnect the LSC with TDM networks, including

    a. DoD TDM networks (e.g., DSN, including EO and Tandem switches within the DSN), both in the United States and worldwide

    b. PSTNs, both in the United States and worldwide

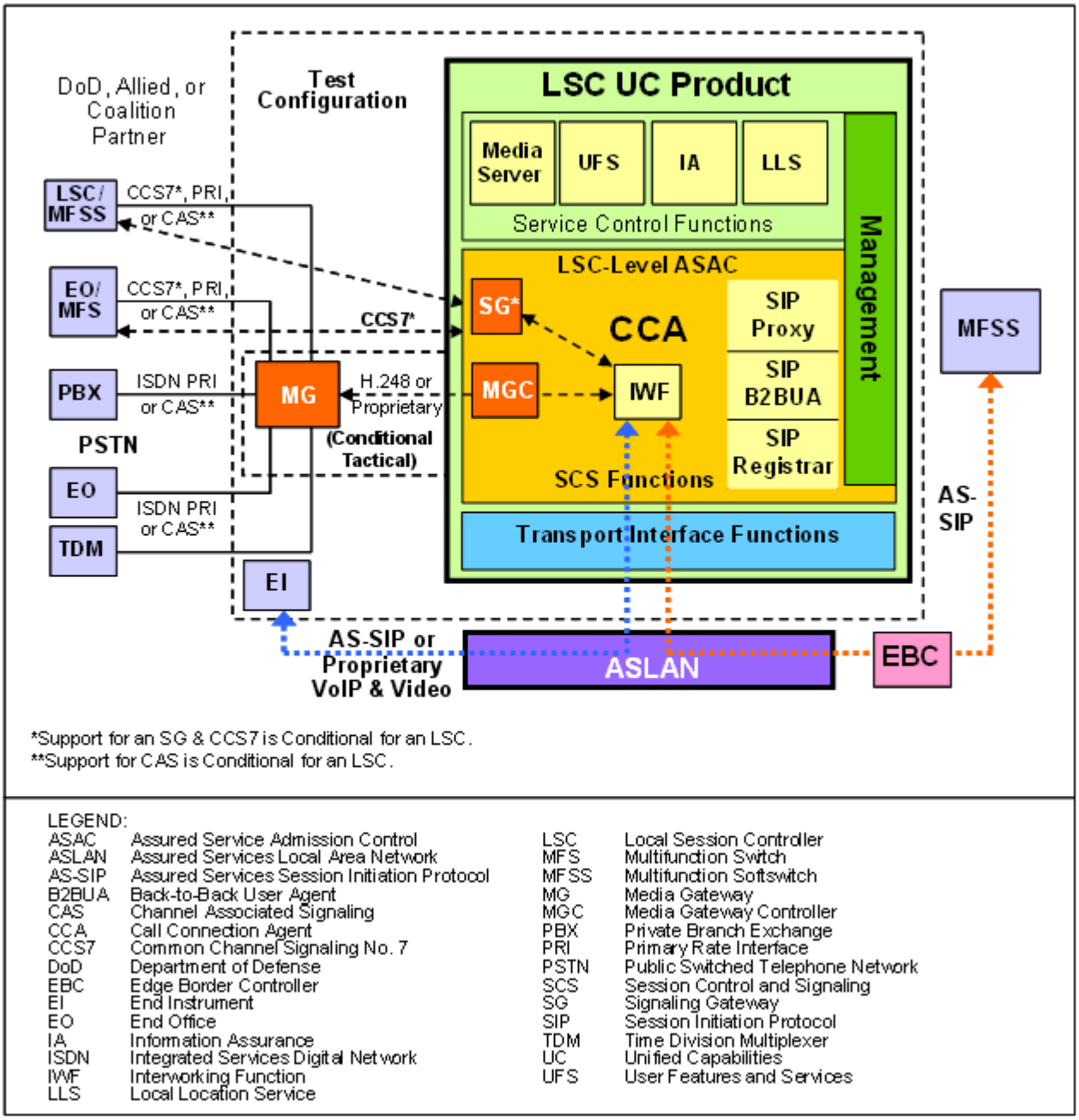
    c. Allied and U.S. coalition partner TDM networks

2. The MG terminates all TDM trunks that interconnect the LSC with TDM PBXs within the same DoD B/P/C/S.

3. The MG supports the physical interconnection of the following TDM trunk groups with the LSC:

    a. **[Conditional: LSC]** DoD CCS7 trunk groups
    b. ISDN PRI trunk groups (for both U.S. PRI and foreign country PRI)
    c. **[Conditional: U.S. and foreign country CAS]** CAS trunk groups

    Media gateway support for these TDM trunk groups is expected to be identical to the support for these trunk groups in DoD TDM PBXs, EOs, Tandem switches, and MFSs today, as specified in UCR 2008, Section 5.2, Circuit-Switched Capabilities and Features.



LEGEND:

ASAC	Assured Service Admission Control	LSC	Local Session Controller
ASLAN	Assured Services Local Area Network	MFS	Multifunction Switch
AS-SIP	Assured Services Session Initiation Protocol	MFSS	Multifunction Softswitch
B2BUA	Back-to-Back User Agent	MG	Media Gateway
CAS	Channel Associated Signaling	MGC	Media Gateway Controller
CCA	Call Connection Agent	PBX	Private Branch Exchange
CCS7	Common Channel Signaling No. 7	PRI	Primary Rate Interface
DoD	Department of Defense	PSTN	Public Switched Telephone Network
EBC	Edge Border Controller	SCS	Session Control and Signaling
EI	End Instrument	SG	Signaling Gateway
EO	End Office	SIP	Session Initiation Protocol
IA	Information Assurance	TDM	Time Division Multiplexer
ISDN	Integrated Services Digital Network	UC	Unified Capabilities
IWF	Interworking Function	UFS	User Features and Services
LLS	Local Location Service		

Figure 5.3.2-14. Functional Reference Model – LSC

4. In the DoD CCS7 case, [Conditional] the MG is responsible for terminating the TDM media trunks, (on the TDM side), and for terminating the VoIP/FoIP/MoIP media streams, (on the VoIP side). In these cases, the separate SG is responsible for terminating the TDM CCS7 signaling links and the VoIP/FoIP/MoIP signaling streams.

5. In the PRI and CAS cases, the MG is responsible for terminating the TDM media trunks and signaling links, on the TDM side, and for terminating the VoIP/FoIP/MoIP media streams and signaling streams, on the VoIP side.

6. On calls that traverse the MG, the MG converts TDM media streams to VoIP, FoIP, or MoIP media streams, and converts VoIP, FoIP, or MoIP media streams to TDM media streams.

7. The MG supports interconnection of VoIP, FoIP, and MoIP media streams with the following LSC functions and end user devices:

   a. **[Required: LSC MG]** The LSC Media Server, which provides tones and announcements for LSC calls and LSC features

   b. **[Conditional: LSC MG]** Proprietary VoIP, FoIP, and MoIP EIs on the LSC

   c. **[Conditional: LSC MG]** SIP EIs on the LSC

   d. **[Conditional: LSC MG]** H.323 EIs on the LSC

   e. **[Conditional: LSC MG]** AS-SIP VoIP, FoIP, and MoIP EIs on the LSC

8. On ISDN PRI calls that traverse the MG, the MG converts TDM signaling streams to VoIP signaling streams and converts VoIP signaling streams to TDM signaling streams. When H.248 control is used, the MG will send and receive encapsulated PRI signaling from and to the CCA.

9. On CAS trunk calls that traverse the MG, the MG converts TDM signaling streams to VoIP signaling streams and converts VoIP signaling streams to TDM signaling streams. When H.248 control is used, the MG will translate between CAS signaling and H.248 protocol messages to and from the CCA.

10. **[Condtional – Tactical: LSC MG]** The MG and the MGC that controls the MG are considered "Conditional – Tactical" for the LSC. Some LSC suppliers may include an MGC and MG in their tactical LSC product, and other LSC suppliers may not. Those suppliers who do should follow the MG requirements defined in UCR 2008.

5.3.2.12.3.1.1 LSC MG VoIP Signaling Interfaces

The LSC MG supports the VoIP signaling interfaces shown in Table 5.3.2-44, LSC MG Support for VoIP Signaling Interfaces. The complete signaling requirements for the LSC are summarized in Table 5.3.2-4, LSC Support for VoIP and Video Signaling Interfaces.

Table 5.3.2-44. LSC MG Support for VoIP Signaling Interfaces

FUNCTIONAL COMPONENT	VoIP SIGNALING INTERFACES	VoIP SIGNALING PROTOCOLS
MG and MGC (CCA)	MG – to – MGC (CCA)	ITU-T H.248 over IP (used with DoD CCS7, ISDN PRI, and CAS trunks)
MG and MGC (CCA)	MG – to – MGC (CCA)	ISDN PRI over IP (North American National ISDN Version, used with ISDN PRI trunks only)
MG and MGC (CCA)	MG – to – MGC (CCA)	Proprietary Supplier Protocols, Used as an alternative to ITU-T H.248 over IP and ISDN PRI over IP (used with DoD CCS7, ISDN PRI, and CAS trunks)

5.3.2.12.3.2 Role of the MG in the MFSS

Figure 5.3.2-15, Functional Reference Model – MFSS, provides the functional reference model of the MFSS. The role of the MG in the MFSS is identical to the role of the MG in the LSC (including the underlying assumptions, roles of the MG and MGC, interactions with other LSC components, and VoIP signaling interfaces), with the following exceptions and extensions:

1. The MG in the MFSS assists the MFSS CCA in providing call denial treatments for CAC, and call preemption treatments for LSC-Level ASAC and WAN-Level ASAC. The MFSS supports LSC-Level ASAC for admission control for calls to and from EIs that it serves directly. The MFSS also supports WAN-Level ASAC for admission control for calls to and from LSCs that it serves directly.

2. The MG in the MFSS supports DoD CCS7 trunks, [Conditional] in addition to supporting ISDN PRI **[Required]** and CAS trunks **[Conditional]**. Support for these DoD CCS7 trunks is a conditional requirement for the MFSS MG and the LSC MG.

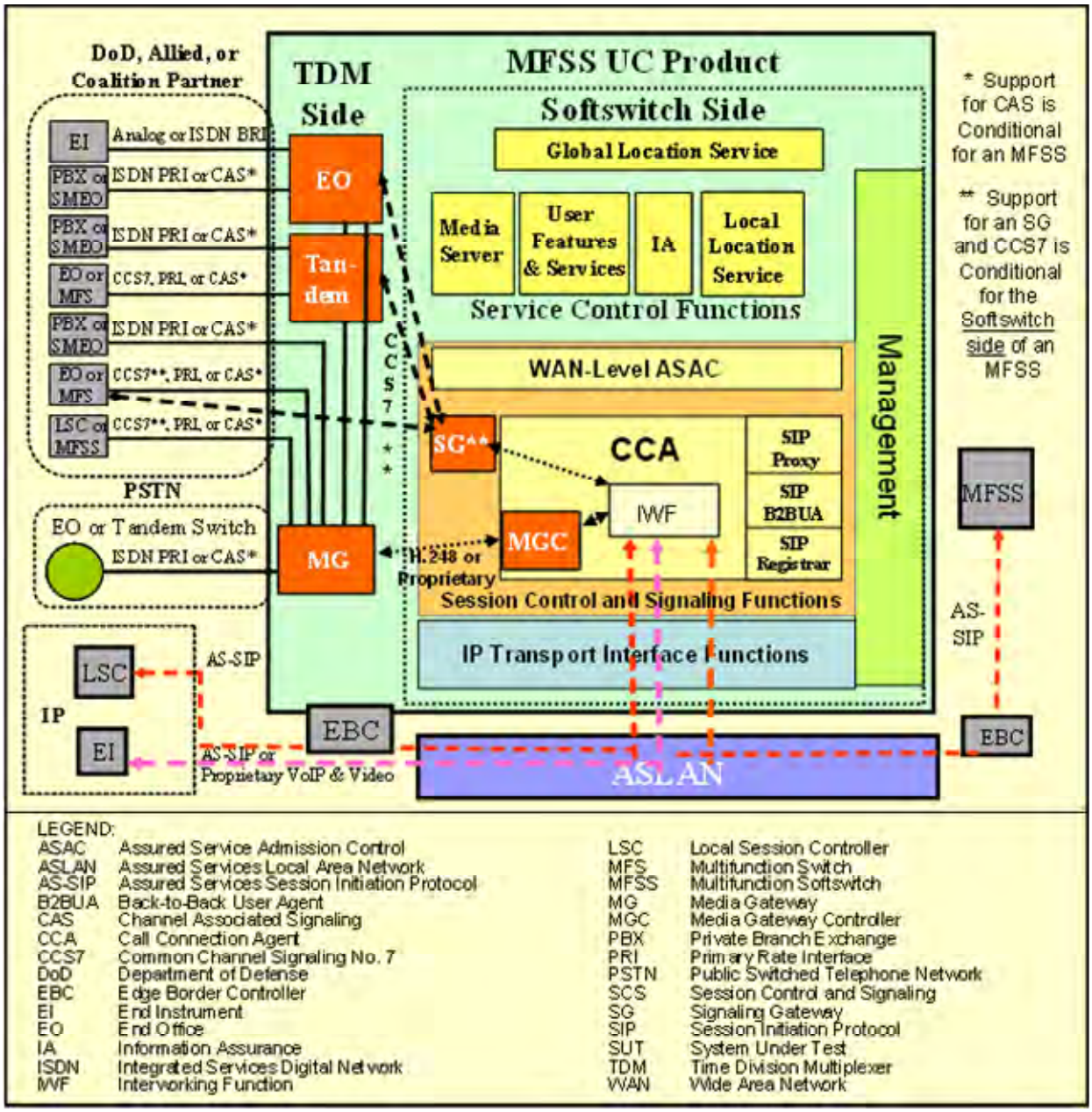


Figure 5.3.2-15. Functional Reference Model – MFSS

NOTE: An LSC within an MFSS will serve a set of (MFSS-internal) LSC EIs and MGs. These LSC EIs and MGs will exchange media streams with EIs and MGs on other LSCs located elsewhere on the DISN WAN. In addition, the MFSS EBC controls these media streams between the (MFSS-internal) LSC EIs and MGs, connected to the MFSS ASLAN, and EIs and MGs on other LSCs, whose separate ASLANs are connected to the DISN WAN.

5.3.2.12.3.2.1 MG Requirements for Interactions between the Softswitch and TDM Sides of the MFSS

The TDM side of the MFSS provides EO and Tandem functions that allow the MFSS to support connectivity to existing TDM switches in DoD networks (i.e., CONUS and Global), allied and coalition networks, and the PSTN worldwide (i.e., CONUS and Global). In addition, the EO function of the TDM side of the MFSS supports TDM users (i.e., analog and ISDN EIs). The softswitch side of the MFSS provides the IP-based features of an LSC with additional features as required to serve as a network-level softswitch.

The CCA/SG/MGC/MG complex in the MFSS must provide interoperability between the softswitch side and TDM side in the MFSS, using connections based on either CCS7, U.S. PRI, or U.S. CAS signaling. In this case, some high-level requirements for this interworking are needed. These high-level requirements are included in this section.

Internal MG connections are used when connecting the softswitch and the TDM sides of an MFSS.

An external MG trunk group" is an MFSS trunk group that connects an MFSS MG with the following:

- The TDM EO or TDM Tandem component of another MFSS in the network
- The MGC/MG component of an LSC or another MFSS in the network
- A TDM PBX, SMEO, EO, Tandem, or MFS in a DoD TDM network
- A TDM PBX, EO, or Tandem in the U.S. PSTN or a foreign country PSTN

[Required] The MFSS MG shall be able to support MG trunk groups (referred to as internal MG connections) that either interconnect the softswitch (VoIP) side of the MFSS with the EO or Tandem functions on the TDM side of the MFSS.

[Conditional] When a DoD CCS7 connection is used between the softswitch and TDM sides of the MFSS, the MFSS MG shall interact with the MFSS MGC so that

- DoD CCS7 signaling is used between the softswitch and TDM sides.

- The CCS7 version of the MLPP feature operates correctly between the softswitch and TDM sides of the MFSS, for both VoIP-to-TDM calls and TDM-to-VoIP calls over this connection.

[Required] When a U.S. ISDN PRI connection is used between the softswitch and TDM sides of the MFSS, the MFSS MG shall interact with the MFSS MGC so that

1. U.S. ISDN PRI signaling (National ISDN PRI signaling, with the Precedence Level IE and related MLPP IEs included) is used between the softswitch and TDM sides.

2. The T1.619/T1.619a version of the ISDN PRI MLPP feature operates correctly between the softswitch and TDM sides of the MFSS, for both VoIP-to-TDM calls and TDM-to-VoIP calls over this connection.

[Conditional] When a U.S. CAS trunk group is used between the softswitch and TDM sides of the MFSS, the MFSS MG shall interact with the MFSS MGC so that

1. U.S. CAS trunk signaling is used between the softswitch and TDM sides.

2. The UCR 2008, Section 5.2, Circuit-Switched Capabilities and Features version of the CAS trunk MLPP feature operates correctly between the softswitch and TDM sides of the MFSS, for both VoIP-to-TDM calls and TDM-to-VoIP calls over this trunk group.

[Required] The MFSS MG shall interact with the MFSS MGC so that internal MG connections between the softswitch and TDM sides of the MFSS support

- TDM calls between the TDM EO/Tandem and VoIP EIs on the MFSS, allowing calls from EO lines to MFSS EIs, and calls from EO and Tandem trunks to MFSS EIs

- TDM calls between the TDM EO/Tandem and the EBC on the MFSS, allowing calls from EO lines to the EBC (and other appliances on the DISN WAN), and calls from EO and Tandem trunks to the EBC (and other appliances on the DISN WAN)

- TDM calls between the TDM EO/Tandem and external MG trunk groups on the MFSS, allowing calls from EO lines to external MG trunk groups, and calls from EO and Tandem trunks to external MG trunk groups

- TDM calls between the TDM EO/Tandem and local MG trunk groups on the MFSS, allowing calls from EO lines to local MG trunk groups, and calls from EO and Tandem trunks to local MG trunk groups (This last case applies when the MFSS supports local MG trunk groups from its MG to subordinate PBX1s and PBX2s, when the subordinate PBX1s and PBX2s have not been migrated to VoIP.)

5.3.2.12.3.2.2 MFSS MG VoIP Signaling Interfaces

The MFSS MG supports the VoIP signaling interfaces shown in Table 5.3.2-45, MFSS MG Support for VoIP Signaling Interfaces.

Table 5.3.2-45. MFSS MG Support for VoIP Signaling Interfaces

FUNCTIONAL COMPONENT	VoIP AND VIDEO SIGNALING INTERFACES	VoIP AND VIDEO SIGNALING PROTOCOLS
MG and MGC	MFSS MG – to – MFSS MGC	ITU-T H.248 over IP (used with DoD CCS7, ISDN PRI, and CAS trunks)
MG and MGC	MFSS MG – to – MFSS MGC	ISDN PRI over IP (North American National ISDN Version, used with ISDN PRI trunks only)
MG and MGC	MFSS MG – to – MFSS MGC	Proprietary Supplier Protocols

Unless stated otherwise, all requirements for an "Appliance MG" are for both the LSC and the MFSS.

5.3.2.12.4 MG Interaction with Network Elements and Functions

The MG is responsible for interacting with elements and functions of the LSC and MFSS to support end user calls, end user features, and other operational capabilities needed by the DoD users (i.e., the Army, Navy, Air Force, and Marines). These other elements include the following:

- ASAC
- Service Control functions (IA and media server)
- Management (FCAPS and audit logs)
- Transport Interface functions
- EBC (not part of the LSC but part of the Local Assured Services Domain)

5.3.2.12.4.1 MG Support for Assured Services Admission Control

The MG interacts with the CCA, which in turn interacts with the ASAC component of the LSC and MFSS, to perform specific functions related to ASAC, such as providing denial treatments for calls that are denied admission to the LSC and/or MFSS, and preemption treatments for calls that are preempted by MLPP.

Requirements for ASAC are handled in two categories: CAC and ASAC, which includes MLPP. In addition, this section covers two different levels of ASAC: LSC-Level ASAC, which is supported in the LSC and the MFSS, and WAN-Level ASAC, which is supported in the MFSS only.

The MG assists the CCA in performing CAC (i.e., call blocking based on budget restrictions) for outgoing TDM calls at MGs, and for incoming TDM calls at MGs.

The MG assists the CCA in performing ASAC (i.e., call preemption based on per-call precedence levels) for outgoing TDM calls at MGs, and for incoming TDM calls at MGs.

In addition, please see UCR 2008, Section 5.3.2.2.2.3, ASAC – Open Loop, and UCR 2008, Section 5.3.4.10, Precedence and Preemption, for detailed requirements on how ASAC is supported by CCAs in LSCs and MFSSs.

5.3.2.12.4.1.1 MG Call Denial Treatments to Support CAC

When the CCA determines that a VoIP session request should be blocked because an Appliance CAC restriction applies (e.g., the VoIP session count equals the VoIP session limit for the type of session being requested), the CCA will deny the session request and apply a Call Denial treatment (i.e., a busy signal or call denial announcement) to the calling party on that request. If the calling party is a TDM calling party whose call enters the appliance at an MG trunk group, the MG is responsible for applying the Call Denial treatment also.

[Required] On incoming call requests to a TDM trunk group, where the CCA/MGC applies a CAC Call Denial treatment to that call request, the MG shall connect the TDM called party on the incoming call request to the appropriate CAC Call Denial tone or announcement, when instructed to do so by the MGC.

5.3.2.12.4.1.2 MG Call Preemption Treatments to Support ASAC and MLPP

When the CCA determines that an existing VoIP Session or VoIP Session request should be cleared because an Appliance ASAC preemption applies (e.g., a CAC limit applies, and a call of a higher precedence level needs to complete within the appliance), the CCA will clear the existing session or session request, and apply a Call Preemption treatment (i.e., a Call Preemption tone or announcement) to both the calling and called parties on that request. If the calling party is a TDM calling party whose call entered the appliance at an MG trunk group, or the called party is a TDM called party whose call left the appliance at an MG trunk group, the MG is responsible for applying the Call Preemption treatment also.

[Required] On incoming calls or call requests to a TDM trunk group, where the CCA/MGC applies an ASAC Call Preemption treatment to that call or call request, the MG shall connect the TDM calling party on the incoming call or call request to the appropriate ASAC Call Preemption tone or announcement, when instructed to do so by the MGC.

[Required] On outgoing calls or call requests from a TDM trunk group, where the CCA/MGC applies an ASAC Call Preemption treatment to that call or call request, the MG shall connect the TDM called party on the outgoing call or call request to the appropriate ASAC Call Preemption tone or announcement, when instructed to do so by the MGC.

5.3.2.12.4.2 MG and IA Functions

The MG interaction with IA function is consistent with the DoD IA requirements in UCR 2008, Section 5.4, Information Assurance Requirements.

The IA function within the appliance ensures that end users, EIs, MGs, SGs, and EBCs that use the appliance are all properly authenticated by the appliance. The IA function also ensures that VoIP signaling streams and media streams that traverse the appliance and its ASLAN are properly encrypted, using SIP/TLS and SRTP, respectively).

Requirements for CCA and MGC interaction with the IA Server are found in UCR 2008, Section 5.3.2.10.7, CCA Support for Information Assurance. These requirements, therefore, apply to the MG.

[Required] Each MG within an appliance shall support all the appliance requirements in UCR 2008, Section 5.4, Information Assurance Requirements, that involve an Appliance MG.

The MG performs the following authentication and encryption functions, in conjunction with the CCA and IA:

1. When the MG registers with the MGC in the CCA, the MG exchanges authentication credentials with the CCA and, through the CCA, with IA.

2. The MG exchanges encryption keys with the CCA, and, through the CCA, with IA, before exchanging H.248 messages and encapsulated PRI messages with the MGC in the CCA.

3. The MG uses the exchanged encryption keys to (1) encrypt H.248 messages and encapsulated PRI messages sent in the MG => CCA => IA direction, and to (2) decrypt H.248 messages and encapsulated PRI messages sent in the IA => CCA => MG direction. The encryption and decryption are performed at the IP layer using IPSec packets, instead of being done at the message layer using H.248 messages or PRI messages.

4. The MG also performs the following encryption functions, in conjunction with EIs, the EBC, and the media server in the LSC (NOTE: These functions may or may not use IA, depending on the internal design of the LSC.):

    a. The MG exchanges encryption keys with local EIs and local MGs, remote EIs and remote MGs, via the EBC, and the media server, before exchanging encrypted VoIP media streams with these devices.

    b. The MG uses the exchanged encryption keys to (1) encrypt VoIP SRTP media streams sent in the MG => EI/Other MG/media server direction, and to (2) decrypt VoIP SRTP media streams received in the EI/Other MG/media server => MG direction. The encryption and decryption are performed above the UDP Transport Layer using SRTP packets.

5.3.2.12.4.3 MG Interaction with Service Control Functions

The media server is responsible for playing tones and announcements to calling and called parties on VoIP calls, and for playing audio/video clips (similar to tones and announcements) to calling and called parties on Video calls. In addition, the media server may provide "play announcement and collect digits" functionality to calling and called parties on VoIP and Video calls, when this functionality is required by certain features that the CCA supports. Depending on the complexity of those features, the media server may act as a full Interactive Voice Response (IVR) system for Appliance EIs and other assured services end users, providing IVR-like features to local and remote VoIP callers, and providing Video-enhanced IVR-like features to local and remote Video callers.

The MG is responsible for routing individual VoIP, FoIP, and MoIP media streams to the media server when instructed to do so by the CCA/MGC. The MG is responsible for removing individual VoIP, FoIP, and MoIP media streams from the media server, and for either disconnecting them entirely, or routing them on to other LSC end users (e.g., VoIP or Video EIs), when instructed to do so by the CCA/MGC.

[Required] When instructed to do so by the MGC, the MG shall direct TDM calls and call requests to the media server, so that the media server can

1. Play tones and announcements to TDM parties on TDM calls and call requests (e.g., busy tone or announcement, call pre-emption tone or announcement).

2. Provide "Play announcement and collect digits" functionality, when required by an Appliance VoIP feature.

3. Provide full IVR-like functionality, when required by an Appliance VoIP feature.

The interface and protocols used to interconnect the MG with the media server are internal to the appliance and are therefore supplier-specific.

5.3.2.12.4.4 Interactions with IP Transport Interface Functions

The Transport Interface functions in the LSC provide interface and connectivity functions with the ASLAN and its IP packet transport network. High-level requirements for these functions are outlined in this section. The detailed implementation methods for these requirements are left up to the vendor. Examples of Transport Interface functions include:

- Network Layer functions: IP, IPSec
- Transport Layer functions: IP Transport Protocols (e.g., TCP, UDP), TLS
- LAN protocols

The MG interacts with Transport Interface functions by using them to communicate with EIs and the EBC (and through the EBC to remote EIs and MGs served by other LSCs and MFSSs) over the ASLAN. The following LSC elements and Local Assured Services Domain elements are all IP end points on the ASLAN:

- Each EI served by the LSC

- The MG itself

- Any other MGs that are served by the LSC (even though the other MGs may be connected physically to the CCA/MGC over an internal proprietary interface, instead of being logically connected to the CCA/MGC over the ASLAN)

- The CCA and its IWF and MGC

- The EBC, which the MG uses to communicate over the DISN WAN with other EIs and MGs that are served by other LSCs and MFSSs

As an example, the CCA interacts with the LSC Transport Interface functions when it uses IP, TLS, UDP, or TCP, and the native ASLAN protocols to exchange SIP signaling messages with EIs and the EBC over the ASLAN.

The MGs controlled by the CCA interact with the LSC Transport Interface functions when they use IP, UDP, and the native ASLAN protocols to route SRTP media streams to and from EIs, other LSC MGs, and the EBC over the ASLAN.

[Required] Since each Appliance MG is an IP end point on the Appliance LAN, each MG shall support assignment of the following items to itself:

- At least one MG IP address
- An MG FQDN that maps to that IP address,
- An MG SIP URI that uses that MG FQDN as its domain name, and maps to a "SIP User Agent" function within the MG. (This MG SIP URI is recommended for consistency with the SIP URIs of the MGC and the Appliance EIs, even though the MG may use H.248, proprietary, and/or tunneled-ISDN-PRI signaling instead of SIP signaling to communicate with the MGC.)

[Required] The MG shall interact with the Transport Interface functions in the appliances in the following cases:

1. When the MG uses the native LAN protocols, IP, and UDP to exchange SRTP media streams with EIs, other MGs, and the EBC over the Appliance LAN.
2. **[Objective]** When the MG uses the native LAN protocols, IPSec, and UDP, TCP, or SCTP, to exchange H.248 signaling messages with the MGC over the Appliance LAN.
3. **[Objective]** When it uses the native LAN protocols, IPSec, and UDP, TCP, or SCTP, to exchange encapsulated PRI messages with the MGC over the Appliance LAN.

5.3.2.12.4.5 MG – EBC Interaction

The EBC provides SBC and firewall capabilities for the ASLAN, the EIs, and the IP-based components of the LSC, including the CCA, and its IWF and MGC, and the MGs.

The MG interacts with the EBC by sending SRTP media streams to it (for call media destined for an EI or MG that is served by another appliance outside the LSC) or by accepting SRTP media streams from it (for call media arriving from an EI or MG that is served by another appliance outside the LSC).

The SRTP media streams exchanged between the LSC MG and a remote EI or MG must pass through the EBC. The EBC's ability to modify SRTP media streams (e.g., by doing NAT or NAPT on them) needs to be considered when writing MG SRTP requirements for the LSC.

The VoIP MG in the MFSS or LSC needs to interact with VoIP Media Transfer functions in the EBC, which

1. Transfers media streams between the EIs and MGs on the appliance, and EIs and MGs on remote appliances, located elsewhere on the DISN WAN.

2. Supports SBC functions, such as NAT and NAPT.

3. Supports IP firewall functions.

4. Supports CE Router functions.

High-level MG requirements are needed for interacting with an EBC. These requirements are as follows:

[Required] When sending VoIP media streams to EIs and MGs served by other network appliances, the MG shall direct these VoIP media streams to the EBC, so that the EBC can process them before sending them on to the remote EIs and MGs via the DISN WAN. The MG shall use the network-level IP addresses of the destination EIs and MGs, rather than the local IP address of the EBC, when directing the VoIP media streams through the EBC to the DISN WAN and the remote EIs and MGs.

[Required] The MG shall direct VoIP media streams to remote EIs and MGs through the EBC in the following cases:

- When the MG is part of an LSC and is directing VoIP media streams to EIs and MGs on another LSC on the DISN WAN

- When the MG is part of an LSC and is directing VoIP media streams to EIs and MGs on an MFSS on the DISN WAN

- When the MG is part of an MFSS and is directing VoIP media streams to EIs and MGs on an LSC on the DISN WAN

- When the MG is part of an MFSS and is directing VoIP media streams to EIs and MGs on another MFSS on the DISN WAN. This other MFSS on the DISN WAN may be

- A "peer" MFSS to the MG's MFSS (e.g., one DoD MFSS in Europe communicating with another one in the Pacific),

- A "higher level" MFSS to the MG's MFSS (e.g., a DoD MFSS in Italy communicating with a theater headquarters MFSS for the DoD in Germany), or

- A "lower level" MFSS to the MG's MFSS (e.g., a theater headquarters MFSS for the DoD in Germany communicating with a DoD MFSS in Italy).

[Required] When accepting VoIP media streams from EIs and MGs served by other network appliances, the MG shall accept these VoIP media streams from the appliance EBC, because the EBC relays them from the DISN WAN and the remote EIs and MGs on the DISN WAN. The MG shall recognize and act on the network-level IP addresses of the remote EIs and MGs, rather than recognizing and acting on the IP address of the EBC, when accepting the VoIP sessions through the EBC from the DISN WAN and the remote EIs and MGs.

[Required] The MG shall accept VoIP media streams from remote EIs and MGs through the EBC in the following cases:

- When the MG is part of an LSC and is accepting VoIP media streams from EIs and MGs on another LSC on the DISN WAN

- When the MG is part of an LSC and is accepting VoIP media streams from EIs and MGs on an MFSS on the DISN WAN

- When the MG is part of an MFSS, and is accepting VoIP media streams from EIs and MGs on an LSC on the DISN WAN

- When the MG is part of an MFSS, and is accepting VoIP media streams from EIs and MGs on another MFSS on the DISN WAN

5.3.2.12.4.6 MG Support for Appliance Management Functions

The Management function in the EBC, LSC, and MFSS supports functions for EBC/LSC/MFSS FCAPS management and audit logs. Detailed requirements for the MG support of the appliance management functions are covered in UCR 2008, Section 5.3.2.18.3, Management Requirements of the MG Function.

The MG interacts with the Appliance Management function by:

1. Making changes to its configuration and to its trunks' configuration, in response to commands from the Management function that request these changes.

2. Returning information to the Management function on its FCAPS, in response to commands from the Management function that request this information.

3. Sending information to the Management function on a periodic basis (e.g., on a set schedule), keeping the Management function up-to-date on MG activity. An example of this update would be a periodic transfer of trunk media error logs from the MG to the Management function, so that the Management function either could store the records locally or transfer them to a remote NMS for remote storage and processing.

5.3.2.12.4.7 IP-Based PSTN Interface Requirements

[Conditional] Voice and video over IP interfaces to the PSTN have not been defined. Therefore, for IOC, the LSC and MFSS to PSTN interface will remain TDM as specified in UCR 2008, Section 5.2, Circuit-Switched Capabilities and Features. Interfaces from an LSC or MFSS to the PSTN will be via an MG with TDM interfaces as specified in UCR 2008, Section 5.2.

5.3.2.12.4.8 MG Requirements: Interactions with VoIP EIs

The MG in the MFSS or LSC needs to interact with VoIP EIs served by that MFSS or LSC, and with VoIP EIs served by other MFSSs or LSCs. The VoIP signaling interface between the EI and the MFSS or LSC is left up to the network appliance supplier in IOC, and may be left up to the supplier in FY12 and beyond. Detailed requirements for this VoIP interface are beyond the scope of this section.

However, the following high-level requirements on VoIP EIs do apply and are part of the MG requirements for the MFSS and LSC:

1. **[Required]** The MG shall support the exchange of VoIP media streams with the following voice EIs both on the local appliance and on remote network appliances:

    a. Supplier-proprietary voice EIs

    b. Voice SIP EIs when the appliance supplier supports these EIs

    c. Voice H.323 EIs when the appliance supplier supports these EIs

d. **[Required for FY12]** Voice AS-SIP EIs when the appliance supplier supports these EIs

2. **[Conditional]** When the MG supports the exchange of Voice media streams with Voice H.323 EIs (both on the local network appliance and on remote network appliances), the MG shall support a mechanism for interworking the G.7xx/SRTP/UDP/IP-based VoIP media streams that the MG uses with the H.323-based VoIP media streams that the H.323 EI uses.

5.3.2.12.4.9 MG Support for User Features and Services

[Required] The MG shall support the operation of the following features for VoIP and Video end users, consistent with the operation of this feature on analog and ISDN lines in DoD TDM switches today:

- Call Hold
- Music on Hold
- Call Waiting
- Precedence Call Waiting
- Call Forwarding Variable
- Call Forwarding Busy Line
- Call Forwarding No Answer
- Call Transfer
- Three-Way Calling
- Hotline Service
- Calling Party and Called Party ID (number only)

5.3.2.12.5 MG Interfaces to TDM Network Elements in DoD Networks: PBXs, EOs, and MFSs

[Required] Each appliance MG shall support TDM trunk groups that can interconnect with the following network elements in DoD networks, in the United States and worldwide:

- PBXs
- SMEOs
- EOs
- MFSs
- LSCs in the DISN/DoD network
- MFSSs in the DISN/DoD network

[Required] Each appliance MG shall support TDM trunk groups that can interconnect with DISN and DoD network elements in the United States and worldwide using the following types of trunk groups:

- **[Conditional: LSC, MFSS]** DoD CCS7 per UCR 2008, Section 5.2, Circuit-Switched Capabilities and Features, where the MG handles the media trunks, and the SG handles the signaling links

  – ANSI T1.619 and T1.619A support is required for CCS7 MLPP signaling, per UCR 2008, Section 5.2, Circuit-Switched Capabilities and Features.

- **[Required: LSC, MFSS]** U.S. National ISDN PRI per UCR 2008, Section 5.2, Circuit-Switched Capabilities and Features where the MG handles both the media channels and the signaling channel

  – ANSI T1.619 and T1.619A support is required for PRI MLPP signaling per UCR 2008, Section 5.2, Circuit-Switched Capabilities and Features.

- **[Conditional: LSC, MFSS]** U.S. CAS trunks per UCR 2008, Section 5.2, Circuit-Switched Capabilities and Features where the MG handles both media and signaling on the same channel

  – CAS MLPP signaling is required per UCR 2008, Section 5.2, Circuit-Switched Capabilities and Features when U.S. CAS trunk is supported.

[Required] Media Gateway support for these TDM trunk groups shall be identical to the support for these trunk groups in DoD TDM PBXs, EOs, Tandem switches, and MFSs today, as specified in UCR 2008, Section 5.2, Circuit-Switched Capabilities and Features.

5.3.2.12.6 MG Interfaces to TDM Network Elements in Allied and Coalition Partner Networks

The appliance suppliers should support TDM trunk groups on their MG product that can interconnect with network elements in U.S. allied and coalition partner networks worldwide.

[Conditional] The MG shall support foreign country CCS7 trunk groups where the MG handles the media trunks, and the SG handles the signaling links:

1. For interconnection with an allied or coalition partner network, using foreign CCS7 from the network of the allied or coalition partner.

2. Support for MLPP using CCS7, per ITU-T Recommendation Q.735.3 is conditional on LSC and MFSS trunk groups, when these trunk groups are used to connect to an allied or coalition partner from an OCONUS ETSI-compliant country.

[Required] The MG shall support foreign country ISDN PRI trunk groups where the MG handles both the media channels and the signaling channel:

1. For interconnection with an allied or coalition partner network, using foreign ISDN PRI from the network of the allied or coalition partner.

2. Support for MLPP using ISDN PRI per ITU-T Recommendation Q.955.3 is required on LSC trunk groups, when these trunk groups are used to connect to an allied or coalition partner from a U.S. OCONUS ETSI-compliant country.

3. Support for MLPP using ISDN PRI per ITU-T Recommendation Q.955.3 is required on MFSS trunk groups, when these trunk groups are used to connect to an allied or coalition partner from a U.S. OCONUS ETSI-compliant country.

[Conditional] The MG shall support foreign country CAS trunk groups where the MG handles both media and signaling on the same channel:

1. For interconnection with an allied or coalition partner network, using foreign CAS trunk groups from the network of the allied or coalition partner.

2. Support for MLPP using CAS trunk signaling is not required on these trunk groups.

[Conditional] When appliance suppliers support allied and coalition partner network TDM trunk groups on their MG, MG support for these trunk groups shall be identical to the support for these trunk groups in DoD TDM PBXs, EOs, Tandem Switches, and MFSs today, as specified in UCR 2008, Section 5.2, Circuit-Switched Capabilities and Features.

5.3.2.12.7 MG Interfaces to TDM Network Elements in the PSTN in the United States

[Required] Each appliance MG shall support TDM trunk groups that can interconnect with network elements in the PSTN in the United States, including CONUS, Alaska, Hawaii, and U.S. Caribbean and Pacific Territories.

[Required] Each appliance MG shall support TDM trunk groups that can interconnect with the U.S. PSTN, using the following types of trunk groups:

1. **[Required]** U.S. National ISDN PRI, where the MG handles both the media channels and the signaling channel

    a. Required for U.S. PSTN network elements nationwide.
    b. Support for MLPP using ISDN PRI is not required on these trunk groups.

2. **[Conditional]** U.S. CAS trunks, where the MG handles both media and signaling on the same channel

    a. Conditional for U.S. PSTN network elements nationwide.
    b. Support for MLPP using CAS trunk signaling is not required on these trunk groups.

[Required] Media Gateway support for these TDM trunk groups to the U.S. PSTN shall be identical to the support for these trunk groups in DoD TDM PBXs, EOs, Tandem switches, and MFSs today, as specified in UCR 2008, Section 5.2, Circuit-Switched Capabilities and Features.

5.3.2.12.8 MG Interfaces to TDM Network Elements in OCONUS PTT Networks

The appliance supplier (i.e., LSC or MFSS supplier) should support TDM trunk groups on its MG product that can interconnect with network elements in foreign country PTT networks (OCONUS) worldwide.

[Required] The MG shall support foreign country ISDN PRI, where the MG handles both the media channels and the signaling channel:

1. For interconnection with a foreign country PSTN using foreign country ISDN PRI, from the country where the DoD user's B/P/C/S is located.

2. Support for ETSI PRI is required on LSC trunk groups, when the LSC is used in OCONUS ETSI-compliant countries.

3. Support for ETSI PRI is required on MFSS trunk groups, when the MFSS is used in OCONUS ETSI-compliant countries.

4. Support for MLPP using ISDN PRI is not required on the above trunk groups.

[Conditional] The MG shall support foreign country CAS trunks (where the MG handles both media and signaling on the same channel):

1. For interconnection with a foreign country PSTN, using foreign country CAS trunk groups from the country where the DoD User's B/P/C/S is located.

2. Support for MLPP using CAS trunk signaling is not required on foreign country CAS trunk groups.

[Conditional] If an appliance supplier supports foreign country PSTN TDM trunk groups on its MG, MG support for these trunk groups shall be identical to the support for these trunk groups in DoD TDM PBXs, EOs, Tandem switches, and MFSs today, as specified in UCR 2008, Section 5.2, Circuit-Switched Capabilities and Features.

5.3.2.12.9 MG Support for DoD CCS7 Trunks

[Conditional: LSC, MFSS] The MG shall support TDM trunk groups that are controlled by a separate CCA-to-SG signaling link that carries DoD CCS7 protocol. The MG shall support these TDM trunk groups, and the SG shall support DoD CCS7 signaling, conformant with the detailed DoD CCS7 trunk and protocol requirements in the following DoD and ANSI documents:

- UCR 2008, Section 5.2.2, Multilevel Precedence and Preemption, including
  - Section 5.2.2.4.3, Preempt Signaling, Common Channel Signaling Number 7 (CCS7)
  - Section 5.2.2.9, MLPP Common Channel Signaling Number 7 (CCS7)
  - UCR 2008, Section 5.2.4.6, Signaling - Common Channel Signaling Number 7 (CCS7)
  - ANSI T1.619-1992 (R2005
  - ANSI T1.619a-1994 (R1999

[Conditional: LSC, MFSS] When used in OCONUS ETSI-Compliant Countries, the MG shall also support DoD CCS7 trunk groups that support ITU-T Recommendation Q.735.3 for MLPP, consistent with UCR 2008, Section 5.2, Circuit-Switched Capabilities and Features.

[Conditional: LSC, MFSS] The MG shall support multiple CCS7 trunk groups, based on the needs of the DoD user deploying the appliance. The MG shall allow each CCS7 trunk group at the MG to connect to a different DoD TDM or IP network element (i.e., LSC, MFSS) based on the interconnection needs of the DoD user.

The MG shall have knowledge of which DoD TDM network element (i.e., SMEO, EO, MFS, MFSS EO, MFSS Tandem) or DoD IP network element (i.e., LSC, MFSS) each CCS7 MG trunk group is connected to.

5.3.2.12.10 MG Support for ISDN PRI Trunks

[Required] The MG shall support ISDN PRI trunk groups that carry the U.S./National ISDN version of the ISDN PRI protocol. The MG shall support these U.S. PRI trunk groups conformant with the detailed U.S. ISDN PRI requirements in the following DoD and ANSI documents:

1. UCR 2008, Section 5.2.9, Integrated Services Digital Network, including Table 5.2.9-4, PRI Access, Call Control, and Signaling, and Table 5.2.9-5, PRI Features.

    a. The "MFS" column in these tables shall apply to the MFSS.
    b. The "PBX1" column in these tables shall apply to the LSC.

2. UCR 2008, Section 5.2.2, Multi-Level Precedence and Preemption, including

    a. Section 5.2.2.4.2, Primary Rate Interface PRI

    b. Section 5.2.2.7, ISDN MLPP PRI

    c. ANSI T1.619-1992 (R2005)

    d. ANSI T1.619a-1994 (R1999)

[Required: MFSS, LSC for ETSI PRI – Conditional: MFSS, LSC for Other Foreign PRI] The appliance supplier (i.e., LSC or MFSS supplier) has the option of supporting one or more foreign versions of the ISDN PRI protocol on its product. As used here, the term "foreign version of ISDN PRI protocol" means the version of the PRI protocol that is used in the PSTN of a foreign country.

If an appliance supplier supports a foreign version of the ISDN PRI protocol on its product, the MG shall support ISDN PRI trunk groups that support the version of the PRI protocol that is used in the PSTN of a foreign country. The MG shall support these foreign PRI trunk groups conformant with the PRI protocol standards that are used in the PSTN of that foreign country. Examples of these standards include ETSI standards and ITU-T standards.

When used in OCONUS ETSI-compliant countries, the MG shall support ISDN PRI trunk groups that support ITU-T Recommendation Q.955.3 for MLPP, consistent with UCR 2008, Section 5.2, Circuit-Switched Capabilities and Features.

[Required] The MG shall support multiple U.S. PRI trunk groups, based on the needs of the DoD user deploying the appliance. The MG shall allow each U.S. PRI trunk group at the MG to connect to TDM EO and tandem components of the local MFSS, to a different U.S. PSTN TDM network element (e.g., PBX, TDM switch), to a different DoD TDM network element (e.g., PBX, TDM switch), or to a different DoD IP network element (e.g., LSC, MFSS), based on the interconnection needs of the DoD user.

The MG shall have knowledge of which U.S. PSTN TDM, DoD TDM, and DoD IP network element each U.S. PRI trunk group is connected to.

[Required: MFSS, LSC for ETSI PRI – Conditional: MFSS, LSC for Other Foreign PRI] When the appliance supplier supports foreign ISDN PRIs, the MG shall support multiple foreign PRI trunk groups, based on the needs of the DoD user deploying the appliance. The MG shall allow each foreign PRI trunk group at the MG to connect to a different foreign PSTN TDM, a different allied network element, or coalition partner TDM network element (e.g., PBX, switch) based on the interconnection needs of the DoD user.

The MG shall have knowledge of which foreign PSTN TDM, allied or coalition partner TDM network element each foreign PRI trunk group is connected to.

[Required] The MG shall support reception of ISDN PRI messages from the CCA MGC, and transmission of ISDN PRI messages to the CCA MGC.

The mechanisms that the MG uses to exchange ISDN PRI messages with the CCA MGC (i.e., use of vendor-proprietary protocols with security protection, or use of ISDN User Adaptation Layer protocols over Transport Layer Protocols over IPSec) are described in Section 5.3.2.12.12.6, MG Support for VoIP Interworking for ISDN PRI Trunks.

5.3.2.12.11 MG Support for CAS Trunks

[Conditional: LSC, MFSS] The MG shall support CAS trunk groups that carry the U.S. version of the CAS protocol. The MG shall support these U.S. CAS trunk groups conformant with the detailed CAS trunk and CAS trunk signaling requirements in the following DoD documents:

- UCR 2008, Section 5.2.4, Signaling, including

  - Section 5.2.4.3, Trunk Supervisory Signaling
  - Section 5.2.4.4, Control Signaling
  - Section 5.2.4.5, Alerting Signals and Tones

- UCR 2008, Section 5.2.2, Multilevel Precedence and Preemption, including

  - Section 5.2.2.4.1, Channel Associated Signaling

  - Section 5.2.2.9.6, DSN MLPP CCS7 IAM Called Party Number Format, including CAS-to-CCS Trunk Interworking Matrix (Line-to-Trunk and Trunk-to-Line), and Table 5.2.2-14, CAS-to-CAS Trunk Interworking Matrix (Trunk-to-Trunk)

[Conditional] The appliance supplier (i.e., LSC or MFSS supplier) has the option of supporting one or more foreign versions of CAS trunks and trunk signaling on its product. As used here, the term "foreign version of CAS trunks and trunk signaling," means the version of CAS trunks and trunk signaling that is used in the PSTN of a foreign country.

If an appliance supplier supports a foreign version of CAS trunks and trunk signaling on its product, the CCA IWF shall support the version of CAS trunks and CAS trunk signaling that is used in the PSTN of a foreign country, conformant with the CAS trunk standards that are used in the PSTN of that foreign country. Examples of these standards include ETSI CAS trunk standards and ITU-T CAS trunk standards.

The MG shall support multiple U.S. CAS trunk groups, based on the needs of the DoD user deploying the appliance. The MG shall allow each U.S. CAS trunk group at the MG to connect to a TDM EO and Tandem components of the local MFSS, to a different U.S. PSTN TDM network element (i.e., PBX, TDM Switch), to a different DoD TDM network element (i.e., PBX, TDM switch) or DoD IP network element (i.e., LSC, MFSS), based on the interconnection needs of the DoD user.

The MG shall have knowledge of which U.S. PSTN TDM, DoD TDM, or DoD IP network element (i.e., LSC, MFSS), each U.S. CAS trunk group is connected to.

[Conditional] When the appliance supplier supports foreign CAS trunk groups, the MG shall support multiple foreign CAS trunk groups, based on the needs of the DoD user deploying the appliance. The MG shall allow each foreign CAS trunk group at the MG to connect to a different foreign PSTN, allied or coalition partner TDM network element (e.g., PBX, TDM switch) based on the interconnection needs of the DoD user.

The MG shall have knowledge of which foreign PSTN TDM, allied or coalition partner TDM network element each foreign CAS trunk group is connected to.

[Conditional] The MG shall support reception of U.S. CAS trunk signaling sequences (i.e., Supervisory, Control, and Alerting) from the CCA MGC and transmission of U.S. CAS trunk signaling sequences to the CCA MGC.

[Conditional: LSC, MFSS] The MG shall support the requirements for MLPP Trunk Selection (Hunting) in the following sections of the UCR 2008. The MG shall support these MLPP Trunk Selection requirements on MG CAS trunk groups to DSN EOS and DSN MFSs. The MG shall also support these requirements on MG CAS trunk groups to DSN SMEOs, PBX1s, and PBX2s (when supported).

- UCR 2008, Section 5.2.2.2.3, MLPP Trunk Selection (Hunting)
- UCR 2008, Section 5.2.2.2.3.1, Hunt Sequence for Trunks
- UCR 2008, Section 5.2.2.2.3.1.1, ROUTINE Precedence Calls
- UCR 2008, Section 5.2.2.2.3.1.2, Precedence Calls Above ROUTINE Precedence
- UCR 2008, Section 5.2.2.2.3.1.2.1, Method 1
- UCR 2008, Section 5.2.2.2.3.1.2.2, Method 2

To meet the above requirements, the MG shall support the definitions of Precedence Level/Calling Area (PL/CA), classmarks, voice-grade trunk groups, data-grade trunk groups, route digit, direct route, alternative route, preemptive search, and friendly search from UCR 2008, Section 5.2, Circuit-Switched Capabilities and Features.

5.3.2.12.12 MG Requirements: VoIP Interfaces, Internal to an Appliance

The requirements in the following section assume that a supplier-specific Gateway Control Protocol is used between the MGC-MG interface. In this case, these requirements assume that the protocol layers below the application layer that carries the supplier-specific Gateway Control Protocol can be either industry-standard (as described below) or supplier-specific, which is outside the scope of this document.

When the H.248 Gateway Control Protocol is used over the open interface between the MG and the MGC, this open interface supports industry-standard protocol layers (i.e., physical, data link,

network, and transport) below the application layer that carries the Gateway Control Protocol. The support for these protocol layers are identified as an Objective.

5.3.2.12.12.1 MG Support for VoIP Interconnection at the Physical and Data Link Layers

[Required] The MG shall connect to the ASLAN of the appliance using the physical layer and data link layer protocols of the ASLAN. In this case, the MG shall appear to the MGC, EBC, and Appliance EIs as a physical layer and data link layer end point on a LAN switch in the ASLAN.

5.3.2.12.12.2 MG Support for VoIP Interconnection at the Network Layer

[Required] The MG shall connect to the ASLAN of the appliance using the IP as a network layer protocol. In this case, the MG shall appear to the MGC, EBC, and appliance EIs as an IP end point on an IP router on the ASLAN.

[Required] The MG shall support IP Version 4 (IPv4) as a Network Layer protocol, conformant with RFC 791.

[Required] The MG shall also support IPv6 as a Network Layer protocol, conformant with RFC 2460.

[Required] Conformant with UCR 2008, Section 5.3.5, IPv6 Requirements, the MG shall support dual IPv4 and IPv6 stacks (i.e., support both IPv4 and IPv6 in the same IP end point) as described in RFC 4213.

[Objective] When an open MGC-MG interface is used, the MG shall support IPSec for use with securing IP packets containing H.248 signaling messages and encapsulated ISDN PRI signaling messages. The MG support for IPSec shall be conformant with the appliance IPSec requirements in UCR 2008, Section 5.4, Information Assurance Requirements.

NOTE: The MG is not required to support IPSec for use in IP packets containing SRTP media streams for VoIP, FoIP, and MoIP calls.

5.3.2.12.12.3 MG Support for VoIP Interconnection at the Transport Layer

The following requirements apply when an open MGC-MG interface, which is an objective, is supported.

[Objective] When an open MGC-MG interface is used, the MG shall support transport of H.248 signaling messages and encapsulated ISDN PRI signaling messages using the TCP as a Transport Layer Protocol. In this case, the MG shall support TCP conformant with RFC 793.

[Objective] When an open MGC-MG interface is used, the MG shall support transport of H.248 signaling messages and encapsulated ISDN PRI signaling messages using the UDP as a Transport Layer Protocol. In this case, the MG shall support UDP conformant with RFC 768.

[Objective] When an open MGC-MG interface is used, the MG shall support transport of H.248 signaling messages and encapsulated ISDN PRI signaling messages using the SCTP as a Transport Layer Protocol. In this case, the MG shall support SCTP conformant with RFC 2960 and RFC 3309.

[Objective] When an open MGC-MG interface is used, the MG shall support a per-MG parameter that controls which of the three Transport Layer Protocols (i.e., UDP, TCP, or SCTP) are used to exchange H.248 signaling messages and encapsulated PRI signaling messages with the MGC. This parameter shall support the following values:

1. When this parameter is set to “TCP,” the MG shall exchange application layer messages with the MGC using TCP.

2. When this parameter is set to “UDP,” the MG shall exchange application layer messages with the MGC using UDP.

3. When this parameter is set to “SCTP,” the MG shall exchange application layer messages with the MGC using SCTP.

NOTE: The MG is not required to support Transport Layer Security (TLS) at the Transport Layer for securing H.248 signaling messages or encapsulated PRI signaling messages that are exchanged with the MGC using UDP, TCP, or SCTP. IPSec, which provides security at the Network Layer, is used in these cases instead of TLS, which provides security at the Transport Layer. Transport Layer Security is used elsewhere in the appliance to secure AS-SIP signaling messages on the appliance-to-EI and appliance-to-appliance interfaces, but it is not used to secure H.248 or PRI signaling messages on the MG-to-MGC interface.

NOTE: SCTP is used in other telecommunication industry documents as the Transport Layer Protocol for communication between VoIP softswitches and their MGs.

5.3.2.12.12.4 MG Support for VoIP Interconnection for Media Stream Exchange above the Transport Layer

[Required] The MG shall support exchange of VoIP media streams with appliance EIs, other appliance MGs, and the appliance EBC (and through the appliance EBC, with other EIs and MGs on other network appliances) using the following IETF-defined Media Transfer Protocols:

- SRTP, conformant with RFC 3711
- SRTCP, conformant with RFC 3711

[Required] The MG shall secure all VoIP media streams exchanged with appliance EIs, other appliance MGs, and the appliance EBC (and through the EBC, with EIs and MGs on other network appliances) using SRTP and SRTCP.

[Required] The MG shall use UDP as the underlying Transport Layer Protocol and IP as the underlying Network Layer Protocol, when SRTP is used for media stream exchange.

5.3.2.12.12.5 MG Support for VoIP Interconnection for Signaling Stream Exchange above the Transport Layer

[Objective] When an open MGC-MG interface is used, the MG shall support exchange of VoIP signaling streams with the appliance MGC. When the VoIP Signaling Streams contain ISDN PRI signaling messages at the Application Layer, the MG shall use the ISDN User Adaptation (IUA) Protocol between the Transport Layer and the Application Layer (the ISDN PRI signaling). The MG shall support the IUA Protocol consistent with RFC 4233.

NOTE: IUA is used in other telecommunication industry documents as the ISDN Adaptation Layer Protocol above the SCTP Transport Layer Protocol for ISDN communication between VoIP softswitches and their MGs.

[Required] When the VoIP Signaling Streams contain supplier-proprietary protocol messages instead of H.248 or ISDN PRI messages, the MG shall secure the proprietary protocol message exchange with the MGC using mechanisms that are as strong as or stronger than the use of IPSec to secure H.248 and PRI message exchange."

5.3.2.12.12.6 MG Support for VoIP Interworking for ISDN PRI Trunks

[Required] When an MG interworks a TDM call from an ISDN PRI trunk group with a VoIP session within the network appliance, the MG shall perform the following:

1. **[Required]** Convert between the ISDN media stream on the ISDN PRI B-Channel and the VoIP SRTP/Transport Layer/IP media stream within the appliance.

2. **[Objective]** Convert between ISDN signaling messages (ITU-T Recommendation Q.931 messages in Q.921 frames) on the ISDN PRI D-Channel and encapsulated ISDN signaling messages (ITU-T Q.931 messages in IUA frames) in a VoIP IUA/Transport Layer/IPSec signaling stream within the appliance.

NOTE: The method of converting PRI signaling into VoIP signaling and the method of conveying this information to and from the CCA are dependent on the Media Gateway Control Protocol used. Some protocols will not use encapsulation at all. If H.248 is used, signaling is encapsulated between the MG and CCA.

5.3.2.12.12.6.1 MG Support for VoIP Interworking for National ISDN PRI

[Objective] For U.S. ISDN PRI trunks carrying National ISDN PRI signaling, the MG shall interwork the National ISDN PRI Data Link Layer protocol (the National ISDN Version of ITU-T Q.921) with the IETF IUA protocol and the underlying Transport Layer and IPSec protocols.

5.3.2.12.12.6.2 MG Support for VoIP Interworking for CAS Trunks

The MG needs to read and understand incoming CAS signaling sequences, before translating them into MGC messages and sending them to the MGC using IP. Similarly, the MG has to understand and generate outgoing CAS signaling sequences, after receiving signaling messages from the MGC using IP, and translating the signaling messages into the appropriate CAS signaling sequences. The method of converting CAS signaling into VoIP signaling and the method of conveying this information to and from the CCA are dependent on the MG control protocol used. The H.248 protocol provides a standard way of doing this.

5.3.2.12.12.6.3 MG Support for VoIP Interworking for U.S. CAS Trunks

[Conditional] When an MG interworks a TDM call from a CAS trunk with a VoIP session within the appliance, the MG shall perform the following:

1. Convert between the TDM media stream on the CAS trunk and the VoIP SRTP/Transport Layer/IP media stream within the appliance.

2. Convert between the CAS signaling sequences on the CAS trunk and the VoIP signaling sequences within the appliance.

5.3.2.12.12.6.4 MG Support for VoIP Interworking for Foreign CAS Trunks

[Objective] When the MG supplier supports foreign CAS trunks, an MG shall interwork a TDM call from a CAS trunk with a VoIP Session within the appliance and shall perform the following:

1. Convert between the TDM media stream on the foreign CAS Trunk and the VoIP SRTP/Transport Layer/IP media stream within the appliance.

2. Convert between the CAS signaling sequences on the foreign CAS trunk and the VoIP signaling sequences within the appliance.

5.3.2.12.12.6.5 MG Support for VoIP Codecs for Voice Calls

The MG must support a set of internationally standard and DISN-standard VoIP codecs for use in converting TDM media streams to VoIP media streams, and in converting VoIP media streams to TDM media streams.

[Required] The MG shall support TDM Voice streams using the following:

- ITU-T 64 kbps G.711 u-law PCM over digital trunks
- ITU-T 64 kbps G.711 A-law PCM over digital trunks
- North American 56 kbps G.711 u-law PCM over digital trunks
- North American analog voice transmission over analog trunks on TDM trunk groups on the TDM side of the MG

[Required] The MG shall convert between North American 56 kbps G.711 (u-law PCM and ITU-T 64 kbps G.711 (u-law PCM in cases where North American 56 kbps TDM voice trunks are used on the TDM side of the MG.

[Required] The MG shall convert between North American analog voice transmission and ITU-T 64 kbps G.711 (μ-law PCM in cases where North American analog voice trunks are used on the TDM side of the MG.

[Conditional] When the MG supplier supports <u>analog</u> foreign CAS trunks, the MG shall support TDM voice streams using international (foreign) analog voice transmission over analog trunks on TDM trunk groups on the TDM side of the MG.

[Conditional] When the MG supplier supports analog foreign CAS trunks, the MG shall convert between international (foreign) analog voice transmission and ITU-T 64 kbps G.711 A-law PCM in cases where international (foreign) analog voice trunks are used on the TDM side of the MG.

5.3.2.12.12.6.5.1 Support for Uncompressed, Packetized VoIP per ITU-T G.711

[Required] The MG shall support uncompressed, packetized VoIP streams using ITU-T Recommendation G.711 (μ-law PCM and ITU-T G.711 A-law PCM (ITU-T Recommendation G.711, November 1998, plus Appendix I, September 1999, and Appendix II, September 2000) over the IP network on the VoIP side of the MG.

[Required] The MG shall packetize/depacketize G.711 media streams received or sent between its TDM side and its VoIP side.

[Required] The MG shall transport each packetized G.711 VoIP stream to and from the destination local EI, local MG, remote EI (via an EBC), or remote MG (via an EBC) using SRTP, UDP, and IP protocol layers on the VoIP side of the MG.

[Required] The MG shall support the use of uncompressed, packetized G.711 (μ-law and A-law VoIP media streams for both strategic and tactical applications. (Support for G.711 VoIP is necessary in tactical applications so that voice EIs in tactical environments can communicate with "G.711-only" voice EIs in strategic environments, and with G.711-based TDM voice devices in DoD, allied, and coalition partner networks, and with G.711-based TDM voice devices in U.S. and foreign PSTNs.)

5.3.2.12.12.6.5.2 Support for Compressed, Packetized VoIP per ITU-T G.72x

[Required] The MG shall support compressed, packetized VoIP streams using international standards via internal codecs over the IP network on the VoIP side of the MG, according to the following:

- ITU-T Recommendation G.723.1
- ITU-T Recommendation G.729, plus Erratum 1, and Annexes A through J, and Appendices I, II, and III.

The MG will use internal G.723.1 and G.729 codecs to perform this compression and decompression. These compressed VoIP codecs are referred to collectively as G.72x in this section.

[Required] The MG shall transport each packetized G.72x VoIP stream to and from the destination local EI, local MG, remote EI (via an EBC), or remote MG (via an EBC) using SRTP, UDP, and IP protocol layers on the VoIP side of the MG.

[Required] The MG shall support the use of packetized G.72x VoIP media streams for both tactical and strategic applications. (Support for G.72x may be necessary in strategic applications so that voice EIs in strategic environments, TDM voice devices in DoD, allied, and coalition partner networks, and TDM voice devices in U.S. and foreign PSTNs can communicate with "G.72x-only" voice EIs in tactical environments.)

5.3.2.12.12.6.6 MG Support for Group 3 Fax Calls

[Required] The MG shall support Group 3 Facsimile (G3 Fax) calls between TDM trunk, EI, MG, and EBC interfaces on the MG.

The MG shall support G3 Fax calls on TDM trunks for the following TDM trunk types:

- **[Conditional: LSC, MFSS]** DoD CCS7
- U.S. ISDN PRI
- U.S. CAS trunk (Conditional: when the MG supplier supports U.S. CAS trunks)
- Foreign ISDN PRI (Required: when the MG supplier supports ETSI PRI – Conditional: when the MG supplier supports other foreign ISDN PRIs)

[Required] The MG support for G3 Fax calls on the TDM trunk types listed above shall be identical to the support for G3 Fax calls on these trunk groups in DoD TDM PBXs, EOs, Tandem switches, and MFSs today, as specified in the UCR 2008, Section 5.2.2, Multilevel Precedence and Preemption.

[Required] The MG support for G3 Fax calls on the TDM trunk types listed above shall allow G3 Fax calls to the following:

1. Originate from an EI supporting G3 Fax or a G3 Fax device in a TDM network (i.e., DoD, U.S. or foreign PSTN, allied or coalition partner) and terminate on a G3 Fax device in a TDM network (i.e., DoD, U.S. or foreign PSTN, allied or coalition partner) or an EI supporting G3 Fax.

2. Originate from a G3 Fax device in a TDM network, and terminate to a G3 Fax device in a TDM network, where either TDM network can be DoD, U.S. or foreign PSTN, allied or coalition partner, when the voice network is used as a tandem network in between the originating TDM network and the terminating TDM network.

3. Originate from an IP EI supporting G3 Fax, and terminate to an IP EI supporting G3 Fax, where the two EIs can be on the same appliance or different appliances.

[Required] The MG shall support a mechanism to detect FoIP calls, to distinguish them from VoIP calls, and to treat them differently from VoIP calls. The MG shall support this FoIP detection mechanism on both TDM-to-FoIP calls (i.e., inbound from a TDM network to the IP appliance) and FoIP-to-TDM calls (i.e., outbound from the IP appliance to a TDM network).

[Required] The MG shall not rely on Called Number Screening or Calling Number Screening for detecting inbound TDM-to-FoIP calls or outbound FoIP-to-TDM calls.

In other words, the IP appliance administrator should not be required to maintain a list of "Calling and Called Fax Numbers" that are local to the IP appliance (representing FoIP end points within the appliance), and a list of "Calling and Called Fax Numbers" that are outside of the IP appliance (representing G3 Fax and FoIP end points outside of the appliance) to determine whether the call is a FoIP call.

[Required] The MG, in conjunction with the MGC, shall support two separate options for "Handling of FoIP calls within the IP appliance":

- Handle FoIP calls as G.711 VoIP calls (no compression or decompression).
- Handle FoIP calls as ITU-T T.38 FoIP calls (Fax Relay).

The MG and the MGC shall allow the IP appliance administrator to set the value of this option on a per-MG basis. Compression of FoIP calls via ITU-T G.723.1 or ITU-T G.729 should not be permitted.

[Required] In the case where an FoIP call enters the IP appliance MG over one TDM trunk, and then leaves the same IP appliance MG over another TDM trunk, the MG shall support the ability to interconnect the two-way TDM media streams from the first trunk directly with the two-way TDM media streams from the second trunk, without performing any TDM-to-FoIP and FoIP-to-TDM conversions on those two TDM media streams.

5.3.2.12.12.6.6.1 MG Option to "Handle FoIP Calls as G.711 VoIP Calls"

[Required] When the MG is configured to "Handle FoIP calls as G.711 VoIP Calls," the MG shall support the use of uncompressed, packetized G.711 (μ-law and A-law FoIP media streams for both strategic and tactical applications.

NOTE: Support for G.711 FoIP is necessary in tactical applications so that G3 Fax EIs in tactical environments can communicate with G3 Fax EIs in strategic environments, and with TDM G3 Fax devices in DoD, allied, and coalition partner networks, and with TDM G3 Fax devices in U.S. and foreign PSTNs.

[Required] When the MG is configured to "Handle FoIP calls as G.711 VoIP Calls," the MG shall handle FoIP calls within the appliance in exactly the same way that it handles G.711 VoIP calls within the appliance (e.g., the MG shall not allow compression of the media streams on these calls).

[Required] When the MG is configured to "Handle FoIP calls as G.711 VoIP Calls," the MG shall support uncompressed, packetized FoIP streams using ITU-T G.711 μ-law PCM and ITU-T G.711 A-law PCM over the IP network on the FoIP side of the MG.

[Required] When the MG is configured to "Handle FoIP calls as G.711 VoIP Calls," the MG shall transport each packetized G.711 FoIP stream to and from the local EI, local MG, remote EI (via an EBC), or remote MG (via an EBC) using SRTP, UDP, and IP protocol layers on the FoIP side of the MG.

MG Option to "Handle FoIP Calls as T.38 FoIP Calls"

[Required] When the MG is configured to "Handle FoIP Calls as T.38 FoIP Calls," the MG shall not handle FoIP calls within the appliance in the same way that it handles G.711 VoIP calls within the appliance. Instead, upon detection that a VoIP call request is actually a FoIP call request, the MG shall direct the FoIP call request to a "T.38 Fax Server" that is internal to the appliance.

NOTE: This "T.38 Fax Server" may be part of the MG, or part of the separate UFS Server in the appliance, or part of the separate media server in the appliance.

[Required] The T.38 Fax Server shall support the full set of procedures and protocols for Fax Relay in ITU-T Recommendation T.38.

[Required] The T.38 Fax Server shall support the full set of procedures and protocols for Group 3 Facsimile Reception and Transmission in ITU-T Recommendation T.4.

5.3.2.12.12.6.7 MG Support for Voice band Data Modem Calls

Support is needed for Voice band Data (VBD) modem calls within the IP network, in cases where

1. A VBD modem call enters the IP network at the MG of one IP appliance, and leaves the IP network at the MG of another IP appliance

2. A VBD modem call is originated or terminated by a VBD-capable EI served by an IP appliance

NOTE: This section on VBD modem calls has some similarity to Section 5.3.2.12.12.6.6, MG Support for Group 3 Fax Calls, on G3 Fax calls. The key differences are as follows:

1. This section addresses MoIP calls instead of FoIP calls

2. This section points to ITU-T V.150.1 for transport of VBD Modem calls over IP networks, where Section 5.3.2.12.12.6.6, MG Support for Group 3 Fax Calls, pointed to ITU-T T.38 for transport of Group 3 Fax calls over IP networks.

MoIP calls are included here to support EIs that contain VBD dial-up modems, Secure Telephone Units (STUs), and Secure Telephone Equipment (STEs). Each EI will include both of the following:

- A TA or IAD that connects the EI via IP to the local CCA, MG, and EBC

- A VBD device (i.e., dial-up modem, STU, or STE) that connects to this TA or IAD over either 1) a conventional two-wire analog interface, or 2) an equivalent interface within the EI

[Required] The MG shall support VBD modem calls between TDM trunks, Appliance Eis, and EBC interfaces.

In each of the previous cases, the MG shall support VBD modem calls on TDM trunks for the following TDM trunk types:

- **[Conditional: LSC, MFSS]** DoD CCS7

- U.S. ISDN PRI

- **[Conditional: when the MG supplier supports U.S. CAS trunks]** U.S. CAS trunk

- **[Required: when the MG supplier supports ETSI PRI – Conditional: when the MG supplier supports other foreign ISDN PRIs]** Foreign ISDN PRI

- **[Conditional: when the MG supplier supports foreign CAS trunks]** Foreign CAS trunk

[Required] The MG support for VBD modem calls on these TDM trunk groups shall be identical to the support for VBD modem calls on these trunk groups in DoD TDM PBXs, Eos, Tandem switches, and MFSs today, as specified in UCR 2008, Section 5.2.2, Multilevel Precedence and Preemption.

[Required] The MG support for VBD modem calls on these trunk groups shall allow VBD modem calls to originate or terminate between an IP EI supporting a VBD modem and a VBD modem device in a TDM network (i.e., DoD, U.S. or foreign PSTN, allied or coalition partner). This includes the case where both the calling and called VBD modems are on TDM networks and the IP-based network is used as a tandem network in between the originating TDM network and the terminating TDM network.

[Required] The MG shall support a mechanism to detect MoIP calls, to distinguish them from both VoIP and FoIP calls, and to treat them differently from both VoIP and FoIP calls. The MG shall support this MoIP detection mechanism on both TDM-to-MoIP calls (i.e., inbound from a TDM network to the IP appliance) and MoIP-to-TDM calls (i.e., outbound from the IP appliance to a TDM network).

The MG shall <u>not</u> rely on Calling Number Screening or Called Number Screening for detecting inbound TDM-to-MoIP calls or outbound MoIP-to-TDM calls.

In other words, the IP appliance administrator should not be required to maintain a list of "Calling and Called Modem Numbers" that are local to the IP appliance (i.e., representing MoIP end points within the appliance), and a list of "Calling and Called Modem Numbers" that are outside of the IP appliance (i.e., representing VBD modem and MoIP end points outside of the appliance) to determine whether the call is a MoIP call.

[Required] The MG, in conjunction with the MGC, shall support two separate options for "Handling of MoIP calls within the IP appliance" as follows:

- Handle MoIP calls as V.150.1 Voice Band Data calls (no compression or decompression).

- Handle MoIP calls as V.150.1 Modem Relay calls.

The MG, and MGC, shall allow the IP appliance administrator to set the value of this option on a per-MG basis. Compression of V.150.1 Voice Band Data calls via ITU-T Recommendations G.723.1 or G.729 should not be allowed.

[Required] When a MoIP call enters the IP appliance MG over one TDM trunk and then leaves the same IP appliance MG over another TDM trunk, the MG shall support the ability to interconnect the two-way TDM media streams from the first trunk directly with the two-way TDM media streams from the second trunk, without performing any TDM-to-MoIP and MoIP-to-TDM conversions.

MG Option to "Handle MoIP Calls as V.150.1 Voice Band Data Calls"

[Required] When the MG is configured to "Handle MoIP calls as V.150.1 Voice Band Data calls," the MG shall handle MoIP calls within the appliance in exactly the same way that it handles G.711 VoIP calls within the appliance (e.g., the MG shall not allow compression of the media streams on these calls).

[Required] When the MG is configured to "Handle MoIP calls as V.150.1 Voice Band Data calls," the MG shall support <u>uncompressed</u>, packetized MoIP streams using ITU-T G.711 (μ-law PCM and ITU-T G.711 A-law PCM over the IP network on the MoIP side of the MG.

[Required] When the MG is configured to "Handle MoIP calls as V.150.1 Voice Band Data calls," the MG shall transport each packetized G.711 MoIP stream to and from the local EI, local MG, remote EI (via an EBC), or remote MG (via an EBC) using SRTP, UDP, and IP protocol layers on the MoIP side of the MG.

MG Option to "Handle MoIP Calls as V.150.1 Modem Relay Calls"

[Required] When the MG is configured to "Handle MoIP Calls as V.150.1 Modem Relay Calls" and it detects that a VoIP call request is actually a MoIP call request, the MG shall direct the MoIP call request to a "V.150.1 Modem Relay Server" that is internal to the IP appliance.

NOTE: This V.150.1 Modem Relay Server may be part of the MG, or part of the separate UFS Server in the appliance, or part of the separate media server in the appliance.

[Required] The V.150.1 Modem Relay Server shall support the full set of procedures and protocols for V.150.1 Relay calls in ITU-T Recommendation V.150.1, “”plus Addendum 1.

[Required] Since the V.150.1 Modem Relay Server communicates with VBD modem devices in DoD networks, allied and coalition partner networks, and PSTNs worldwide, the V.150.1 Modem Relay Server shall support, at a minimum, the full set of procedures and protocols for VBD modem reception and transmission in the following ITU-T standards:

- ITU-T Recommendation V.90
- ITU-T Recommendation V.92

5.3.2.12.12.6.8 MG Support for SCIP over IP Calls

This section requires the MG to support additional functionality for Secure Communication Interoperability Protocol (SCIP) over IP calls. SCIP over IP calls are unique in the following ways:

a. In the TDM environment, SCIP calls can be placed between two SCIP phone end points. In the IP environment, SCIP over IP calls can be placed between two SCIP IP phone endpoints. A SCIP IP phone is an IP EI that supports SCIP and is served by an IP LSC.

It is possible to have a SCIP over IP call between two IP Eis supporting SCIP, a SCIP over IP call between an IP EI supporting SCIP and a TDM EI supporting SCIP, and (in the less common TDM-IP-TDM interworking case) a SCIP over IP call between two TDM Eis supporting SCIP.

In the IP-EI-to-TDM-EI case, it is necessary to have a SCIP-over-IP-capable MG in the call signaling and media paths to interwork between the IP and TDM sides of the SCIP call. In the TDM-IP-TDM case, it is necessary to have two SCIP-over-IP capable MGs in the call path.

2. As noted earlier, SCIP over IP streams are a subset of all possible V.150 Modem Relay streams. For the purposes of the UCR 2008, the term SCIP over IP is synonymous with the transmission of SCIP over V.150.1 Modem Relay. However, since MoIP calls can be supported using either V.150.1 Voice Band Data or V.150.1 Modem Relay, and SCIP over IP calls are only supported using V.150.1 Modem Relay, this section still makes a distinction between MoIP calls (i.e., for analog modems, STUs, and STEs) and SCIP over IP calls (for SCIP telephones). This distinction between SCIP over IP calls and MoIP calls may be revised in a later version of this document.

The SCIP over IP requirements in this section are similar to the MoIP requirements in Section 5.3.2.12.12.6.7.2, MG Option to "Handle MoIP Calls as V.150.1 Modem Relay Calls," even though SCIP over IP is based on V.150.1 Modem Relay. The two sets of requirements for "SCIP over IP calls" and "Modem over IP calls" may be merged into a single set of requirements for "Modem and SCIP over IP calls" in a later version of this document.

3. A "SCIP Phone," as used here, means a telephone that supports SCIP, and that is served by a line on a TDM switch in either the DSN or the commercial PSTN. A "SCIP over IP Phone," as used here, means an IP EI that supports SCIP, and that is served by an ASLAN on an IP LSC in the network.

   a. A "SCIP over IP Gateway," as used here, means an MG associated with an IP LSC in the network that supports signaling and media interworking for calls between SCIP Phones on TDM DSN switches (or TDM commercial switches) and SCIP over IP Phones on LSCs.

   NOTE: The SCIP over IP Gateway that supports this signaling and media interworking for a SCIP over IP call may be located at a different IP LSC than the IP LSC that serves the SCIP over IP Phone on that call.

   For example, the SCIP over IP call may be originated from a SCIP over IP Phone on a calling IP LSC and its associated IP MFSS, and then routed to another IP MFSS serving the called DSN number, which then points to an MFSS MG, a terminating TDM trunk group, a terminating TDM EO, and a destination TDM SCIP Phone. In this case, this MFSS MG is responsible for the SCIP-over-IP ⇔ SCIP-over-TDM interworking. But this MG is located on the MFSS associated with the called SCIP Phone, and the calling EI is located on the IP LSC on the separate MFSS associated with the calling SCIP over IP Phone.

   a. NOTE: The SCIP over IP Gateway that supports this signaling and media interworking may be located at a different IP appliance than the IP LSC that serves the SCIP over IP Phone on that call.

   For example, the SCIP over IP call can be originated from a SCIP over IP Phone on a calling IP LSC , routed to the IP softswitch serving this LSC, and then routed to another IP softswitch serving the called DSN number. At this second IP softswitch, the call is routed through the softswitch's MG to the TDM MFS at that location, and then routed through that MFS to a terminating TDM trunk group, a terminating TDM EO, and a destination TDM SCIP Phone. The second softswitch's MG is responsible for the SCIP-over-IP ⇔ SCIP-over-TDM interworking in this case. But this MG is located on the IP softswitch

serving the TDM EO associated with the called SCIP Phone, and the calling EI is located on the IP LSC on the separate IP softswitch associated with the calling SCIP Phone.

These additional requirements are based on the following U.S. Government SCIP over IP documents:

- SCIP-215
- SCIP-216

The first document gives requirements for support over "SCIP over IP Phones" on an IP network. The second document gives requirements for support over "SCIP over IP Gateways" on an IP network, where the gateways are based on the ITU-T V.150.1 Recommendation.

NOTE: The following SCIP over IP requirements for MGs are in addition to the previous MoIP requirements on MGs. The MoIP requirements on MGs are based on the commercial V.150.1 standard. The separate SCIP over IP requirements on MGs are based on the U.S. Government's SCIP-215 and SCIP-216 standards, which use the V.150.1 MER instead of V.150.1. This means that an MG that is SCIP over IP-compliant and MoIP-compliant needs to be capable of detecting SCIP over IP calls, of separately detecting MoIP calls, of providing V.150.1 MER-based treatment for the SCIP over IP calls, and of providing V.150.1-based treatment for the MoIP calls.

[Required] The MG shall support SCIP over IP calls between TDM trunks, IP Eis (SCIP over IP Phones), and EBC interfaces.

In each of the previous cases, the MG shall support SCIP over IP calls on TDM trunks for the following TDM trunk types:

- **[Conditional: LSC, MFSS]** DoD CCS7

- U.S. ISDN PRI

- **[Conditional: when the MG supplier supports U.S. CAS trunks]** U.S. CAS trunk

- **[Required: when the MG supplier supports ETSI PRI – Conditional: when the MG supplier supports other foreign ISDN PRIs]** Foreign ISDN PRI

- **[Conditional: when the MG supplier supports foreign CAS trunks]** Foreign CAS trunk

[Required] Media Gateway support for SCIP over IP calls on the TDM trunk types listed above shall be identical to the support for SCIP calls on these trunk groups in DoD TDM PBXs, Eos, Tandem switches, and MFSs today, as specified in UCR 2008, Section 5.2, Circuit-Switched Capabilities and Features.

[Required] Media Gateway support for SCIP over IP calls on the TDM trunk types listed above shall allow SCIP over IP calls to complete between an EI supporting SCIP and a SCIP device in a TDM network (i.e., DoD, U.S. or foreign PSTN, allied or coalition partner). This includes the case where both the calling and called SCIP Phones are on TDM networks, and the IP network is used as a tandem network in between the originating TDM network and the terminating TDM network.

[Required] The MG shall support a mechanism to detect SCIP over IP calls, to distinguish them from VoIP, FoIP, and MoIP Calls, and to treat them differently from VoIP, FoIP, and MoIP calls. The MG shall support this SCIP over IP detection mechanism on both TDM-to-SCIP over IP calls (i.e., inbound from a TDM network to the IP appliance) and SCIP over IP-to-TDM calls (i.e., outbound from the IP appliance to a TDM network).

The MG shall <u>not</u> rely on Called Number Screening or Calling Number Screening for detecting inbound TDM-to-SCIP over IP calls or outbound SCIP over IP-to-TDM calls.

In other words, the IP appliance administrator should not be required to maintain a list of "Calling and Called SCIP Phone Numbers" that are local to the IP appliance (i.e., representing SCIP over IP end points within the appliance), and a list of "Calling and Called SCIP Phone Numbers" that are outside of the IP Appliance (i.e., representing SCIP end points outside of the appliance) to determine whether or not the call is a SCIP over IP call.

[Required] The MG, in conjunction with the MGC, shall support two separate options for "Handling of SCIP over IP calls within the IP Appliance" as follows:

- Handle SCIP over IP calls as V.150.1 Voice Band Data calls (no compression or decompression)

- Handle SCIP over IP calls as V.150.1 Modem Relay/SCIP-216 calls

The MG, and MGC, shall allow the IP appliance administrator to set the value of this option on a per-MG basis. Compression of SCIP over V.150.1 Voice Band Data calls via ITU-T G.723.1 or ITU-T G.729 should not be allowed.

[Required] When a SCIP over IP call enters the IP appliance MG over one TDM trunk and then leaves the same IP appliance MG over another TDM trunk, the MG shall support the ability to

interconnect the two-way TDM media streams from the first trunk directly with the two-way TDM media streams from the second trunk, without performing any TDM-to-SCIP over IP and SCIP over IP-to-TDM conversions.

MG Option to "Handle SCIP over IP Calls as G.711 VoIP Calls"

[Required] When the MG is configured to "Handle SCIP over IP calls as V.150.1 Voice Band Data calls," the MG shall support uncompressed, packetized SCIP over IP streams using ITU-T G.711 (μ-law PCM and ITU-T G.711 A-law PCM over the IP network on the SCIP-over-IP side of the MG for both strategic and tactical applications.

[Required] When the MG is configured to "Handle SCIP over IP calls as V.150.1 Voice Band Data calls," the MG shall handle SCIP over IP calls within the appliance in exactly the same way that it handles G.711 VoIP calls within the appliance (e.g., the MG shall not allow compression of the media streams on these calls).

MG Option to "Handle SCIP over IP Calls as V.150.1 Modem Relay/SCIP 216 Calls"

[Required] When the MG is configured to "Handle SCIP over IP Calls as V.150.1 Modem Relay/SCIP 216 calls" and it detects that a VoIP call request is actually a SCIP over IP call request, the MG shall direct the SCIP over IP call request to a "V.150.1 Modem Relay/SCIP 216 Server" that is internal to the appliance.

NOTE: This V.150.1 Modem Relay/SCIP 216 Server may be part of the MG, or part of the separate UFS Server in the appliance, or part of the separate media server in the appliance. The role of the V.150.1 Modem Relay/SCIP 216 Server is to detect and process SCIP over IP calls, in conformance with the V.150.1 MER. The role of the V.150.1 Modem Server is to detect and process MoIP calls, in conformance with SCIP 261.

[Required] An MG that supports both SCIP over IP and MoIP should be capable of detecting SCIP over IP calls, of detecting MoIP calls, of providing SCIP 216-based treatment for the SCIP over IP calls, and of providing V.150.1-based treatment for the MoIP calls.

[Required] The V.150.1 Modem Relay/SCIP 216 Server shall support the full set of procedures and protocols for SCIP over IP Gateways in U.S. Government document SCIP-216.

[Required] The V.150.1 Modem Relay/SCIP 216 Server shall be fully interoperable with Eis that support the full set of procedures and protocols for SCIP over IP Phones in U.S. Government document SCIP-215.

5.3.2.12.12.6.9 MG Support for ISDN over IP Calls and 64kbps Clear Channel Data Streams

The MG is expected to support ISDN over IP calls and 64 kbps unrestricted digital information (i.e., 64 kbps Clear Channel Data) streams from ISDN interfaces, in addition to the other types of voice streams (i.e., FoIP, MoIP, SCIP over IP) described in the previous sections. For 64 kbps Clear Channel Data, the MG is not expected to perform any media processing for TDM ⇔ IP conversion other than packetization and depacketization. In this case, the MG's main role is to provide a transparent relay of a 64 kbps Clear Channel Data stream across the IP network using RTP packets. RFC 4040 specifies the SDP coding that should be used to support this scenario.

[Required] The MG shall support 64 kbps Clear Channel Data on TDM trunks for the following TDM trunk types:

- U.S. ISDN PRI
- **[Required: when the MG supplier supports ETSI PRIs – Conditional: when the MG supplier supports other foreign ISDN PRIs]** Foreign ISDN PRI

[Required] Media Gateway support for 64 kbps Clear Channel Data calls on the TDM trunk types listed above shall be identical to the support for 64 kbps Clear Channel Data on these trunk groups in DoD TDM PBXs, Eos, Tandem switches, and MFSs today, as specified in UCR 2008, Section 5.2.2, Multilevel Precedence and Preemption.

[Required] Media Gateway support for 64 kbps Clear Channel Data calls on the trunk types listed above shall allow 64 kbps Clear Channel Data calls to originate or terminate between an EI supporting 64kbps Clear Channel Data and an ISDN terminal supporting 64 kbps Clear Channel Data in a TDM network (i.e. DoD, U.S. or foreign PSTN, allied or coalition partner). This includes when both the calling and called ISDN terminals are on TDM networks and the IP network is used as a tandem network in between the originating TDM network and the terminating TDM network.

Required] The MG shall support a mechanism to detect 64 kbps Clear Channel Data calls, to distinguish them from VoIP, FoIP, MoIP, and SCIP over IP calls, and to treat them differently from VoIP, FoIP, MoIP, and SCIP over IP calls. The MG shall support this 64 kbps Clear Channel Data detection mechanism on both TDM-to-IP calls (i.e., inbound from a TDM network to the IP appliance) and IP-to-TDM calls (i.e., outbound from the IP appliance to a TDM network).

[Required] When a 64 kbps Clear Channel Data call enters the IP appliance MG over one TDM trunk and then leaves the same IP appliance MG over another TDM trunk, the MG shall support

the ability to interconnect the two-way TDM media streams from the first trunk directly with the two-way TDM media streams from the second trunk, without performing any TDM-to- IP and IP-to-TDM conversions.

[Required] The MG shall support the procedures and protocols for carrying 64kbps Clear Channel Data streams over IP, UDP, and RTP as described in RFC 4040“.” This shall include the coding of SDP Multipurpose Internet Mail Extension (MIME) parameters in the following manner (as excerpted from RFC 4040):

1. MIME media type name: audio

2. MIME subtype name: clearmode

3. Optional parameters: ptime, maxptime

    a. “ptime” gives the length of time in milliseconds represented by the media in a packet, as described in RFC 2327.

    b. “maxptime” represents the maximum amount of media, which can be encapsulated in each packet, expressed as time in milliseconds, as described in RFC 2327.

4. Encoding considerations: This type is only defined for transfer via RTP.

5. Parameter mapping considerations:

    a. The MIME type (audio) goes in the SDP “m=” attribute as the media name.

    b. The MIME subtype (clearmode) goes in the SDP “a=rtpmap” attribute as the encoding name.

    c. The optional parameters “ptime” and “maxtime” go in the SDP “a=ptime” and “a=maxptime” attributes, respectively.

5.3.2.12.12.6.10 MG Support for “Hair-Pinned” MG Calls

[Required] The MG shall support VoIP sessions between trunks on the same MG, including all combinations of TDM-call-legs and VoIP media end points.

[Required] In the TDM-to-TDM sessions, the MG shall not establish any IP, UDP/TCP/SCTP, RTP, or VoIP codec communication between the “call-originating” and “call-terminating” side of the MG. In addition, the MG shall not establish any TDM-to-VoIP media conversion or

VoIP-to-TDM media conversion on either side of the MG, for either direction of media transmission.

5.3.2.12.13 Echo Cancellation

5.3.2.12.13.1 MG Requirements for Echo Cancellation

The following basic requirements for MG Echo Cancellation are based on the commercial VoIP network Echo Cancellation requirements in Telcordia Technologies GR-3054-CORE (for the trunk gateway serving CCS7 trunk groups) and GR-3055-CORE (for the access gateway serving ISDN PRI and CAS trunk groups). These Echo Cancellation requirements may be updated in a later version of this section to align with the Echo Cancellation capabilities in UCR 2008, Section 5.2.12.1, Echo Cancellation Requirements.

5.3.2.12.13.1.1 Trunk Gateway Echo Cancellation

In any 2-wire or combination 2- and 4-wire telephone circuit, echo is caused by impedance mismatch. Echo cancellers (Ecs) are voice-operated devices placed in the 4-wire portion of a circuit, which may be an individual circuit path or a path carrying a multiplexed signal, and are used for reducing the echo by subtracting an estimated echo from the circuit echo.

The echo cancellers are assumed to be “half” echo cancellers, i.e., those in which cancellation takes place only in the send path due to signals present in the receive path. In particular, echo cancellation should be enabled for all voice calls. The ITU-T requirements for echo cancellation are specified in ITU-T Recommendation G.168.

5.3.2.12.13.1.1.1 Echo Control Design

An example MG echo control design is illustrated in Figure 5.3.2-16, Example IP Network Echo Control Design.

The EC function in MG A (controlled by LSC A) is pointing toward the PRI interface to the PBX, cancelling voice-frequency (VF) echo returning from the local PBX and the telephone end users behind that PBX. The EC function in MG B (controlled by LSC B) is pointing toward the CAS interface to the other PBX, canceling VF echo returning from the local PBX and the telephone end-users behind that PBX.

On a call between Party A and Party B, the EC function in MG A protects the “far-end party” (Party B) from excessive acoustical echo from the “near-end party” (Party A). Similarly, the EC function in MG B protects the “far-end party” (Party A) from excessive acoustical echo from the “near-end party” (Party B).

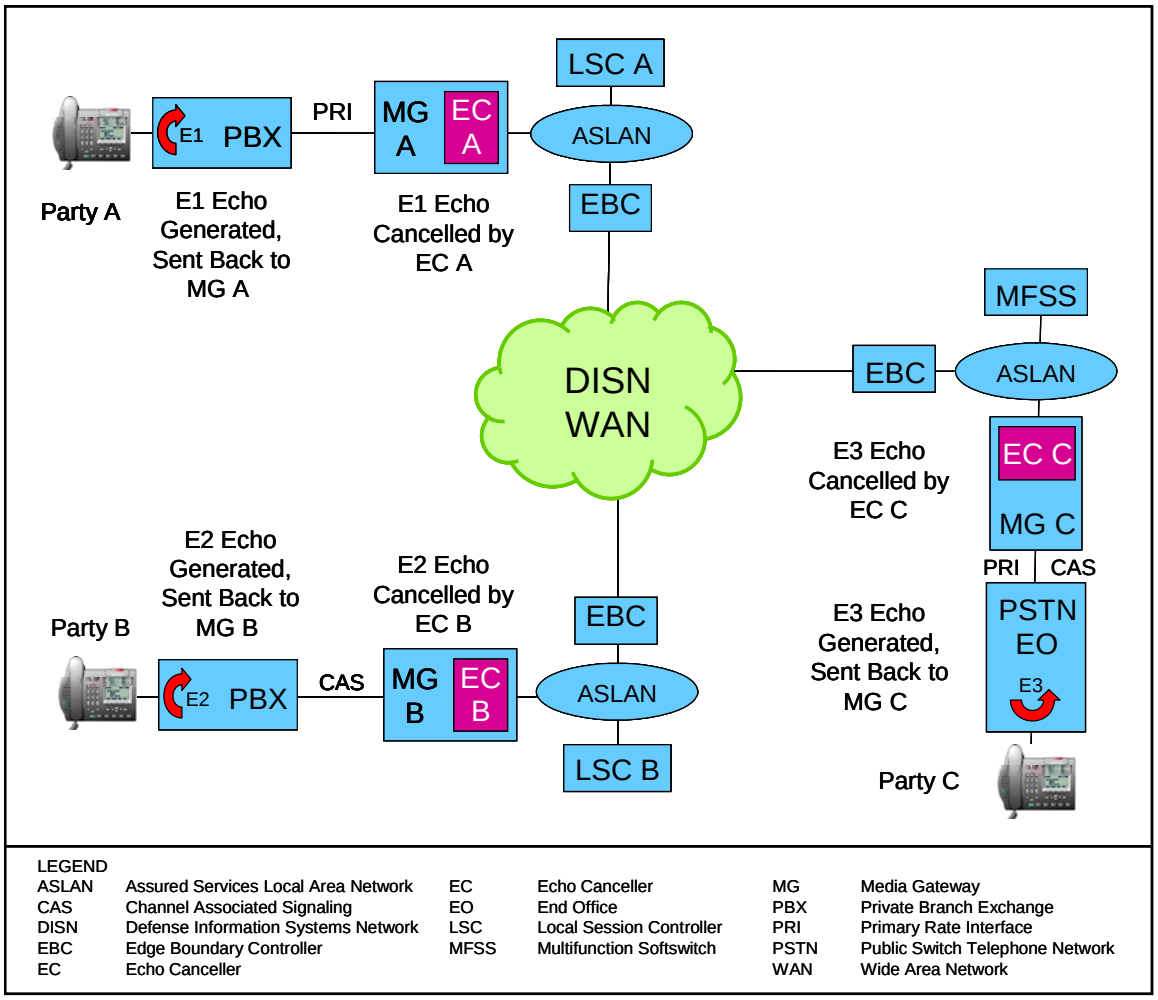


Figure 5.3.2-16. Example IP Network Echo Control Design

In addition, the EC function in MG C (controlled by the MFSS) is pointing toward the PRI or CAS interface to the PSTN EO, cancelling VF echo returning from that EO and the telephone end users behind that EO. On a connection between Party A and Party C (a PSTN-served customer), the EC function in MG 'C' is protecting the IP-network-served party (Party A) from excessive acoustical echo. Similarly, the EC function in MG A is controlling the VF echo returned toward the PSTN-served party (Party C).

5.3.2.12.13.1.1.2 Echo Cancellation Criteria

The echo path capacity of an echo canceller is the maximum echo path delay for which the device is designed to operate.

[Required] The MG shall provide an echo canceller capability with an echo path capacity (echo tail length) of at least 64 ms.

[Objective] It is an objective that the MG shall provide an echo canceller capability with an echo path capacity (echo tail length) of at least 128 ms.

According to ITU G.168, echo cancellers may remain active for several types of non-voice calls as well, in particular, for G3 Fax calls and VBD modem calls.

[Required] The MG shall provide echo cancellation for voice, G3 Fax, and VBD modem fax calls. (In the G3 Fax and VBD modem call cases, the MG shall provide echo cancellation if an "echo canceller disabling signal" is not sent by any end user's equipment on the G3 Fax or modem call.) This echo cancellation shall conform to the echo cancellation requirements specified in ITU-T Recommendation G.168.

[Required] Each MG echo canceller shall be equipped with an "echo canceller disabling signal" tone detector. This tone detector shall detect and respond to an in-band echo canceller disabling signal from an end user's G3 Fax, or VBD modem device. The echo canceller disabling signal detected shall consist of a 2100-Hertz (Hz) tone with periodic phase reversals inserted in that tone.

[Required] The MG tone detector/echo canceller disabler shall detect the echo canceller disabling signal" and disable the MG echo canceller when, and only when, that signal is present for G3 Fax or VBD modem.

Media Gateways serving DoD CCS7 trunk groups need to perform CCS7 Continuity Checks on individual trunks within those trunk groups. As part of these continuity checks, the MGs send and receive in-band tones on the individual CCS7 trunks. The presence of active echo cancellers on these trunk circuits interferes with the exchange of these in-band tones, and therefore interferes with the CCS7 Continuity Checks.

As a result, it is necessary for the MG to disable the echo cancellers on trunk circuits during CCS7 Continuity Checks, and to re-enable the echo cancellers on these circuits, after the CCS7 Continuity Checks have been completed.

[Conditional] The MG shall disable its MG echo canceller on an individual trunk circuit while a CCS7 Continuity Check is being run on that circuit,(without requiring that the echo canceller disabling signal be detected on either the send path or receive path on that circuit). .

5.3.2.12.14 MG Requirements for Clock Timing

[Required] The MG shall derive its clock timing from a designated T1 or PRI interface. See UCR 2008, Section 5.2, Circuit-Switched Capabilities and Features, for detailed requirements on how clock synchronization is supported in DSN TDM switches today.

5.3.2.12.15 MGC-MG CCA Functions

Per UCR 2008, Section 5.3.2.9.2.2, CCA MGC Component, the role of the MGC within the CCA is to:

1. Control all MGs within the LSC or MFSS.

2. Control all trunks (DoD CCS7, PRI, CAS) within each MG

    a. **[Required: LSC, MFSS]** Support for DoD ISDN trunks
    b. **[Conditional: LSC, MFSS]** Support for CAS trunks

3. Control all signaling and media streams on each trunk within each MG

4. Accept IP-encapsulated signaling streams from an SG or MG, and return IP-encapsulated signaling streams to the SG or MG accordingly.

    a. This approach is used for CCS7 signaling to/from an SG **[Conditional: in both the MFSS and LSC cases]**, and for PRI signaling to/from an MG.

5. Within the LSC, use either ITU-T H.248 or a supplier-proprietary protocol to accomplish these controls.

The MGC and the MG that it controls are Conditional – Tactical for the LSC (Conditional for tactical LSC deployments), but are required for the MFSS. The MGC and the MG that it controls are required for strategic LSC deployments.

[Required] The MGC within the CCA shall be responsible for controlling all the MGs within the LSC or MFSS.

[Required] The MGC within the CCA shall be responsible for controlling all the trunks (i.e., DoD CCS7, PRI, or CAS) within each MG within the LSC or MFSS.

[Required] The MGC within the CCA shall be responsible for controlling all media streams on each trunk within each MG.

[Required] The MGC within the CCA shall accept IP signaling streams from an MG, conveying received PRI or CAS trunk signaling. The MGC shall return IP signaling streams to the MG accordingly, for conversion to transmitted PRI or CAS trunk signaling.

[Conditional] When the appliance supplier supports foreign PRI or CAS trunks on its product, the CCA shall know which national variant of PRI or CAS signaling (e.g., ETSI/TTC/TTA; Germany/Japan/South Korea) the Foreign PRI or CAS Trunk supports.

[Required] Within the appliance (i.e., LSC or MFSS), the MGC shall use either ITU-T H.248 (Gateway Control Protocol Version 3) or a supplier-proprietary protocol to accomplish the MG, trunk, and media stream controls described previously.

5.3.2.12.15.1 MG Support for MGC-MG Signaling Interface

An open MGC-MG interface that involves ITU-T H.248 is optional in IOC (i.e., a closed MGC-MG interface can be used instead).

[Objective] It is desirable that the MGC use ITU-T H.248 for MG control.

[Required] The MGC protocol for MG control (MG Control Protocol) shall support the following:

1. Control message exchanges that are functionally equivalent to the control message exchanges used in ITU-T H.248.

2. Transport Layer functionality, including message sequencing, detection of message loss, and recovery from message loss, which are functionally equivalent to the sequencing, loss detection, and loss recovery mechanisms in TCP and SCTP.

3. Strong security for the exchange of gateway control messages and their underlying Transport Layer packets and Network Layer packets, so security controls (i.e., MG and MGC authentication, encryption and decryption of exchanged messages down to the Network Layer) are at least as strong as the IPSec security protection used when ITU-T H.248 is used as the MGC-MG protocol. This strong security shall be supported consistent with the H.248-over-IPSec requirements in UCR 2008, Section 5.4, Information Assurance Requirements.

[Required] The CCA and MGC shall be able to select the VoIP codec used by the MG to match the type of end point (i.e., EI, EBC) and service requested (i.e., uncompressed VoIP, compressed VoIP, FoIP, MoIP, SCIP over IP, or Video over IP).

[Required] The CCA and MGC shall ensure that both end points of each RTS session use the same RTS codec, for both directions of media stream transmission between the MG and the peer EBC, EI, or other MG. ("RTS session," as used here, includes VoIP sessions, FoIP sessions, MoIP sessions, SCIP over IP sessions, and Video over IP sessions.)

[Required] If the VoIP codec requested by a calling or called EI or EBC end point does not match any of the RTS codecs supported by a called or calling MG end point (based on CCA signaling with the EI or EBC, and MGC signaling with the MG), the CCA shall reject the RTS media "offer" from this calling or called end point, and indicate to the calling or called end point which RTS codec(s) should be used to send compatible RTS media to that MG.

"EBC end point," as used here, means a remote EI or MG end point served by another appliance elsewhere on the DISN WAN, whose signaling and media streams enter the Local Assured Services Domain from the DISN WAN via that Domain's EBC.

"RTS codec," as used here, includes VoIP codecs, FoIP codecs, MoIP codecs, SCIP over IP codecs, and Video over IP codecs.

"RTS media," as used here, includes VoIP media, FoIP media, MoIP media, SCIP over IP media, and Video over IP media.

[Required] Since the CCA and MGC support selection and negotiation of VoIP codecs on calls to and from MGs, the CCA and MGC shall at a minimum support the following set of ITU-T standard VoIP codecs:

- ITU-T Recommendation G.711, both North American (μ-law and international A-law variants
- ITU-T Recommendation G.723.1
- ITU-T Recommendation G.729

5.3.2.12.15.2 MG Support for Encapsulated National ISDN PRI Signaling

[Required] The MG shall transport ISDN PRI signaling messages between the MG and the MGC. In this case, the MG shall support the following:

- Transparent passing of ISDN PRI messages between the MG and MGC
- Preservation of correct message sequences, in both directions of transmission

- Detection of message loss and recovery from message loss (e.g., by retransmission of lost messages), in both directions of transmission

- Detection of message errors and correction of message errors (e.g., by retransmission of errored messages), in both directions of transmission

- Securing of ISDN PRI messages using MG and MGC encryption, in both directions of transmission

The MG shall support all these capabilities over the supplier-specific protocol so the resulting exchange of ISDN PRI messages (and security of exchanged ISDN PRI messages) is identical to what would occur if IUA, UDP/TCP/SCTP, and IPSec were used.

When an open protocol is used to support the transport of ISDN PRI signaling messages between the MG and MGC, the following objective applies:

1. **[Objective]** The MG shall use the following protocol stack to support encapsulation of ISDN PRI signaling messages sent from the MG to the MGC, and de-encapsulation of ISDN PRI signaling messages sent from the MGC to the MG when an open interface is used:

    a. National ISDN PRI signaling messages, as described in Telcordia Technologies SR-4994.

    b. IUA frames, where IUA shall be supported as defined in RFC 4233.

    c. One of the following IETF-standard Transport Layer Protocols:

        (1) TCP
        (2) UDP
        (3) SCTP

    d. IPSec packets, secured using mutual MGC and MG encryption, at the IP Network Layer. This encryption shall be performed consistent with the MGC and MG encryption of encapsulated ISDN PRI messages described in UCR 2008, Section 5.4, Information Assurance Requirements.

5.3.2.12.15.3 MG Support for Mapped CAS Trunk Signaling, using H.248 Packages for MF and DTMF Trunks

[Conditional] The MG shall transport the CAS trunk signaling between the MG and the MGC. In this case, the MG shall still support the following:

- Transparent passing of CAS trunk signaling (or indications of CAS trunk signaling) using supplier-specific messages between the MG and MGC
- Preservation of correct message sequences, in both directions of transmission
- Detection of message loss and recovery from message loss (e.g., by retransmission of lost messages), in both directions of transmission
- Detection of message errors and correction of message errors (e.g., by retransmission of errored messages), in both directions of transmission
- Securing of supplier-specific messages using MGC and MG encryption, in both directions of transmission

The MG shall support all these capabilities over the supplier-specific protocol so the resulting exchange of CAS trunk signaling (and security of the messages carrying the CAS trunk signaling) is identical to what would occur if H.248, UDP/TCP/SCTP, and IPSec were used.

When an open protocol is used to support the transport of CAS signaling messages between the MG and MGC, the following requirements apply:

1. **[Conditional]** The MGC shall use the following protocol stack to support encapsulation of CAS trunk signaling sent from the MG to the MGC, and de-encapsulation of CAS trunk signaling sent from the MGC to the MG:

   a. ITU-T H.248 signaling messages carrying indications of MGC-to-MG and MG-to-MGC signaling for DTMF trunks and MF trunks. This H.248 signaling message shall include DTMF, MF, and CAS information from the following H.248 packages:

      (1) Basic DTMF Generator Package (from ITU-T H.248.1)
      (2) DTMF Detection Package (from ITU-T H.248.1)

      (3) Multi-Frequency Tone Generation and Detection Packages (from ITU-T H.248.24)

(4) Basic CAS Packages (from ITU-T H.248.25)

(5) International CAS Packages (from ITU-T H.248.28)

b. One of the following IETF-standard Transport Layer Protocols:

(1) TCP
(2) UDP
(3) SCTP

c. IPSec packets, secured using mutual MG and MGC encryption, at the IP Network Layer. This encryption shall be performed consistent with the MG and MGC encryption of H.248 messages described in UCR 2008, Section 5.4, Information Assurance Requirements.

[Conditional] The MGC shall support the following set of CAS trunk signals, consistent with their use in Telcordia Technologies GR-3055-CORE (for the MG) and GR-3051-CORE (for the MGC):

1. Seizure Signal. A signal, sent from the originating switching system (or MGC/MG) to the terminating switching system (or MGC/MG), that defines the transition from the trunk idle state to the trunk seizure state.

2. Addressing Control Signal. A signal that marks the transition from the seizure state to the addressing state. Two addressing control methods of operation exist:

   a. Wink Start. After receiving a seizure signal, the terminating switching system (or MGC/MG) sends an off-hook signal with a defined duration (wink) to indicate that it is prepared to receive address information.

   b. Immediate-Dial. No addressing control signal is used. The originating switching system (or MGC/MG) waits for a specified time after sending a seizure signal before sending the first address digit.

3. Answer Signal. A signal that defines the transition from the call-processing state to the communications state, and persists for the duration of the communications state.

4. Transfer of address digits using DTMF signaling for DTMF trunk groups.

5. Transfer of address digits using MF signaling for MF trunk groups.

6. Disconnect Signal. A signal that defines the transition from the call-processing state or the communications state to the idle state.

5.3.2.12.15.4 MG Support for Glare Conditions on Trunks

As defined in UCR 2008, Section 5.2, Circuit-Switched Features and Capabilities, "Glare occurs when both interfaces of switching systems connected to the same inter-switching-system facility (trunk) apply a seizure signal at approximately the same time." In this section, at least one of the "switching systems connected to the same inter-switching-system facility (trunk)" is an LSC or MFSS MG, as represented by a CAS trunk group.

NOTE: MG support for CAS trunks is conditional...

[Conditional: LSC, MFSS] The MG shall provide functions required to handle a glare situation on CAS trunks as specified in Telcordia Technologies GR-506-CORE, Section 11.5, Glare Resolution.

5.3.2.12.15.5 MGC and IWF Treatments for PRI-to-AS-SIP Mapping for MLPP

[Required] In conjunction with the IWF, the MGC shall support the following mapping of PRI-signaled MLPP information to AS-SIP signaled RPH information, on calls or sessions that involve MLPP and PRI/AS-SIP interworking:

1. The four Network Identity (NI) digits received in Octets 5 and 6 of the ISDN PRI Precedence Level IE shall be mapped to the "Network domain" subfield of the "Namespace" field in the AS-SIP RPH.

2. The "MLPP Service domain" information received in octets 7, 8, and 9 of the ISDN PRI Precedence Level IE shall be mapped to the "Precedence domain" subfield of the "Namespace" field in the AS-SIP RPH.

3. The "Precedence level" information received in bits 4 through 1 of octet 4 of the ISDN PRI Precedence Level IE shall be mapped to the "Resource priority (r-priority)" field in the AS-SIP RPH.

In the absence of a received ISDN PRI Precedence Level IE:

1. **[Required]** The MGC/IWF shall use a default "Network domain" value of "dsn" in the "Namespace" field in the AS-SIP RPH.

2. **[Required]** The MGC/IWF shall use a default "Precedence domain" value of "000000" in the "Namespace" field in the AS-SIP RPH.

3. **[Required]** The MGC/IWF shall use a default "Resource priority" value of "0 (Routine)" in the "r-priority" field in the AS-SIP RPH.

[Required] The MGC/IWF shall support mapping of the four NI Digits to the "Network domain" subfield of the "Namespace" field in the RPH as follows:

1. For the FY08-to-FY12 time frame, the MGC/IWF shall always use the value "dsn" in the "Network domain" subfield, independent of the NI Digits received.

2. For the FY12-and-onwards time frame, the MGC/IWF shall first check the NI digits translation table that is configured in the CCA for the PRI on which the Precedence Level IE was received. Table 5.3.2-46, NI Digit Translation Table, shall contain a set of valid NI digit sequences (e.g., 0000, 0001, 0002) that the MGC/IWF will accept on that PRI, and the corresponding set of RPH "Network domain" values (e.g., "dsn", "drsn", "dod", "nato") that the valid NI digit sequences map to.

Table 5.3.2-46. NI Digit Translation Table

LEVEL IE NI DIGITS	OUTPUT SIP RPH NETWORK DOMAIN
0000	dsn
0001	drsn
0002	dod
0003	nato
LEGEND IE Information Element NI Network Identifier	 RPH Resource Priority Header SIP Session Initiation Protocol

3. For the FY12-and-onwards time frame, the MGC/IWF shall set the value in the "Network domain" subfield to the "Network domain" value that is configured for the received NI digits in this translation table for the PRI in question.

If the received NI digits are not included in the translation table for this PRI, the MGC/IWF shall use a default "Network domain" value of "dsn" for this call.

[Required] The MGC/IWF shall support mapping of the PRI "MLPP Service domain" field to the "Precedence domain" subfield of the "Namespace" field in the RPH as follows:

1. The MGC/IWF shall convert the three octet hexadecimal values from the three-octet PRI "MLPP Service domain" field into a text string consisting of six text characters. The MGC/IWF shall use this six-character string as the "Precedence domain" subfield of the "Namespace" field in the RPH. For example:

- For the FY12-and-onwards time frame, the MGC/IWF shall set the NI Digits value to the NI Digits value that is configured for the received "Network domain" value in this translation table for the PRI in question.

2. If the received "Network domain" value is not included in the translation table for this PRI, the MGC/IWF shall use a default NI Digits value of "0000" for this call.

[Required] The MGC/IWF shall support mapping of the "Precedence domain" subfield of the "Namespace" field in the RPH to the PRI "MLPP Service domain" field as follows:

- The MGC/IWF shall replace the six-character text string from the RPH "Precedence domain" with the hexadecimal-encoded number "000000" in the three-octet PRI "MLPP Service domain" field. The MGC/IWF shall use this three-octet hexadecimal-encoded number, "000000," in the "MLPP Service domain" field in the ISDN PRI Precedence Level IE.

[Required] The MGC/IWF shall support mapping of the "Resource Priority" field of the RPH to the PRI "Precedence Level" field (a semi-octet) as follows:

1. If the "Network domain" field in the RPH is "dsn," then the MGC/IWF shall set the "Precedence Level" field in the ISDN PRI Precedence Level IE according to Table 5.3.2-47, Mapping of RPH r-priority Field to PRI Precedence Level Value.

2. If the "Network domain" field in the RPH is any value other than "dsn," then the MGC/IWF shall set the "Precedence Level" field in the ISDN PRI Precedence Level IE to the value of "0 1 0 0" (4, meaning Routine).

5.3.2.12.15.6 MGC Support for MG-to-MG Calls

[Required] The MGC shall be able to support multiple MGs.

[Required] The MGC shall support VoIP sessions between trunks on the same or different MGs of the MGC, without requiring them to route to a VoIP EI on the appliance, or requiring them to be routed through the appliance's EBC to the DISN WAN.

Table 5.3.2-47. Mapping of RPH r-priority Field to PRI Precedence Level Value

MLPP PRECEDENCE LEVEL	PRI PRECEDENCE LEVEL VALUE (DECIMAL NUMBER, SEMI-OCTET)	RPH R-PRIORITY FIELD (SINGLE CHARACTER, TEXT)
ROUTINE	4	0
PRIORITY	3	2
IMMEDIATE	2	4
FLASH	1	6
FLASH-OVERRIDE	0	8
Spare, not used	5 through 15	0

[Required] For MG-to-MG sessions where a single MG is involved, the MGC shall handle MG-to-MG calls within a single MG as TDM-to-TDM calls that are local to the MG, rather than as TDM-to-VoIP-to-TDM calls that use VoIP resources within the MG and other appliance components. In this case, the MGC shall instruct the MG to locally connect the TDM media from the one TDM leg of the call to the TDM media from the other TDM leg of the call, for both directions of TDM media transmission.

5.3.2.13 Signaling Gateway Requirements

5.3.2.13.1 Introduction

The purpose of this section is to provide Generic System Requirements (GSR) for the Signaling Gateway (SG). The SG is a conditional functional component in the MFSS and LSC.

The scope of these SG requirements covers CCS7 signaling connectivity for Defense Switched Network (DoD) CCS7.

5.3.2.13.1.1 SG Requirements Assumptions

The SG functional requirements are based on the following key assumptions:

1. The SG together with the CCA is modeled as a Signaling End Point in the CCS7 network.

2. The SG is assigned a unique Signaling Point Code (SPC) in the CCS7 network.

3. The SG connects to a pair of mated STPs in the CCS7 network using two Access Link Sets (A-link sets),

4. The SG supports MTP2 links (56-kbps or 64 kbps based on the interconnected CCS7 network).

5. Depending on vendor-specific implementation, the SG can be physically combined with the CCA or physically separated and located in a different location from the CCA.

6. The requirements in this section assume that the SG and CCA are part of the same solution platform.

7. The SG-CCA interface is assumed to be an internal, unexposed interface. This interface could be based on proprietary protocols or standard protocols defined for such an interface (e.g., IETF SIGTRAN Adaptation protocols over the SCTP/IP).

8. An MFSS may support multiple SGs for reliability and scalability.

5.3.2.13.1.2 SG Primary Function and Interfaces

In general, the primary function of the SG is to provide CCS7 signaling interface functions on the CCS7 network side, provide connectivity to IP transport, and relay CCS7 signaling messages to and from the CCA. These functions can be grouped based on the two main interfaces of the SG:

- SG-CCS7 Interface (circuit switched side)
- SG-CCA Interface (IP side)

The SG-CCS7 network interface provides CCS7 link and network connectivity functions facilitating end-to-end exchanges of CCS7 call control (i.e., ISUP – **[Required]**) and services control (e.g., TCAP – **[Conditional]**) signaling messages between the CCA and Signaling End Points (SEPs) in interconnected TDM networks. The SG will provide signaling connectivity with DoD CCS7 networks.

The SG-CCA interface provides transport functions to convey CCS7 information between the SG and CCA functional components.

5.3.2.13.2 Role of the SG in Appliances

The SG described in the following requirements is part of the Session Control and Signaling (SCS) functions of the MFSS and LSC products. The primary function of the SG is to provide the necessary functions for CCS7 signaling connectivity to circuit-switched networks. The SG together with the CCA and the MG will provide the systems and functions necessary for interconnection between the IP packet network and circuit-switched network. Specifically, the

SG will provide the necessary functions to facilitate call and service control signaling for CCS7 control trunks (bearer connections) to the MG.

5.3.2.13.2.1 MFSS Functional Reference Model

Figure 5.3.2-17, Functional Reference Model – MFSS, shows the functional reference model for the MFSS. Shown are the functional components of the MFSS (e.g., SG, CCA, MGC, and MG) and the relationships between the various components. For a description of the different functional components of the MFSS, please refer to UCR 2008, Section 5.3.2.8, Multifunction Softswitch.

5.3.2.13.3 SG's Role – Interacting with MFSS Functions and Elements

5.3.2.13.3.1 End Office and Tandem Side of the MFSS

The TDM side of the MFSS supports EO and Tandem Switch functionality. The EO and Tandem functions in the MFSS provide circuit-switched network functions that terminate CCS7/TDM trunks, ISDN lines, and analog lines.

The SG interacts with the EO and Tandem functions through industry-standard external interfaces (e.g., CCS7 signaling links and TDM media trunks, as shown in the MFSS functional model), or through internal interfaces that use protocols that are specific to an appliance supplier's solution.

5.3.2.13.3.2 SG, CCA, and IWF Relationships

The role and functions of the CCA including the IWF are described in UCR 2008, Section 5.3.2.9, Call Connection Agent. The SG does not provide call processing or call control and service control functions. The primary role of the SG is to transfer the call control and service control signaling messages to the CCA of the MFSS where these functions are provided. The SG interacts with the CCA component of the MFSS as follows:

1. Transfers CCS7 call and service control signaling messages to and from the CCA in support of DoD CCS7 trunk connections supported by the MG of the MFSS. The SG is responsible for conveying the CCS7 call control signaling and service control signaling to the CCA IWF for processing. The CCA IWF in the MFSS supports the necessary interworking of the DoD CCS7 protocols with AS-SIP, and with ISDN PRI and CAS protocols for TDM trunk signaling.

2. Needs to support consistent procedures for encapsulation and de-encapsulation of DoD CCS7 messages in IP packets for transport to and from the CCA in the MFSS.

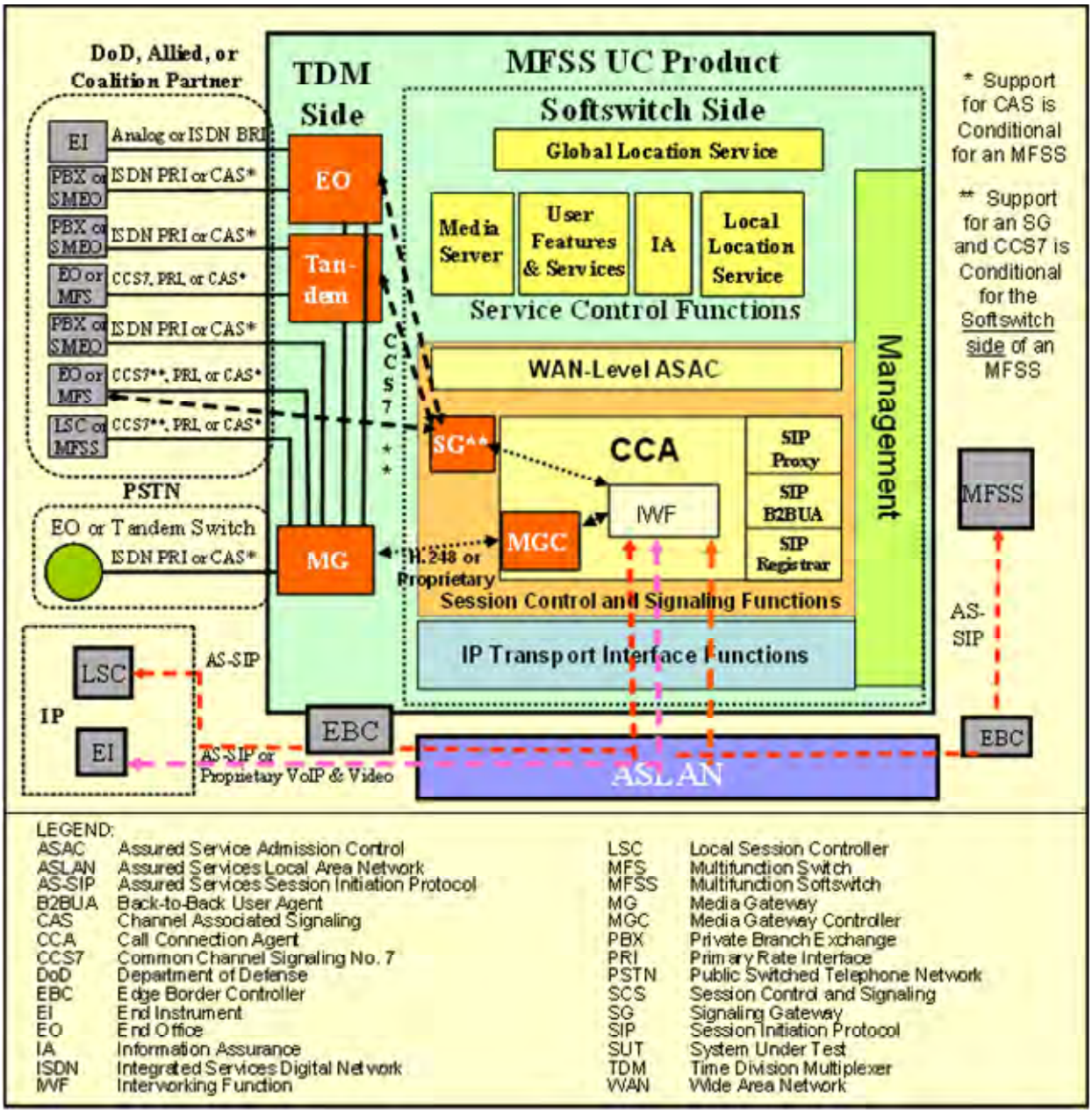


Figure 5.3.2-17. Functional Reference Model – MFSS

5.3.2.13.3.3 CCA Interactions with SG

[Conditional: LSC, MFSS] The role of the CCA with respect to the SG in the appliance is as follows:

- Controls all SGs within the appliance
- Controls all signaling links (DoD CCS7) within each SG.

[Conditional: LSC, MFSS] The CCA shall be responsible for controlling all of the SGs within the MFSS and LSC. (NOTE: This covers cases where there is a single SG within the appliance, and cases that are more complex where there are multiple SGs within the appliance.)

[Conditional: LSC, MFSS] The CCA shall be responsible for controlling each signaling link within each SG within the MFSS or LSC.

[Conditional: LSC, MFSS] The CCA shall be responsible for controlling the DoD CCS7 signaling stream(s) within each signaling link within each SG.

[Conditional: LSC, MFSS] Within the appliance (the MFSS and LSC), the CCA shall use either an IETF-standard set of CCS7-over-IP protocols or a supplier-proprietary protocol to accomplish the previously discussed SG, signaling link, and signaling stream controls.

5.3.2.13.3.3.1 CCA Support for CCA SG Signaling Interface

[Objective] It is desirable that the CCA use IETF-standard CCS7-over-IP protocols for SG control. In this case, the CCA shall transport the CCS7 messages that it exchanges with the SG using one of the following IETF-standard Transport Layer Protocols:

- TCP
- UDP or
- SCTP

[Conditional] When the CCA uses IETF-standard CCS7-over-IP protocols for SG control, the CCA shall secure the CCS7-over-IP information that it exchanges with the SG using IPSec at the IP Network Layer, consistent with the IA requirements in UCR 2008, Section 5.4, Information Assurance Requirements.

[Conditional: LSC, MFSS] For SG control, the CCA shall

1. Support Transport Layer functionality, including message sequencing, detection of message loss, and recovery from message loss, which are functionally equivalent to the sequencing, loss detection, and loss recovery mechanisms in TCP and SCTP.

2. Support strong security for the exchange of CCS7 messages and any underlying Transport Layer packets and Network Layer packets, so the security controls (SG and CCA authentication, encryption, and decryption of exchanged messages down to the Network Layer) are at least as strong as the security controls used when UDP/TCP/SCTP and IPSec are used to transport CCS7 messages over IP. This strong security shall be supported

consistent with the IPSec requirements in UCR 2008, Section 5.4, Information Assurance Requirements.

[Conditional: MFSS, LSC] When CCS7 ISUP messages are transported between the CCA and SG, the CCA shall support

- Transparent passing of CCS7 ISUP messages between the SG and CCA
- Preservation of correct message sequences, in both directions of transmission
- Detection of message loss and recovery from message loss (e.g., by retransmission of lost messages), in both directions of transmission
- Detection of message errors and correction of message errors (e.g., by retransmission of errored messages), in both directions of transmission
- Securing of CCS7 ISUP messages using CCA and SG encryption, in both directions of transmission

The CCA shall support all these capabilities so the resulting exchange of CCS7 ISUP messages and security of exchanged CCS7 ISUP messages is identical to what would occur if IETF-standard CCS7-over-IP protocols were used.

5.3.2.13.3.3.2 CCA Support for SG-to-CCA-to-SG Signaling Paths

[Conditional: LSC, MFSS] The CCA shall be able to support multiple SGs.

[Conditional: LSC, MFSS] Since the CCA supports per-call ISUP signaling that enters the appliance on one SG signaling link and then leaves the appliance on another SG signaling link, the CCA shall support SG-to-CCA-to-SG ISUP signaling paths within the appliance, which link per-call ISUP signaling on a signaling link on one SG with per-call ISUP signaling on a signaling link on the same or another SG.

5.3.2.13.3.4 SG Interactions with Appliance Management Functions

The Management function in the MFSS supports functions for MFSS FCAPS management and audit logs. Details on FCAPS management and audit logs for the SG function in the MFSS are covered in UCR 2008, Section 5.3.2.18.2, Management Requirements of the SG Function.

The SG interacts with the MFSS Management function by:

1. Making changes to its configuration in response to commands from the Management function that request these changes.

2. Returning information to the Management function on its FCAPS, in response to commands from the Management function that request this information.

3. Sending information to the Management function on a periodic basis (e.g., on a set schedule), keeping the Management function up-to-date on SG activity. An example of this update would be a periodic transfer of audit reports from the SG to the Management function, so that the Management function could either store the report locally or transfer it to a remote NMS for remote storage and processing.

5.3.2.13.4 SG Protocol Design

Figure 5.3.2-18, SG Protocol Design, shows the protocol design for the SG and the relationship with the CCA and signaling points in the interconnected CCS7 network.

The SG can be viewed as a functional component with two primary interfaces providing application-level connectivity between CCS7 SEPs and the CCA. The protocol stack interfacing with the SCCS7 signaling network is a standard CCS7 protocol stack. The protocol stack interfacing with the CCA is an internal unexposed interface that can be based on proprietary protocols or IETF SIGTRAN protocols. For example, the interface between the SG and the CCA can use SIGTRAN Adaptation protocols (i.e., SCCP User Adaptation (SUA) specified in RFC 3868; Message Transfer Part 3 (MTP3) User Adaptation (M3UA) specified in RFC 4666; Message Transfer Part 2 (MTP2) Peer-to-Peer Adaptation (M2PA) specified in RFC 4165; or MTP2 User Adaptation (M2UA) specified in RFC 3331 over SCTP/IP. An Interworking Layer is required at the SG in order to act as a mediation function between the two interfaces as shown in the diagram.

5.3.2.13.4.1 SG and CCS7 Network Interactions

5.3.2.13.4.1.1 SG-CCS7 Interface Functions

The SG provides the following primary functions on the CCS7 network side:

1. CCS7 Network Connectivity. Standard CCS7 link connectivity to the DSN CCS7 network. This includes the necessary link and data link functions and procedures.

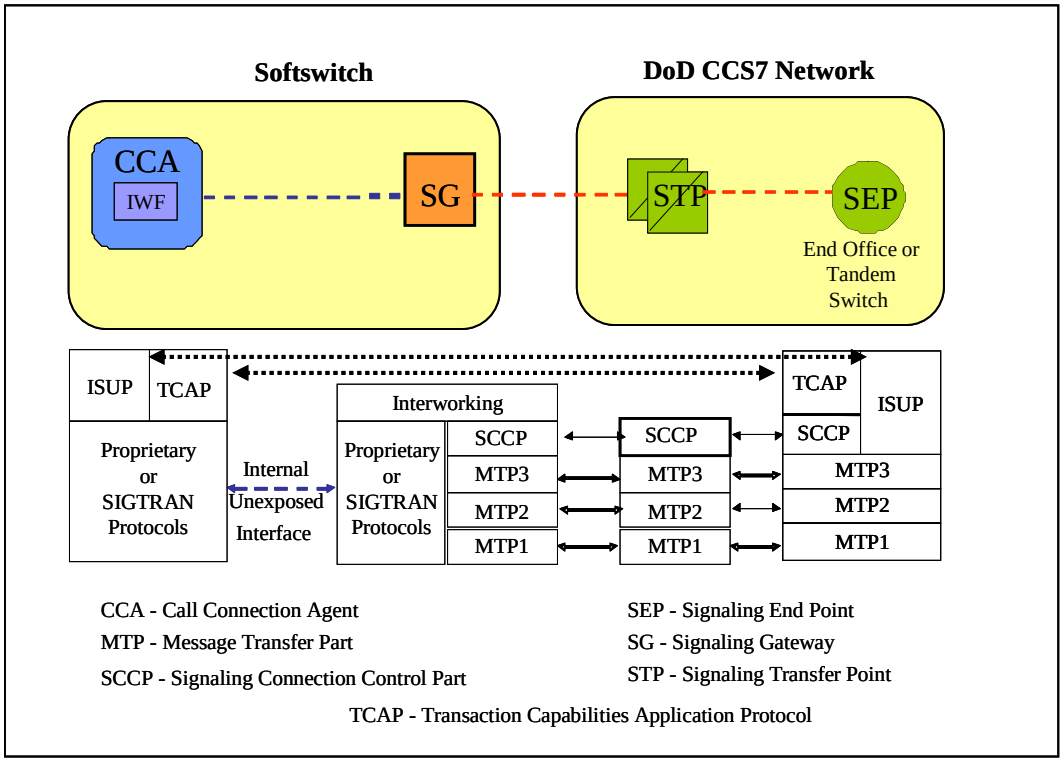


Figure 5.3.2-18. SG Protocol Design

2. <u>CCS7 Message Transfer Network Functions</u>. These functions include the following:

   a. Receiving CCS7 messages over a set of links from an CCS7 node (e.g., an STP)

   b. Encapsulating or translating the user information contained in the message (i.e., ISUP information for call setup and service-related signaling, or (SCCP) TCAP information for other service-related signaling) for delivery to the CCA.

   c. Processing received encapsulated ISUP, SCCP/TCAP, and MTP information from the CCA.

   d. Transferring the message to the interconnecting CCS7 node after stripping off the IP packet information.

   e. Populating the lower layer CCS7 information in the message.

3. <u>CCS7 MTP3 Network Management Functions</u>. These functions include receiving MTP3 NM messages from interconnected CCS7 networks and performing the necessary network management functions and procedures. This includes flow control-related functions between the CCS7 interface and the CCA interface.

4. Transport Protocol Interworking Functions. These functions include providing necessary transport protocol interworking between the CCS7 transport protocols (i.e., MTP protocols) on the CCS7-SG interface and IP transport protocols (i.e., SIGTRAN or proprietary protocols) on the SG-CCA interface.

5. CCS7 Network Gateway Screening and Security Functions. These functions include providing gateway screening functions to inspect fields and parameters of received CCS7 messages, and providing signaling network monitoring capabilities and functions for security.

5.3.2.13.4.1.2 SG-CCS7 Interface Protocols

MTP Level 1, MTP Level 2, and MTP Level 3 of the CCS7 protocol stack shall be used by the SG for connectivity between the SG and the DISN CCS7 network. The CCS7 MTP protocols are specified in ANSI T1.111.

MTP Level 1 (Signaling Data Link Functions) defines the physical, electrical, and functional characteristics of a signaling data link and the means to access it. The Level 1 element provides a bearer for a signaling link. Signaling Data Link is specified in ANSI T1.111, Chapter T1.111.2, Signalling Data Link.

MTP Level 2 (Signaling Link Functions) defines the functions and procedures for, and relating to, the transfer of signaling messages over one individual Signaling Data Link. The Level 2 functions together with a Level 1 Signaling Data Link as a bearer provides a signaling link for reliable transfer of signaling messages between two points.

A signaling message delivered by the higher levels is transferred over the signaling link in variable length signal units. For proper operation of the signaling link, the signal unit comprises transfer control information in addition to the information content of the signaling message.

Signaling Link functions include the following:

- Delimitation of signal unit by means of flags
- Flag imitation prevention by bit stuffing
- Error detection by means of check bits included in each signal unit
- Error correction by retransmission and signal unit sequence control by means of explicit sequence numbers in each signal unit and explicit continuous acknowledgments

- Signaling link failure detection by means of signal unit error rate monitoring and signaling link recovery by means of special procedures

The protocol specification for signaling link functions is given in ANSI T1.111, Chapter T1.111.3, Signalling Link.

MTP Level 3 (Signaling Network Functions) defines the transport functions and procedures that are common to, and independent of, the operation of individual signaling links. These functions fall into two major categories:

1. Signaling Message Handling Functions. These functions, at the actual transfer of a message, direct the message to the proper signaling link or higher level function.

2. Signaling Network Management Functions. These functions, based on predetermined data and information about the status of the signaling network, control the current message routing and configuration of signaling network facilities. In the event of changes in the status, they control reconfigurations and other actions to preserve or restore the normal message transfer capability.

The protocol specification for MTP3 (Signaling Network Functions) is given in ANSI T1.111, Chapter T1.111.4, Signalling Network Functions and Messages. Some means for testing and maintenance of the signaling network are given in ANSI T1.111, Chapter T1.111.7, Testing and Maintenance.

The SCCP provides additional functions to the MTP to provide both connectionless as well as connection-oriented network services to transfer circuit-related and non-circuit-related signaling information and other types of information.

The SCCP protocol is specified in ANSI T1.112.

5.3.2.13.4.2 SG and CCA Interactions

5.3.2.13.4.2.1 SG-CCA Interface Functions

The SG provides the following primary functions on the CCA side:

1. Connectivity to the CCA. Provides connectivity to the CCA via an internal unexposed interface within a vendor solution platform.

2. Message Transfer Functions.

a. Delivery of encapsulated user information contained in CCS7 messages received from the CCS7 side (i.e., ISUP information for call setup and service-related signaling, or SCCP/TCAP information for other service-related signaling) to the CCA.

b. Receiving encapsulated ISUP, SCCP/TCAP, and MTP information from the CCA, stripping off the IP packet information, populating the lower layer CCS7 information in the message, and transferring the message to the interconnecting CCS7 node.

3. SG-CCA Transport Network Management Functions. Provide necessary transport network management functions on the SG-CCA interface based on events on the CCS7 network side (e.g., network congestion and signaling node failure).

5.3.2.13.4.2.2 SG-CCA Interface Protocols

The protocol stack interfacing with the CCA is an internal unexposed interface that can be based on proprietary protocols or IETF SIGTRAN protocols. For example, this interface can use applicable IETF SIGTRAN Adaptation protocols over the SCTP/IP.

5.3.2.13.4.3 SG Interworking Functions

To enable seamless operation of the peer-to-peer CCS7 call control and service control protocols (i.e., ISUP and TCAP) in the CCS7 SEPs and the CCA, the SG will provide the necessary interworking functions between the transport protocols on the CCS7 side and the CCA side. The interworking function's purpose is to deliver the CCS7 information received from the CCS7 interface in an appropriate form to be conveyed to the CCA. This internal SG function delivers CCS7 messages received from the CCA to the CCS7 interface, after the appropriate NAT, mapping, and appropriate formatting for routing. This function is viewed as an implementation-specific function, depending on vendor-specific solutions.

5.3.2.13.5 Detailed SG Requirements

The requirements identified in this section are **[Conditional: LSC, MFSS]**.

5.3.2.13.5.1 SG and CCS7 Network Interactions

5.3.2.13.5.1.1 General Functional Requirements

[Conditional] The SG shall support signaling connectivity to the DoD CCS7 network based on UCR 2008, Section 5.2, Circuit-Switched Capabilities and Features, specifications for CCS7.

NOTE: The detailed requirements for the SG described in the following sections are based on ANSI CCS7 standards and on UCR 2008, Section 5.2, Circuit-Switched Capabilities and Features, specifications for DoD CCS7.

5.3.2.13.5.1.2 CCS7 Network Protocol Interface

This section describes the MTP requirements for the SG to interface with the DoD CCS7 network using MTP2 signaling links.

5.3.2.13.5.1.2.1 Signaling Data Link Functions (MTP Level 1)

A "signaling data link" is a bidirectional transmission path for signaling, comprised of two "data transmission paths" operating together in opposite directions at the same data rate. It is the lowest functional level (Level 1) in the CCS7 functional hierarchy.

[Conditional] The SG shall support the physical, electrical, and functional characteristics of a Signaling Data Link as specified in ANSI T1.111, Chapter T1.111.2, Signalling Data Link, for a 56-kbps data rate.

5.3.2.13.5.1.2.2 Signaling Link Functions (MTP Level 2)

The Signaling Link functions, together with the data link as bearer, provide a signaling link for the reliable transfer of signaling messages between two directly connected signaling points (e.g., the SG and an STP). Signaling messages received from the MTP3 are transferred over the signaling link in variable-length "signal units." The Signaling Link function comprises the following:

- Signal unit delimitation
- Signal unit alignment
- Signal unit error detection
- Signal unit error correction
- Signaling link initial alignment
- Signaling link error monitoring
- Flow control

5.3.2.13.5.1.2.2.1 Signaling Unit Format, Delimitation, and Alignment

[Conditional] The SG shall support the signaling unit formats and coding as specified in ANSI T1.111 Chapter T1.111.3, Signalling Link.

[Conditional] The SG shall perform the protocol procedures as specified in ANSI T1.111, Chapter T1.111.3, Signalling Link, for signaling unit delimitation and alignment.

5.3.2.13.5.1.2.2.2 Signaling Unit Acceptance and Error Detection

[Conditional] The SG shall perform the procedures for signaling unit acceptance and signaling unit error detection as specified in ANSI T1.111, Chapter T1.111.3, Signalling Link.

5.3.2.13.5.1.2.2.3 Error Correction

[Conditional] The SG shall support MTP Signaling Link functions for both terrestrial and satellite signaling links. This involves supporting both of the MTP2 error correction methods specified in ANSI T1.111.3, Signalling Link, the basic error correction method and the preventive cyclic retransmission error correction methods.

5.3.2.13.5.1.2.2.4 Signaling Link Initial Alignment

The procedure for signaling link initial alignment is used for activation and restoration of the signaling link.

[Conditional] The SG shall perform the procedure for signaling link initial alignment as specified in ANSI T1.111, Chapter T1.111.3, Signalling Link.

5.3.2.13.5.1.2.2.5 Signaling Link Error Monitoring

ANSI T1.111 specifies two types of error rate monitor as follows:

1. The alignment error rate monitor is used while a signaling link is in the proving state of the initial alignment procedure.

2. The signal unit error rate monitor is used while a signaling link is in service and provides one of the criteria for taking the link out of service.

[Conditional] The SG shall support the procedures for alignment error rate monitor as specified in ANSI T1.111, Chapter T1.111.3, Signalling Link. The alignment error rate monitor procedures shall be performed while a link is in the proving state of the initial alignment procedure.

[Conditional] The SG shall support the procedures for signal unit error rate monitor as specified in ANSI T1.111, Chapter T1.111.3, Signalling Link. The signal unit error rate monitor shall be employed for each active signaling link.

5.3.2.13.5.1.2.2.6 Level 2 Flow Control

The procedure for Level 2 flow control is used to control congestion situations at MTP2.

[Conditional] The SG shall support the procedures for Level 2 flow control as specified in ANSI T1.111, Chapter T1.111.3, Signalling Link.

5.3.2.13.5.1.2.2.7 Processor Outage

A processor outage condition occurs when the use of a link is precluded due to factors at a functional level higher than MTP2. An example of this would be if Level 2 could not transfer signaling messages to Level 3. Though one possible cause for this condition is central processor failure, it is possible that the condition would not affect all links in the SG. Furthermore, it is still possible that MTP3 would be able to control the operation of the signaling link, even if it cannot communicate to the other levels.

The goal of the processor outage procedures in different signaling points is to remove the affected link from service when a processor outage condition occurs and return the link to service when the processor outage condition ceases, all in a coordinated manner between signaling points. These procedures use the changeover and changeback procedures to divert traffic to and from other links.

[Conditional] The SG shall support the processor outage procedures as specified in ANSI T1.111, Chapter T1.111.3, Signalling Link.

[Conditional] The SG shall support the requirements for processor outage that are applicable to a CCS7 SEP, as specified in Telcordia Technologies GR-606-CORE, Section 2.7, Processor Outage.

5.3.2.13.5.1.2.2.8 Provisional Values for Level 2 Timers

[Conditional] The SG shall support the provisional values for MTP2 Timers as specified in Telcordia Technologies GR-606-CORE, Table 1-1, Provisional Values for Level 2 Timers.

5.3.2.13.5.1.2.2.9 Link Performance

1. Signaling Link Availability. Signaling link availability depends on the absence of failures not only for the link itself but also for its associated signaling link terminals. The SG should have sufficient connections to STPs to meet an availability objective (99.9996%) of not more than 2 minutes per year downtime for network access. Unavailability of network

access would occur if the SG became isolated because all signaling links between the SG and the STPs (or EO or Tandem) on which it is connected became unavailable.

2. Link Output Delay. Link output delay is defined as the interval beginning when the message has been placed in the output signaling link terminal buffer and ending when the last bit of the message has been transmitted on the outgoing signaling data link.

Link output delay is the sum of queuing delay and message emission time. Message emission time is a function of the signaling data link speed, message length distribution, and modem delay. Queuing delay is a function of message emission time and link occupancy.

The SG signaling link terminals should meet the message transmission delay objectives stated in Table 5.3.2-48, Link Output Delay Objective (15 Octet Long Messages), and Table 5.3.2-49, Link Output Delay Objective (279 Octet Long Messages), which are based on the following assumptions:

1. Message retransmissions are not considered when calculating transmission delay.

2. The signaling link is normally loaded to 40 percent of its signaling information transmission capacity (.4 Erlangs traffic loading). The signaling link load under failure conditions is considered to be 8 Erlangs (twice normal loading).

3. Signaling data link speed is 56 kbps.

4. There is no modem delay for the 56-kbps signaling links.

5. Message Signaling Units (MSUs) are a minimum of 15 octets and a maximum of 279 octets in length (see Table 5.3.2-48, Link Output Delay Objective (15 Octet Long Messages), and Table 5.3.2-49, Link Output Delay Objective (279 Octet Long Messages)). These message length limits are derived from the message formatting principles described in ANSI T1.111. Link output delay objectives are stated only for messages of minimum and maximum length; the actual message transmission delays present at the SG will depend on message length distributions, but should be less than that indicated for messages of maximum length (i.e., 279 octets).

Table 5.3.2-48. Link Output Delay Objective (15 Octet Long Messages)

LINK LOAD	MEAN	95 PERCENTILE
0.4 Erlangs	4 ms	6 ms
0.8 Erlangs	7 ms	18 ms

Table 5.3.2-49. Link Output Delay Objective (279 Octet Long Messages)

LINK LOAD	MEAN	95 PERCENTILE
0.4 Erlangs	56 ms	105 ms
0.8 Erlangs	122 ms	323 ms

5.3.2.13.5.1.2.2.10 False Link Congestion

See Section 5.3.2.13.5.1.2.4.6, False Link Congestion.

5.3.2.13.5.1.2.3 Signaling Network Functions and Messages (MTP3)

The MTP3 protocol specifies the functions and procedures that are common to, or independent of, the operation of individual signaling links. Level 3 functions fall into two main categories: signaling message handling and signaling network management functions. The MTP3 protocol is specified in ANSI T1.111, Chapter T1.111.4, Signalling Network Functions and Messages.

5.3.2.13.5.1.2.3.1 CCS7 Message Formatting

Specific guidelines for CCS7 message formatting are specified in ANSI T1.111, Chapter T1.111.4, Signalling Network Functions and Messages.

[Conditional] The SG shall adhere to the rules and specifications for formatting of CCS7 messages and coding of the fields and subfields as specified in ANSI T1.111, Chapter T1.111.4, Signalling Network Functions and Messages.

[Conditional] The SG shall be capable of verifying that messages received from interconnected CCS7 networks are of the proper formats and adhere to the rules for coding of the fields and subfields as specified in ANSI T1.111, Chapter T1.111.4, Signalling Network Functions and Messages.

5.3.2.13.5.1.2.3.2 Message Handling

[Conditional] The SG shall support the procedures for message handling as specified in ANSI T1.111, Chapter T1.111.4, Signalling Network Functions and Messages.

5.3.2.13.5.1.2.3.3 Handling of Messages under Signaling Link Congestion

[Conditional] The SG shall support the procedures for the handling of messages under signaling link congestion for U.S. networks, as specified in Section 2.3.5.2 ANSI T1.111, Chapter T1.111.4, Signalling Network Functions and Messages.

5.3.2.13.5.1.2.3.4 Message Discrimination and Distribution

Message discrimination is the determination of whether the SG receiving a message is the correct destination signaling node. All messages received at the SG should be addressed to the SG.

[Conditional] The SG shall examine each message received to verify that the Destination Point Code (DPC) is valid.

[Conditional] If the DPC of a received message does not correspond to the point code assigned to the SG (and CCA), the SG shall report the event to the Management function and should discard the message without further processing.

After the discrimination validates the DPC, the message distribution function is used to deliver the received message to the appropriate MTP user for further processing. The information required for message distribution is contained in the Service Information Octet (SIO).

The CCS7 User Part protocols (e.g., ISUP and TCAP) are not deployed at the SG. Therefore, in theory, after the discrimination function verifies that the DPC of the message is the SG, the MTP distribution function shall deliver the message to the vendor-specific IWF for further processing and transfer to the CCA.

5.3.2.13.5.1.2.3.5 Message Routing

The MTP message routing involves selecting an outgoing signaling link that will deliver a message to its proper destination node.

[Conditional] Before transmitting an MSU, the SG shall identify the normal (combined) link sets on which the message should be transported.

A link set is the set of links from the SG that terminate at a particular signaling point. Link sets of equal ranking or equal preference for carrying a particular signaling message are referred to as a “combined link set.”

The preferred link set or preferred combined link set with the highest priority for signaling messages to a particular destination is referred to as the “normal link set.” A (combined) link set of lower priority could be identified at the SG in the event that all links in the normal (combined) link set are unavailable. A link set or a combined link set with a lower priority than the normal link set that is used as a backup route to the same destination is referred to as an “alternate link set.” The (combined) link set being used at any given time for traffic to a given destination is referred to as the “current (combined) link set.” This could be either the normal link set or an alternate link set, but not both.

5.3.2.13.5.1.2.3.6 Backup Routing Procedures

For messages having a DPC uniquely associated with a signaling point that is at the remote end of a signaling link set connected to the SG, the normal link set should consist of the single link set that directly connects the two signaling points. For such messages, the SG should be able to identify a link set or combined link set of lower priority to be used in case all links in the normal link set are unavailable. For other messages, the normal combined link set should consist of at least two link sets between the SG and STPs.

[Conditional] The SG shall support backup routing procedures as specified in ANSI T1.111, Chapter T1.111.4, Signalling Network Functions and Messages.

[Objective] The SG shall support the requirements for backup routing procedures as specified in Telcordia Technologies GR-606-CORE, Section 3.3, Message Routing.

5.3.2.13.5.1.2.3.7 Loadsharing

The purpose of loadsharing is to distribute traffic evenly over the links of a link set (combined link set). The loadsharing method to be used on the CCS7 links is specified in ANSI T1.111, Chapter T1.111.5, Section 7.3, Signalling Network Structure. As specified in ANSI T1.111, loadsharing of messages over available links in a link set is done by using the 8-bit Signaling Link Selection (SLS) field and is referred to as “modified SLS rotation.”

[Conditional] The SG shall support procedures for loadsharing as specified in ANSI T1.111, Chapter T1.111.5, Signalling Network Structure.

[Conditional] The SG shall provide loadsharing of messages over all available links in the current (combined) link set by the method of modified SLS rotation. The 256 possible values of the 8-bit SLS field shall be mapped to the available links so that the total number of values assigned to each link shall differ by no more than one.

Previously, the ANSI CCS7 standard used a 5-bit SLS for loadsharing. Therefore, the SG may have to interconnect to signaling points using a 5-bit SLS field.

[Conditional] The SG shall be capable of interconnecting and operating with signaling points using a 5-bit SLS field.

[Conditional] The SG shall be capable of supporting link set sizes of up to 16 links per link set.

5.3.2.13.5.1.2.3.8 Message Sequencing

The CCS7 signaling link protocol is designed to ensure that all messages sent over the same signaling link will be received at the destination point in the order transmitted, since messages are retransmitted in their original order. Signaling network management procedures are designed with the intent that messages having a common SLS assignment as well as identical destinations will be delivered to the destination point in the original order of transmission. Message sequencing for such messages is normally retained even with changes in signaling link availability.

It is assumed that the SLS value is generated by the upper layer CCS7 protocols at the CCA (e.g., ISUP) and provided along with the other information (e.g., DPC and Originating Point Code [OPC]) for the SG to format the outgoing CCS7 message.

5.3.2.13.5.1.2.4 MTP3 Signaling Network Management Functions

5.3.2.13.5.1.2.4.1 Signaling Traffic Management

Signaling traffic management functions are used to divert signaling traffic from a link or route to one or more different links or routes, or to temporarily slow down signaling traffic in the case of congestion at a signaling point.

[Conditional] The SG shall support the following signaling traffic management procedures as specified in ANSI T1.111, Chapter T1.111.4, Signalling Network Functions and Messages:

- Changeover
- Changeback
- Forced rerouting
- Controlled rerouting
- Management inhibiting
- Signaling traffic flow control

[Conditional] The SG shall support the requirements for the following traffic management procedures as specified in Telcordia Technologies GR-606-CORE, Section 4, Signaling Network Management:

- Changeover
- Changeback
- Forced rerouting
- Controlled rerouting
- Management inhibiting

- Signaling traffic flow control

5.3.2.13.5.1.2.4.2 MTP Restart

The MTP restart is described in ANSI T1.111, Chapter T1.111.4, Section 9, MTP Restart. The MTP restart procedure can be separated into actions for being adjacent to a restarting node and actions for a restarting node. The SG is required to perform the actions for being adjacent to a restarting node and performing procedures for a restarting node is an SG IOC (FY2008) objective.

[Objective for a Restarting SG]

At an SG, the full MTP restart procedures provide value because the SG cannot perform effectively until it has re-established signaling links to at least a significant fraction of its adjacent signaling points. Without the MTP restart procedures, each adjacent signaling point in the CCS7 network will send signaling messages to the SG as soon as a signaling link to the SG becomes available, but a call cannot be completed unless the connection to the CCA is established. The MTP restart procedure shields the SG from user traffic (ISUP) until signaling links have been established to sufficient adjacent nodes. Thus, it is desirable that the SG perform MTP restart procedures for a restarting node.

[Objective] It is desirable in FY2008 that the SG supports MTP restart procedures for a restarting node as specified in ANSI T1.111, Chapter T1.111.4, Section 9, MTP Restart.

[Objective] It is desirable in FY2008 that an unavailable SG that is ready to resume operation by making links available and resuming the exchange of signaling traffic shall initiate the MTP restart procedures corresponding to a restarting node when the first link(s) becomes available at Level 3.

Requirements for an SG Adjacent to a restarting signaling point:

- Since the SG will be connected to STPs and EOs that may be supporting the MTP restart procedures, it is necessary that the SG satisfy the requirements for being adjacent to a restarting node.

[Conditional] The SG shall support MTP restart procedures for being adjacent to a restarting node as specified in ANSI T1.111, Chapter T1.111.4, Section 9, MTP Restart.

5.3.2.13.5.1.2.4.3 Signaling Link Management

Signaling link management is used to control the locally connected signaling links. The function provides controls to restore failed links, to activate idle links, and to deactivate aligned links.

[Conditional] The SG shall support the signaling link management procedures for signaling link activation, restoration, and deactivation, and signaling link set activation as specified in ANSI T1.111, Chapter T1.111.4, Signalling Network Functions and Messages, for automatic allocation of signaling data links and signaling terminals.

5.3.2.13.5.1.2.4.4 Signaling Route Management

Signaling route management is used to distribute information about signaling network status and to control signaling routes.

[Conditional] The SG shall support the following signaling route management procedures as specified in ANSI T1.111, Section T1.111.4, Signalling Network Functions and Messages:

- Transfer-prohibited
- Transfer-allowed
- Transfer-restricted
- Signaling-route-set-test
- Transfer-controlled
- Signaling-route-set-congestion

[Objective] The SG shall support the requirements for the following signaling route management procedures as specified in Telcordia Technologies GR-606-CORE, Section 4, Signaling Network Management:

- Transfer-prohibited
- Transfer-allowed
- Transfer-restricted
- Signaling-route-set-test
- Transfer-controlled
- Signaling-route-set-congestion

5.3.2.13.5.1.2.4.5 Message Priority and Congestion Control

Message priorities are indicated in the subservice field of the SIO for CCS7 messages, allowing up to four priority levels. The CCS7 message priorities are not intended to indicate which messages should be processed first, but instead are used to determine which messages should be

discarded in the event of signaling network congestion. Messages assigned priority level "0" are of the lowest priority, while priority level "3" is used for messages of the highest priority. Network management messages, with the exception of signaling-route-set-congestion-test messages, are assigned the highest priority.

[Conditional] The SG shall adhere to the message priority scheme as specified in ANSI T1.111, Section T1.111.5,Signalling Network Structure, Annex A.

[Conditional] The SG shall provide nine congestion thresholds for each signaling link: three congestion thresholds set at each of the three levels. There shall be no congestion thresholds assigned that affect transmission of priority 3 messages. The types of congestion thresholds that shall be used are congestion onset, congestion discard, and congestion abatement.

Congestion onset thresholds are used to detect overload conditions, whereas congestion abatement thresholds detect recovery from congestion.

[Conditional] As the transmit buffer occupancy is increasing and a congestion onset threshold is exceeded, or the buffer occupancy drops below a congestion abatement threshold, the SG shall update the congestion status of the signaling link.

[Conditional] If the condition above causes the congestion status of the signaling route set for a destination to be updated, the SG shall notify the MTP user (via the IWF) of the change in congestion status for affected destinations.

[Conditional] The congestion status of the signaling route set for a destination, which indicates the degree of congestion in a signaling route set, shall be maintained by the SG for destinations to which the SG routes messages.

[Conditional] The congestion status of the signaling route set shall be determined as defined in ANSI T1.111, Chapter T1.111.4, Section 3.8.4.

[Conditional] Messages received from local Level 4 (the IWF) with congestion priorities lower than the current signaling route set congestion status shall be discarded by the SG MTP (see ANSI T1.111, Chapter T1.111.4, Section 11.2.4).

The congestion discard threshold is used in combination with the buffer occupancy to determine the signaling link discard status. The signaling link discard status determines whether, during overload conditions, a message from Level 3 should be transmitted or discarded.

[Conditional] The current signaling link discard status shall be determined by the highest discard threshold exceeded by the current buffer occupancy.

[Conditional] If the current buffer occupancy does not exceed discard threshold 1, then the current signaling link discard status shall be zero.

[Conditional] The SG shall discard all messages from Level 3 with a priority lower than the signaling link discard status, but shall continue to transmit messages from Level 3 that are assigned a priority higher than or equal to the signaling link discard status.

5.3.2.13.5.1.2.4.6 False Link Congestion

False link congestion is a condition where a CCS7 link stays in service but is effectively transmitting or receiving few or no messages. For example, an SG may erroneously believe a link is congested when it is not, or is available when it has failed. There could be more than one root cause of the symptomatic state of an in-service link not effectively transmitting or receiving traffic and not being taken out of service automatically. The effect is harmful, regardless of the root cause: the transmitting end of the link will experience transmit congestion; invoke congestion control Level 3 procedures to stop CCS7 traffic at its source, affecting customer calls and resulting in customer reattempts that increase the call processing and signaling traffic load. One common characteristic of a link experiencing false link congestion is that it stays in one signaling link congestion status for a relatively long period of time. Therefore, if a link is in the same signaling link congestion status for a given period of time, it should be removed from service, as described in the following requirement. The link should be removed from service even if the removal causes a destination to be isolated.

[Conditional] The SG shall support the requirements for false link congestion as specified in Telcordia Technologies GR-606-CORE, Section 2.10.

5.3.2.13.5.1.2.4.7 Signaling Link Tests

The CCS7 protocol provides procedures for testing of operational signaling links. The SG should transmit the signaling link test message upon receiving the request from maintenance personnel.

[Conditional] The SG shall support the signaling link test procedure as specified in ANSI T1.111, Chapter T1.111.7, Testing and Maintenance.

1. The SG shall perform the signaling link test when a signaling link is activated or restored.

2. The SG shall perform the signaling link test every T1.111.7/T2 seconds on links while they are in the available state.

3. The SG shall support an option to turn on or turnoff the periodic signaling link tests on a per-SG basis.

4. The SG shall route signaling link test and signaling link test acknowledgment messages only on the link being tested (there shall be no loadsharing of messages based on their SLS values).

5.3.2.13.5.1.2.4.8 MTP User Flow Control

The procedure for MTP user flow control is used to control MTP User Part traffic flow when unavailability of an MTP user (e.g., ISUP) is detected. It is assumed that the procedure for MTP user flow control is not widely supported by SEPs (e.g., EOs and Tandems). Therefore, the SG itself will not be required to perform User Part Unavailability (UPU) procedures in the CCS7 network. For example, the SG is not required to send UPU messages. However, the SG should be capable of receiving and accepting a valid UPU message.

[Conditional] The SG shall be capable of receiving and accepting valid UPU messages.

In the SG-CCA CCS7 protocol design, the MTP and SCCP protocols are located at the SG, while the ISUP and TCAP protocols are located at the CCA. In this document, failure or unavailability of any of the protocols above MTP3 (i.e., SCCP, TCAP, and ISUP) is considered to be equivalent to loss of connectivity to the CCA, and the procedures in UCR 2008, Section 5.3.2.13.5.1.2.4.10, Actions for Loss of Connectivity to the CCA, applies.

5.3.2.13.5.1.2.4.9 MTP3 Timers

[Conditional] The SG shall support the provisional values and ranges for MTP3 timers as specified in Telcordia Technologies GR-606-CORE, Table 1-2.

5.3.2.13.5.1.2.4.10 Actions for Loss of Connectivity to the CCA

Depending on the implementation design and deployment conditions of the connectivity between the SG and CCA, loss of connectivity to the CCA may occur in certain failure scenarios. When all SG connectivity to the CCA is lost, the MTP in the SG should be notified, based on an implementation-dependent method via the SG IWF. When this occurs, corresponding action must be taken on the CCS7 interface to restrict the traffic being received from the CCS7 network. The corresponding action to be taken on the CCS7 side should be to apply the Processor Outage procedures on all the CCS7 links. This should cause the adjacent STPs (and EOs and Tandems) to stop sending traffic to the SG without having to fail the links on the CCS7 side of the SG.

NOTE: Unavailability of the SCCP, TCAP, and ISUP protocols between the SG and the CCA is considered to be equivalent to loss of SG connectivity to the CCA.

[Conditional] The SG shall be capable of detecting loss of connectivity to the CCA and detecting when connectivity to the CCA is restored.

[Conditional] The SG shall send the Status Indication Processor Outage (SIPO) message on all CCS7 links when loss of connectivity to the CCA is detected. The method for detecting this loss and performing this action is implementation-dependent.

[Conditional] Upon notification that connectivity to the CCA is restored, the SG shall perform the procedures related to cessation of a local processor outage condition as specified in ANSI T1.111, Chapter T1.111.4, Signalling Network Functions and Messages. The method for obtaining the notification and performing this action is implementation dependent.

5.3.2.13.5.1.2.5 SCCP

For IOC, support for TCAP is not a requirement, and therefore, support for the underlying SCCP is not a requirement. No services or features requiring the utility of TCAP have been identified as required in the IOC time frame.

5.3.2.13.5.1.2.5.1 Overview

The SCCP protocol provides special message transport capabilities for non-circuit-related information exchange. The SCCP transport capabilities provide additional functions to the MTP protocol. All SCCP information is contained in the signaling information field of the message. The SCCP information consists of an MTP Routing Label, mandatory and optional SCCP message parameters, and a data field. The information contained in the data field is provided by an SCCP user, such as TCAP.

The SCCP protocol supports both connectionless and connection-oriented services. However, the SG is only required to support connectionless services. Specifically, the SG is required to support the following protocol classes for connectionless services:

1. Class 0 – Basic Connectionless Class. This protocol class provides datagram transport. It is appropriate for MSUs that may be transported independent of all other messages. No attempt is made to guarantee a relationship between two or more messages from the same node.

2. Class 1 – Sequenced (MTP) Connectionless Class. This class is similar to protocol class 0 except that related messages are encoded with identical SLS values to determine the

signaling path used. Protocol class 1 represents an improved quality of service over protocol class 0 in that message sequencing will be maintained under normal conditions.

5.3.2.13.5.1.2.5.2 SCCP Messages and Parameters

[Conditional] The SG shall support the SCCP messages and parameters for connectionless service as specified in ANSI T1.112, Section T1.112.3:

- Unitdata (UDT)
- Extended Unitdata (XUDT)
- Unitdata Service (UDTS)
- Extended Unitdata Service (XUDTS)

[Conditional] The SG shall support the SCCP management messages and parameters for connectionless service as specified in ANSI T1.112, Section T1.112.3:

- Subsystem-Allowed (SSA)
- Subsystem-Prohibited (SSP)
- Subsystem Status Test (SST)

[Conditional] The SG shall adhere to the coding and addressing rules for SCCP parameters and fields as specified in ANSI T1.112, Section T1.112.3.

5.3.2.13.5.1.2.5.3 SCCP Connectionless Procedures

Since the SG together with the CCA of the MFSS or LSC is viewed as a SEP from the CCS7 network perspective, the SG is only required to support SCCP connectionless procedures that are necessary for a SEP.

[Conditional] The SG shall support connectionless procedures necessary for a SEP originating and receiving SCCP messages in the CCS7 network as specified in ANSI T1.112, Section T1.112.4 for:

- Data transfer
- Message return
- Syntax error

5.3.2.13.5.1.2.5.4 SCCP Management Procedures

[Conditional] The SG shall support SCCP management procedures necessary for a SEP originating and receiving SCCP messages in the CCS7 network as specified in ANSI T1.112, Section T1.112.4 for:

- Signaling Point Status Management
- Subsystem Status Management

[Conditional] The SG shall support the requirements specified in Telcordia Technologies GR-606-CORE, Section 5.4, for the following SCCP management procedures:

- Signaling Point Status Management
- Subsystem Status Management

5.3.2.13.5.1.2.6 CCS7 Gateway Screening and Security Functions

5.3.2.13.5.1.2.6.1 CCS7 Message Screening

ANSI T1.111, Chapter T1.111.5, Signalling Network Structure, specifies procedures to prevent unauthorized messages on the CCS7 network. These procedures are commonly referred to as "gateway screening." Gateway screening is performed by the STP in CCS7 networks to check the contents of the incoming message and to determine whether the message should be accepted or rejected (i.e., whether it is authorized) based on criteria specified by the CCS7 network administrator. Typically in CCS7 networks (and as specified in ANSI T1.111), screening at the STP is focused on lower layer protocol information (e.g., MTP and SCCP information). However, screening of ISUP and TCAP information is performed at the CCS7 application level in SEPs.

Since the SG is acting as a gateway network element between the interconnected CCS7 network and VoIP packet network, the SG should support screening functions to minimize the risks (e.g., address spoofing or masquerading) from interconnected CCS7 networks. The screening requirements specified in this document do not impose any solution constraint that the requirements have to be supported by the SG network element itself. However, the SG together with the CCA shall be capable of supporting these requirements.

[Conditional] The SG and CCA shall support procedures to identify unauthorized CCS7 messages (i.e., screening procedures) as specified in ANSI T1.111, Chapter T1.111.5, Section 8, Procedures to Prevent Unauthorized Use of an STP.

[Conditional] In addition, the SG and CCA shall support signaling and control procedures as defined in ATIS Signaling Systems No. 7 (SS7) – SS7 – Network and NNI Interconnection Security Requirements and Guidelines, ATIS-PP-1000012.2006.

[Conditional] It shall be possible to establish and implement SG and CCA CCS7 message screening rules for CCS7 at each network interconnection at the SG.

5.3.2.13.5.1.2.6.2 CCS7 Message Monitoring

CCS7 message screening cannot detect certain types of intrusion (e.g., message deletion, insertion, and replay). Therefore, the SG together with the CCA should support implementation-specific CCS7 message monitoring systems or tools with functions to detect intrusions and attacks that cannot be detected by CCS7 message screening.

[Conditional] The SG and the CCA shall support an implementation-specific solution for CCS7 message monitoring, or tools capable of detecting CCS7 attacks or intrusions that cannot be detected by CCS7 message screening.

Implementation-specific solutions should be designed to detect attacks and problems (e.g., Denial of Service (DoS) events, misuse of management messages) through observation and analysis of message patterns (e.g., frequency, contents, message types). For example, baseline traffic characteristics (norms) can be established, and algorithms can be defined to monitor network traffic. The monitored CCS7 message pattern can be compared with the established norms to identify abnormal events. The pattern algorithms could be keyed to the generic CCS7 information, such as message types (e.g., MTP, SCCP, ISUP, and TCAP message types), information in the message header (e.g., OPC, DPC, and Service Indicator (SI)), or to detailed application level information (e.g., TCAP and ISUP parameters).

Implementation-specific solutions may involve, but are not limited to, the following considerations:

- Monitoring at the network level, individual network element level, component or system level, individual protocol level, and the application/service level.

- Monitoring of generic CCS7 information, such as message types (e.g., MTP, SCCP, ISUP, or TCAP), address information (e.g., OPC, DPC, and SI), and application level information (ISUP and TCAP parameters) against established norms.

- Monitoring of CCS7 traffic volume against established norms.

These solutions may be applied globally to all types of CCS7 message traffic or may be applied selectively to specific types of CCS7 traffic, based on the identified source of the CCS7 traffic.

5.3.2.13.5.1.2.7 Requirements for MLPP

The MTP message priority values used in the PSTN CCS7 network are different from those used in the DoD CCS7 MLPP network. The SG and CCA are required to adhere to the message priority codes and values specified for DoD CCS7 MLPP.

[Conditional] The SG together with the CCA shall adhere to the guidelines and rules for coding of the MTP message priority values for the CCS7 network as shown in Table 5.3.2-50, MTP3 Message Priority Value for DoD CCS7 Network.

5.3.2.13.5.2 SG Interactions with CCA

The SG and CCA are considered part of the same solution platform, and the SG-CCA interface is viewed as an internal unexposed interface. Since this interface can be based on proprietary protocols or on variants of SIGTRAN protocols, the requirements in this section are not based on industry protocol specifications like the SG-CCS7 interface requirements are. Instead, this section provides general functional requirements on the SG-CCA interface without placing any constraint on the protocol solution for the interface.

Table 5.3.2-50. MTP3 Message Priority Value for DoD CCS7 Network

IAM MLPP PRECEDENCE LEVEL	MTP PRIORITY VALUE
FLASH OVERRIDE	3
FLASH	3
IMMEDIATE	2
PRIORITY	1
ROUTINE	0

5.3.2.13.5.2.1 General Requirements

The primary functions of the SG-CCA interface are as follows:

1. Transporting and delivering user information contained in CCS7 messages received from the CCS7 side (i.e., ISUP information for call setup and service-related signaling, or TCAP information for other service-related signaling) to the CCA.

2. Transporting and delivering ISUP, SCCP/TCAP, and MTP information from the CCA to the SG for routing to the interconnecting CCS7 node.

Reliability, integrity, and in-sequence delivery is required for the CCS7 information flow over the SG-CCA connection.

[Conditional] The SG shall support a supplier-specific interface to the CCA for interactions between the SG and CCA. The protocol solution for this interface is implementation specific and can be based on IETF's SIGTRAN protocol solution (e.g., use of adaptation protocols over SCTP/IP).

[Conditional] The signaling message flows and interactions on the supplier-specific SG-CCA interface shall be supported over a reliable transport connection providing message sequencing, integrity, detection of message loss, and recovery from message loss, which are functionally equivalent to the sequencing, loss detection, and loss recovery mechanisms in TCP and SCTP.

[Conditional] The signaling message flows and interactions on the supplier-specific SG-CCA interface shall be supported over a secure transport connection. The SG-CCA connection shall support strong security functions for authentication, confidentiality, and integrity in accordance with the UCR 2008, Section 5.4, Information Assurance Requirements.

5.3.2.13.5.2.2 Congestion Control

[Conditional] The transport connection between the SG and CCA shall support congestion control procedures. The congestion control mechanism shall be equivalent to the mechanisms used in TCP or SCTP and SIGTRAN Adaptation protocols.

5.3.2.13.5.2.3 Performance

The vendor solution for the SG-CCA interface and connection is required to take into consideration CCS7 performance requirements for the end-to-end CCS7 message flow. This means that any delays, errors, or message loss introduced by the SG-CCA connection should not result in the end-to-end CCS7 performance requirements being missed between the CCA and the interconnection CCS7 SEP. For example, MTP3 peer-to-peer procedures require MTP message response times within 500 to 1200 ms. This response time value includes round trip time and processing time at the remote end. Failure to meet this limitation will result in the initiation of error procedures for expiration of specific timers, e.g., ANSI T1.111.4, timer T4. Similarly, the requirement for end-to-end call setup delay in ISUP is that an end-to-end response message (ACM, ANS) be received within 20 to 30 seconds of the sending of the IAM. (NOTE: While this is the ISUP protocol guard timer value, end users will expect faster response time.)

[Conditional] The SG and CCA shall support the message delay requirements (described as protocol guard timers) for MTP, SCCP, ISUP, and TCAP, as specified in ANSI T1.111, T1.112,

T1.113, and T1.114, respectively, for the end-to-end CCS7 message path including the SG-CCA connection.

[Conditional] The SG and CCA shall support the performance requirements for message loss, sequence error, message errors, and availability, specified for MTP in ANSI T1.111, Chapter T1.111.6, Message Transfer Part Signalling Performance, for the end-to-end CCS7 message path including the SG-CCA connection.

5.3.2.13.5.3 SG Interworking Functions

5.3.2.13.5.3.1 General

The SG will terminate CCS7 links on its CCS7 side and transport the CCS7 call control and service control protocols (i.e., ISUP and TCAP) to the CCA. Similarly, the SG will receive CCS7 call control and service control messages from the CCA. The SG is responsible for the appropriate formatting of the messages for transmission on the CCS7 links. To enable seamless operation end-to-end, the SG will provide the necessary IWFs between the transport protocols on its CCS7 side and its CCA side. This includes necessary functions to interwork the MTP network management procedures on its CCS7 side with the management procedures of the transport connection between the SG and the CCA. This function is viewed as an implementation-specific function, depending on vendor-specific solutions.

[Conditional] The SG shall support vendor-implementation specific functions to enable seamless interworking between the CCS7 transport protocols (i.e., MTP and SCCP) on its CCS7 side and the transport connection between the SG and CCA. Specifically, the SG shall take specific actions based on management events in the CCS7 network, provide the necessary interworking actions on the transport connections to the CCA, and inform the CCA to take certain actions depending on these interworking actions.

5.3.2.13.5.3.2 Detection and Notification of Loss of Connectivity to CCS7 Network

If conditions in the CCS7 network change, loss of connectivity to the CCS7 network may occur. In addition, local failure of the SG's MTP may occur, which result in loss of connectivity to the CCS7 network. If loss of connectivity to the CCS7 network occurs, appropriate actions must be taken on the SG-CCA interface and the CCA to stop the traffic. NOTE: The notification from MTP3 that CCS7 connectivity has been lost and the detection of local MTP failure are implementation-dependent. The following requirements describe the procedures necessary for detection and notification of loss of connectivity to the CCS7 network:

1. **[Conditional]** The SG (i.e., the SG IWF) shall monitor the status of the local MTP3 availability. Upon detection of MTP3 failure (and thus loss of connectivity to the CCS7

network), the SG shall notify the CCA that connectivity to the CCS7 network has been lost. The methods for monitoring the local MTP3 and providing notifications to the CCA are implementation-dependent.

2. **[Conditional]** Upon detection of restoral of the local MTP3, which has previously failed, the SG (i.e., the SG IWF) shall notify the CCA that connectivity to the CCS7 network has been restored. The methods for monitoring the local MTP3 and providing notifications to the CCA are implementation-dependent.

5.3.2.13.5.3.3 Detection and Notification of Loss of Connectivity to CCA

Depending on certain events, the SG may lose connectivity to the CCA. The following requirements describe the procedures necessary for notification of loss of connectivity to the CCA:

1. **[Conditional]** The SG (i.e., the SG IWF) shall be capable of detecting loss of connectivity to the CCA and notifying the MTP3 of the loss of connectivity. The methods for detection of connectivity loss and providing notifications to MTP3 are implementation-dependent.

2. **[Conditional]** The SG (i.e., the SG IWF) shall be capable of detecting that connectivity has been restored to the CCA (which was previously inaccessible) and notifying MTP3 of the restored connectivity. The methods for detecting of connectivity restoral and providing notification to MTP3 are implementation-dependent.

NOTE: See Section 5.3.2.13.5.1.2.4.10, Actions for Loss of Connectivity to the CCA, for actions to be taken on the CCS7 side as a result of loss of CCA connectivity.

5.3.2.13.5.3.4 Internal Flow Control Functions

Situations can arise in which the signaling message handling functions at an SG cannot handle messages at the rate at which they are received at the SG. Such situations may result, for example, from a surge of signaling traffic (either to or from the CCA) or from failures that reduce message handling capacity (e.g., MTP2 link set failures). An SG should be able to control the traffic that is destined for the overloaded resources by performing message handling functions in these situations. The CCS7 protocol provides some procedures that may be used to deal with such overload situations. Likewise, the transport connection between the SG and CCA is required to support congestion control procedures. Precise criteria for using each of these procedures in overload situations are dependent on the particular implementation, but some guidelines, objectives, and requirements can be given.

An SG's first defense against an overload of the message handling functions is to reduce the rate at which incoming messages are accepted, to the rate that the message handling functions can process without overload. For interconnection to the CCS7 network, this may result in the invocation of the MTP2 flow control procedures (described in ANSI T1.111, Chapter T1.111.3, Section 9, Level 2 Flow Control), and possibly a triggering of the transfer-controlled procedures or the signaling flow control procedures at adjacent nodes. Use of the Level 2 flow control procedures may be most suitable if there is an overload of the message handling resources associated with a particular incoming link, or if there is a fairly uniform overload of message handling resources at the SG (i.e., the SG-CCA connection has become congested). If the Level 2 flow control procedure is used, it should be designed so that the potential for timer T1.111.3/T6 expiration is not increased.

[Conditional] The SG shall be able to detect when the resources associated with signaling message handling are in danger of becoming overloaded. The method used to detect overload, while supplier-dependent, shall be so congestion controls can be performed by the SG. The following two congestion cases apply:

1. If the congestion occurs for traffic directed towards the CCA (from the CCS7 network), the SG shall execute the MTP2 flow control procedures on the signaling links to the CCS7 network nodes causing the congestion.

2. If congestion occurs for traffic directed toward the CCS7 network (from the CCA), the SG shall execute congestion control procedures on the transport connection to the CCA.

5.3.2.14 Customer Edge Router Requirements

5.3.2.14.1 Traffic Conditioning

[Required: CE Router] The system shall be capable of performing traffic conditioning (policing and shaping) on inbound and outbound traffic. This may involve the dropping of excess packets or the delaying of traffic to ensure conformance with Service Level Agreements (SLAs).

[Required: CE Router] The system shall be capable of traffic conditioning the bandwidth associated with a service class.

5.3.2.14.2 Differentiated Services Support

[Required: CE Router] The system shall be capable of supporting Differentiated Services (DiffServ) in accordance with RFC 2475 and RFC 2474.

NOTE: The DSCP requirements are specified in UCR 2008, Section 5.3.3, Wide Area Network Requirements.

5.3.2.14.3 Per Hop Behavior Support

[Required: CE Router] The system shall be capable of supporting the PHBs.

NOTE: The PHB requirements are specified in UCR 2008, Section 5.3.3, Wide Area Network Requirements.

[Required: CE Router] The system shall be capable of supporting Expedited Forwarding (EF) PHBs in accordance with RFC 3246.

[Required: CE Router] The system shall be capable of supporting the Assured Forwarding (AF) PHB in accordance with RFC 2597.

5.3.2.14.4 Interface to the LSC/MFSS for Traffic Conditioning

[Conditional: CE Router] The CE Router shall be capable of interfacing to the LSC/MFSS in real time to adjust traffic conditioning parameters based on the updated LSC/MFSS budgets.

NOTE: For example, if the LSC budget decreases from ten Voice sessions to five Voice sessions, then the traffic conditioning parameters should change from 10x110=1100 kbps to 5x110=550 kbps in both directions. In IOC, the process will be a manual process to statically configure the PHB allocations. This assumes that traffic conditioning occurs prior to applying the PHBs.

5.3.2.14.5 Interface to the LSC/MFSS for Bandwidth Allocation

[Conditional: CE Router] The system shall be capable of interfacing to the LSC/MFSS in real time to adjust the PHB bandwidth allocations based on the updated LSC/MFSS budgets.

NOTE: For example, if the LSC budget decreases from ten Voice sessions to five Voice sessions, then the EF queue bandwidth allocation should change from 10x110=1100 kbps to 5x110=550 kbps in both directions. In IOC, the process will be a manual process to statically configure the PHB allocations. This assumes that traffic conditioning occurs prior to applying the PHBs.

5.3.2.14.6 Network Management

[Required: CE Router] The system shall support FCAPS Network Management functions as defined in the UCR 2008, Section 5.3.2.17, Management of Network Appliances.

5.3.2.14.7 Availability

Two types of CE Routers are High Availability and Medium Availability. Defining two types of CE Routers is driven by cost factors and the availability that can be provided by COTS products. The Medium Availability CE Router provides a cost-effective solution for locations that serve C2(R) and non-C2 users. Locations serving special C2 and C2 users with IMMEDIATE and above precedence service must install High Availability CE Routers.

[Required: High Availability CE Router] The system shall have an availability of 99.999% including scheduled maintenance (non-availability of no more than 5 minutes per year).

[Required: Medium Availability CE Router] The system shall have an availability of 99.99% including scheduled maintenance.

NOTE: The vendor will provide a reliability model for the system showing all calculations for how the availability was met.

[Required: High and Medium Availability CE Router] The system shall have a component failover time as defined in UCR 2008, Section 5.3.3.9.1, End-To-End Availability.

[Required: High and Medium Availability CE Router] The system shall meet the requirements specified in UCR 2008, Section 5.3.2.5.2, System Quality Factors, with the exceptions previously noted.

5.3.2.14.8 Packet Transit Time

[Required: CE Router] The system shall be capable of receiving, processing, and transmitting an RTS packet within 2 milliseconds (ms) to include executing all internal functions.

NOTE: Internal functions do not include domain name system (DNS) lookups and other external actions or processes.

5.3.2.14.9 Customer Edge Router Throughput Support

The CE Router supports an ASLAN-side connection to the EBC and a WAN-side connection to the DISN WAN. The ASLAN side connection uses an Ethernet interface (10BT or 100 BT).

The WAN side access connection uses a WAN access interface, which is TDM-based or Ethernet-based (i.e., DS-1, DS-3, E1, 10 BT, 100BT). These are all full-duplex interfaces, and support two-way simultaneous information exchange at the "line rate" for the interface (i.e., 1.5 Mbps for DS-1, 45 Mbps for DS-3).

The CE Router needs to support information "throughput" in two directions: from the ASLAN side to the WAN side, and from the WAN side to the ASLAN side. The CE Router also needs to support this throughput in full-duplex mode, which means that the CE Router needs to support the maximum possible throughput on the WAN side interface for packets sent in the ASLAN-to-WAN direction. At the same time, the CE Router needs to support the maximum possible throughput on the WAN side interface for packets sent in the WAN-to-ASLAN direction. The maximum possible throughput for an interface is the maximum line rate for that interface, as provisioned on the CE Router.

A CE Router may support multiple interfaces on the ASLAN side, such as two 100BTs to an EBC and a data firewall, and on the WAN side, such as two DS1s to two different DISN SDNs). These requirements assume that the CE Router only has one WAN side interface active. They also assume that the line rate for the WAN side interface is less than or equal to the sum of the line rates for the ASLAN side interfaces.

[Required: CE Router] The CE Router shall support the maximum possible throughput on the WAN side interface, for a full traffic load of all traffic types sent in the ASLAN-to-WAN direction.

[Required: CE Router] The CE Router shall support the maximum possible throughput on the WAN side interface, for a full traffic load of all traffic types sent in the WAN-to-ASLAN direction.

[Required: CE Router] The CE Router shall support the maximum possible throughput on the WAN side interface in a full duplex mode, for a full traffic load of RTS packets sent simultaneously in both the ASLAN-to-WAN and WAN-to-ASLAN directions.

[Required: CE Router] The maximum possible throughput on the WAN side interface shall be the maximum line rate that the WAN side interface is provisioned for on the CE Router. The following maximum possible throughputs shall apply for the different WAN side interfaces:

- 10 BT: 10 Mbps
- 100 BT: 100 Mbps
- DS-1: 1.5 Mbps
- DS-3: 45 Mbps
- E-1: 2.0 Mbps

5.3.2.15 EBC Requirements

5.3.2.15.1 AS-SIP Back-to-Back User Agent

[Required: EBC] The system shall act as an AS-SIP Back-to-Back User Agent (B2BUA) for interpreting the AS-SIP messages to meet its functions.

NOTE: The requirements of the system to properly secure the AS-SIP messages are specified in UCR 2008, Section 5.4, Information Assurance Requirements, and the proper processing of an AS-SIP message is found in this section and UCR 2008, Section 5.3.4, AS-SIP General System Specification.

1. **[Required: EBC]** The system shall be capable of bidirectionally anchoring (NAT and NAPT) the media associated with a voice or video session that originates or terminates within its enclave.

    a. **[Required: EBC]** The system shall assign a locally unique combination of "c" and "m" lines when anchoring the media stream.

    b. **[Required: EBC]** If an INVITE request is forwarded to a system fronting an MFSS for which the INVITE request is not destined (i.e., the MFSS will forward the INVITE request downstream to another MFSS or LSC), the system shall be capable of anchoring the media upon receipt of the INVITE request, but shall restore the original "c" and "m" lines upon receipt of the forwarded INVITE request from the MFSS.

    NOTE: The MFSS will not modify the "c" and "m" lines. The reason why the anchoring occurs upon receipt of the message is that the system does not know at that point whether the session will terminate within the enclave.

    c. **[Required: EBC]** If a session is forwarded or transferred so the session is external to the enclave (i.e., the session no longer terminates or originates within the enclave), then the system shall restore the original received "c" and "m" lines to the forwarding/transfer message, as appropriate, to ensure that the media is no longer anchored to that system.

2. **[Required: EBC]** The EBC shall be capable of processing Route Headers in accordance with RFC 3261, Sections 20.3, 4 8.1.2, 16.4, and 16.12.

    [Required: MFSS] The MFSS will generate Route Headers for the system to tell the system the next hop for the AS-SIP message.

[Required FY12: LSC, MFSS] Both the LSC and the MFSS will be required to generate Route Headers for the system.

3. **[Required: EBC]** The system shall preserve/pass the CCA-ID field in the CONTACT Header.

4. **[Required: EBC]** The system shall always decrement the Max-Forward Header.

5. **[Required: EBC]** The system shall modify the CONTACT Header to reflect its IP address to ensure it is in the return routing path.

6. **[Required: EBC]** The system fronting an LSC shall be capable of maintaining a persistent TLS session between the EBC fronting the primary MFSS and the EBC fronting the secondary MFSS. Persistent means that the TLS session is established at the time the system joins the signaling network and is not established on a session-by-session basis.

   a. **[Required: EBC]** The EBC shall be capable of distinguishing between the primary (associated with the primary MFSS) and a secondary (associated with the secondary MFSS) TLS path for the purposes of forwarding AS-SIP messages.

   b. **[Required: EBC]** The EBC shall forward all AS-SIP messages across the secondary TLS path if the primary TLS path fails or a notification arrives at the system indicating that the primary MFSS has failed. Once the primary TLS path is restored or the primary MFSS recovers, the system shall forward all AS-SIP messages across the primary TLS paths.

      (1) **[Required: EBC]** The EBC shall fail over to the secondary TLS path when the system receives an AS-SIP message indicating a (408) Request Timeout, (503) Service Unavailable, or (504) Server Timeout.

      (2) **[Required: EBC]** The EBC shall fail over to the secondary TLS path when it detects a configurable number of AS-SIP OPTION request failures. The default number of failures shall be two. NOTE: A failure is indicated by a lack of a response or a failure notice.

      (3) **[Required: EBC]** The EBC shall return to forwarding all calls on the primary TLS path (to the primary MFSS) upon receipt of a 200 OK response from the primary MFSS to an OPTIONS request issued by its LSC.

      (4) **[Required: EBC]** The EBC fronting a secondary MFSS shall respond with a (481) Call/Transaction Does Not Exist when it receives a RE-INVITE,

UPDATE, or BYE AS-SIP message for which it has no match (because the session was established via the primary MFSS).

c. **[Required: EBC]** The EBC initiates a session toward its subtended LSC/MFSS (arriving from the WAN) when receiving an incoming INVITE AS-SIP message from the WAN.

5.3.2.15.2 Call Processing Load

[Required: EBC] The system shall be capable of handling the aggregated WAN call processing load associated with its subtended LSCs and MFSSs.

NOTE: For instance if the B/P/C/S has three LSCs within the B/P/C/S and each LSC is expected to handle 50 WAN calls per minute, then the CE Router subsystem shall handle 150 calls per minute.

5.3.2.15.3 Network Management

[Required: EBC] The system shall support FCAPS Network Management functions as defined in UCR 2008, Section 5.3.2.17, Management of Network Appliances.

5.3.2.15.4 DSCP Policing

[Conditional: EBC] The EBC shall be capable of ensuring that media streams associated with a particular session use the appropriate DSCP based on the information in the AS-SIP RPH.

NOTE: This requires that the system maintain a table of the appropriate DSCP for a RPH marking. The mapping between precedence and DSCP is found in UCR 2008, Section 5.3.3, Wide Area Network Requirements.

5.3.2.15.5 Codec Bandwidth Policing

[Conditional: EBC] The EBC shall be capable of ensuring the media streams associated with a particular session use the appropriate codec (bandwidth) based on the SDP information in the AS-SIP message.

NOTE: For example, if an AS-SIP message signals that the media session will use a G.729a codec, the system shall traffic shape that session to 44 kbps (39.2 kbps (codec) plus 4.8 kbps (safety margin and signaling)). The 39.2 kbps assumes 20 ms samples or 50 pulses per second (pps). Payload is 8000 bits/50 pps equals 160 bits per packet (20 bytes). The IP overhead (40 bytes) plus Ethernet overhead (38 bytes) plus 160 bits per packet/8 bits per byte equals 98 bytes

per packet. The 98 bytes per packet * 50 pps * 8 bits/byte equals 39.2 kbps for IPv4. The IPv6 calculations would occur in the same manner.

5.3.2.15.6 Availability

There are two types of EBCs: High Availability and Medium Availability. Defining two types of EBCs is driven by cost factors and the availability that can be provided by COTS products. The Medium Availability EBC provides a cost-effective solution for locations that serve C2(R) and non-C2 users. Locations serving special C2 and C2 users with IMMEDIATE and above precedence service must install High Availability EBCs.

[Required: High and Medium Availability EBC] The system shall have an availability of 99.999% (non-availability of no more than 5 minutes per year).

NOTE: The vendor will provide a reliability model for the system showing all calculations for how the availability was met.

[Required: High and Medium Availability EBC] The system shall meet the requirements specified in UCR 2008, Section 5.3.2.5, System Physical, Quality, and Environmental Factors, with the following exceptions noted below.

[Required: High Availability EBC] The system shall synchronize the primary and backup call processors so that in the event of a failover between the primary and backup processors, active sessions are not lost.

[Required: Medium Availability EBC] The system does not require synchronization between the primary and backup call processors so that in the event of a failover between the primary and backup processors, active sessions may be lost.

5.3.2.15.7 IEEE 802.1Q Support

[Required: EBC] The system shall be capable of supporting the IEEE 802.1Q 2-byte Tag Control Information (TCI) Field 12-bit Virtual Local Area Network (VLAN) Identification (ID) (VID).

NOTE: The VID field has 12 bits and allows the identification of 4096 (2^{12}) VLANs. Of the 4096 possible VIDs, a VID value of 0 and 4095 (FFF) are reserved, so the maximum possible VIDs are 4094. The component must be capable of distinctly tagging each media (i.e., voice, video, data, signaling, and network management) with any of the 4094 VIDs.

5.3.2.15.8 Packet Transit Time

[Required: EBC] The system shall be capable of receiving, processing, and transmitting an RTS packet within 2 ms to include executing all internal functions.

NOTE: Internal functions do not include DNS lookups and other external actions or processes.

5.3.2.15.9 H.323 Support

[Conditional: EBC] If the EBC supports H.323 video, then the system shall be capable of processing and forwarding H.323 messages in accordance with UCR 2008, Section 5.4, Information Assurance Requirements.

5.3.2.16 World Wide Numbering and Dialing Plan

[Required: LSC, MFSS, EI] The precedence level and dialed number input to the EI shall be as specified in UCR 2008, Section 5.2.3.5.1.2, Interswitch and Intraswitch Dialing.

5.3.2.16.1 DSN Worldwide Numbering and Dialing Plan

[Required: LSC, MFSS] The DSN Worldwide Numbering and Dialing Plan will be used as the addressing schema within the current DSN and its migration into the SIP environment. The highlights of the DSN Worldwide Numbering and Dialing Plan are summarized in the following paragraphs; the detailed specifications of this plan are provided in UCR 2008, Section 5.2, Circuit-Switched Capabilities and Features. The LSC shall operate with the dialing format illustrated in Table 5.3.2-51, DSN User Dialing Format. The parts shown in parentheses may not be dialed by the DSN user on all calls.

Table 5.3.2-51. DSN User Dialing Format

ACCESS DIGIT	PRECEDENCE OR SERVICE DIGIT	ROUTE CODE	AREA CODE	SWITCH CODE	LINE NUMBER
(N)	(P or S)	(1X)	(KXX)	KXX	XXXX
where: P is any precedence digit 0–4 and will be used on rotary-dial or 12-button DTMF keysets. S is the service digit 5–9. N is any digit 2–9. X is any digit 0–9. K is any digit 2–8.					
NOTES: 1. Digits shown in parentheses are not dialed by the DSN user on all calls. 2. The Access Digit plus the Precedence or Service Digit constitute the Access Code.					

The highlights of the DSN Worldwide Numbering and Dialing Plan are described as follows:

1. The current DSN numbering plan will be used in the foreseeable future by DISN Assured Services users as the means of specifying a called party address within the converged DISN. (Simply stated, an originating user will dial a DSN telephone number.) That means the subscriber's telephone number will be used as a basis for routing call requests within the AS-SIP-based converged network. The following attributes are associated with the DSN numbering plan:

    a. The internal DSN numbering plan is a private network plan (internally, a DSN number is not an E.164 number), which is modeled after the North American Numbering Plan (NPA-NNX-XXXX). Internally within the DSN, the DSN numbers are not part of the E.164-based global numbering plan, therefore, internally within the DSN, addressing will be based on a "SIP URI" employing the "tel URI" with "phone context = 'dsn'" and not the Electronic Numbering (ENUM) schema. The tel URI method will provide the flexibility required when the DSN numbering plan is expanded to allow variable numbering schemes that will be used in support of coalition partner networks. The rationale is outlined as follows:

        (1) Most all DSN telephones can be direct dialed from the PSTN/ PTT telephone; in addition to being direct dialed from internal DSN telephones. This is made possible because the PSTN/PTTs have assigned public telephone numbers to most DSN locations. The PSTN/PTT numbers are part of the global PSTN/PTT E.164 numbering plan. This is significant, because in the future, the PTTs can use the ENUM scheme within their own IP-based networks to address DSN numbers.

        (2) The DSN telephone number is the fundamental and globally unique address element of both the TDM and VoIP (e.g., SIP) based real-time DSN.

Examples of internal DSN telephone numbers and their corresponding numbers, which are used when dialing through the PSTN, are illustrated in Table 5.3.2-52, Examples of Internal DSN Numbers and Their Corresponding Global E.164 PSTN Telephone Numbers.

2. Next, it is important to understand the relationship between basic SIP addressing, subscriber identification, and the existing DSN addressing plan and how it will be used as part of the SIP signaling messages. NOTE: The following examples use the SIP connotation.

Table 5.3.2-52. Examples of Internal DSN Numbers and Their Corresponding Global E.164 PSTN Telephone Numbers

COUNTRY/ DSN LOCATION	CIVILIAN E.164 NUMBERS	DSN INTERNAL PRIVATE NUMBER
U.S./Scott AFB	+(1) 618-229-xxxx	(312) 779-xxxx
U.S./Wheeler AAF	+(1) 808-656-xxxx	(315) 456-xxxx
Germany/ Patch Barracks	+(49) 711-68639-xxxx	(314) 430-xxxx
Bahrain/TCCC	+(973) 1785-xxxx	(318) 439-xxxx
Korea/Yongsan Main	+(822) 7913-xxxx	(315) 723-xxxx

a. The simplest form of a SIP signaling message is:

sip:sgtbill@patch.eur.dsn.mil

This is sgtbill's sip identity. (Note the absence of a telephone number.)

b. The sip identity is a type of URI called a SIP URI (RFC 3261, Section 19.1, SIP and SIPS (Session Initiation Protocol Secure) Uniform Resource Indicators (URI)).

c. The SIP URI has a form similar to an e-mail address, typically containing a username and a host name. In the above example, patch.eur.dsn.mil is the domain of sgtbill's SIP service provider (e.g., the LSC at Patch Barracks in the European Theater DSN within the .mil top-level domain).

3. The addressing system needs to correlate sgtbill's telephone number as part of the SIP URI (sip:sgtbill@patch.eur.dsn.mil). This can be accomplished by analyzing the SIP URI format outlined as follows (RFC 3261, Section 19.1, SIP and SIPS Uniform Resource Indicators):

a. The SIP URI general form is as follows:

sip:user;password@host:port;uri-parameters?headers

(1) User: This is the identifier of a particular resource at the host being addressed.

The userinfo part of a URI consists of the following:

User field, Password field, and the @ sign following them.

NOTE: The RFC does not recommend using the Password field.

(2) The "Host" field represents the host (LSC) providing the SIP resources. The Host field contains either an FQDN, an IPv4 address, or IPv6 address. The RFC recommends using an FQDN for the Host field.

(3) Because we are addressing hosts that can process telephone numbers (e.g., an LSC), we will use a "telephone-subscriber" field to populate the "user" field. [RFC 3966] This is accomplished by using the tel URI.

(a) The tel URI specifies the telephone number as an identifier.

(b) The termination point of the tel URI telephone number is not restricted. It can be in the public telephone network, a private telephone network, or the internet.

(c) It can be fixed or wireless and address a fixed wired, mobile, or nomadic terminal.

(d) The terminal addressed can support any electronic communication service, including voice, data, and fax.

(e) The tel URI specifies the telephone number as an identifier, which can be either globally unique, or only valid within a local context.

In summary, the tel URI allows us to bring a DSN telephone number into the internal DSN SIP addressing schema.

4. RFC 3966 defines the extent to which a telephone number is valid within a private network (e.g., a "local" number), or as a number part of the global public telephone system (e.g., a "global" number).

a. The DSN, being a private line network (although geographically it is a global network), with an internal standard numbering plan recognized by all DSN voice service locations, allows the definition of the entire DSN numbering plan as "local" telephone numbers at all LSCs in accordance with RFC 3966.

b. Local telephone numbers must have a "phone context" parameter that identifies the scope of their validity. Standard 10-digit DSN numbers are valid throughout the DSN, and thus, the phone context parameter becomes phone-context=dsn.mil.

Therefore, an example of a SIP URI containing a 10-digit DSN number becomes:

sip:3144301123;phone-context=dsn.mil

Finally, there are two ways for SIP signaling to search for the called subscriber.

sip:sgtbill@patch.eur.dsn.mil becomes:

sip:3144301123;phone-context=dsn.mil@patch.eur.dsn.mil;user=phone

5. There are two ways of using the SIP URI to direct the network-wide search for the SIP end point address, i.e., by NPA NNX or by a combination of a "username" (sgtbill) in conjunction with the FQDN assigned to an LSC (patch.eur.dsn.mil). In the foreseeable future, call requests will be forwarded (routed) based on the telephone number contained within the SIP request.

Table 5.3.2-53, Mapping of DSN tel Numbers to SIP URIs, provides examples of DSN numbers using SIP URIs that use the syntax defined in RFC 3966 and referenced in RFC 3261, Section 19.1.6.

Table 5.3.2-53. Mapping of DSN tel Numbers to SIP URIs

ALIAS TYPE	SIP URI
7-digit intradomain (LSC enclave) call	sip:4305335;phone-context=dsn.mil@patch.eur.dsn.mil;user=phone
7-digit interdomain (LSC enclave) call within same area code	sip:4801235;phone-context=dsn.mil@rsx.eur.dsn.mil;user=phone
10-digit interdomain (LSC enclave) call to another area code	sip:3157261135;phone-context=dsn.mil@ysm.pac.dsn.mil;user=phone

[Required: LSC, MFSS] The CCA shall allow session requests from LSC, MFSS EIs, other appliances, and MFSS MGs to contain

- Called addresses including DSN numbers from the DSN numbering plan, and
- Called addresses including E.164 numbers from the E.164 numbering plan.

NOTE: The LSC and MFSS may require the use of a DSN escape code, such as "98" or "8" as a prefix to a DSN number from the DSN numbering plan.

NOTE: The LSC and MFSS may require the use of a PSTN escape code, such as "99" or "9" as a prefix to an E.164 number from the E.164 numbering plan.

[Required: LSC, MFSS] When a session request's called address includes a DSN number from the DSN numbering plan, the CCA shall determine whether the called DSN number is local to the LSC or MFSS, or external to the LSC or MFSS.

If the called DSN number is local to the LSC or MFSS, the CCA shall complete the session request within the LSC or MFSS.

If the called DSN number is external to the LSC or MFSS, the CCA shall route the session request outside of the LSC or MFSS, using either of the following:

- The external IP address of the next appliance (i.e., LSC or MFSS) that should handle the session request, or

- The local IP address of the LSC or MFSS MG and MG trunk group that should handle the session request.

[Required: LSC, MFSS] When a session request's called address includes an E.164 number from the E.164 numbering plan, the CCA shall determine whether the called E.164 number is local to the LSC or MFSS, or external to the LSC or MFSS.
If the called E.164 number is local to the LSC or MFSS, the CCA shall complete the session request within the LSC or MFSS.

If the called E.164 number is external to the LSC or MFSS, the CCA shall route the session request outside of the LSC or MFSS, using either of the following:

- The external IP address of the next signaling appliance that should handle the session request, or

- The local IP address of the LSC or MFSS MG and MG trunk group that should handle the session request.

5.3.2.16.1.1 CCA and GLS Support for Dual Assignment of DSN and E.164 Numbers to MFSS EIs

[Required: LSC, MFSS] The CCA shall allow each VoIP and Video EI served by an LSC or MFSS to have both a DSN number assigned and an E.164 number assigned.

[Required: LSC, MFSS] For VoIP and Video EIs that have both a DSN number and an E.164 number assigned, the CCA shall be able to match each EI's DSN number with its E.164 number, and to match each EI's E.164 number with its DSN number.

5.3.2.16.1.2 CCA Differentiation between DSN Numbers and E.164 Numbers

[Required: LSC, MFSS] The CCA shall be able to distinguish DSN called numbers from E.164 called numbers, when processing VoIP and Video session requests from EIs, EBCs, and MG trunk groups.

[Required: LSC, MFSS] The CCA shall be able to distinguish local DSN called numbers from external DSN called numbers, when processing VoIP and Video session requests from EIs, EBCs, and MG trunk groups.

[Required: LSC, MFSS] The CCA shall be able to distinguish local E.164 called numbers from external E.164 called numbers, when processing VoIP and Video session requests from EIs, EBCs, and MG trunk groups.

[Objective: LSC, MFSS] On SIP and AS-SIP calls from EIs and the EBC, it is desirable that the CCA (and its LLS and GLS Servers) use the contents of the phone-context parameter in the called SIP URI to determine

- Whether the session request is intended for a DSN number or an E.164 number, and
- In the E.164 case, whether the E.164 number is locally significant, nationally significant, or internationally significant.

[Conditional: MFSS] On DoD CCS7 calls from an MFSS MG, the CCA shall use the contents of the Nature of Address Indicator and Numbering Plan fields in the ISUP Called Party Number parameter in the IAM to determine

- Whether the call request is intended for a DSN number or an E.164 number, and
- In the E.164 case, whether the E.164 number is locally significant, nationally significant, or internationally significant.

[Required] On ISDN PRI calls from an MFSS MG, the CCA shall use the contents of the Type of Number and Numbering Plan Identification fields in the ISDN Called Party Number IE in the SETUP message to determine

- Whether the call request is intended for a DSN number or an E.164 number, and

- In the E.164 case, whether the E.164 number is locally significant, nationally significant, or internationally significant.

[Conditional] On CAS trunk calls from an MFSS MG, the CCA shall use the identity of the trunk group that the call was received on (and the presence or absence of prefix digits in the received Called Party Number) to determine

- Whether the call request is intended for a DSN number or an E.164 number, and

- In the E.164 case, whether the E.164 number is locally significant, nationally significant, or internationally significant.

5.3.2.16.1.3 CCA Use of SIP "phone-context" to Differentiate between DSN and E.164 Numbers

[Objective] On SIP and AS-SIP calls from MFSS EIs and other appliances, it is desirable that the MFSS CCA use the contents of the "phone-context" parameter in the called SIP URI to distinguish DSN numbers from E.164 numbers as follows:

1. If the "phone-context" parameter in the "User" portion of the called SIP URI indicates "dsn.mil" (or a subordinate domain name built on "dsn.mil"), then the CCA shall treat the 10-digit number that precedes the "phone-context" parameter as a DSN number.

2. If the "phone-context" parameter in the "User" portion of the called SIP URI indicates a sequence of digits, possibly prefixed with a "+" character, then the CCA shall treat the variable length number that precedes the "phone-context" parameter as an E.164 number.

[Objective] On SIP and AS-SIP calls from MFSS EIs and other appliances, it is desirable that the MFSS CCA use the contents of the "phone-context" parameter in the called SIP URI to distinguish local, national, and international E.164 numbers from one another as follows:

1. If there is no "phone-context" parameter in the "User" portion of the called SIP URI, then the CCA shall treat the variable length number in the "User" portion of this URI as an international E.164 number.

2. If the "phone-context" parameter in the "User" portion of the called SIP URI contains a "+" character followed by an E.164 country code, but no area code or city code, then the CCA shall treat the variable length number that precedes the "phone-context" parameter as a national E.164 number (for the country identified by the country code).

3. If the "phone-context" parameter in the "User" portion of the called SIP URI contains a "+" character followed by an E.164 country code and an area code or city code, then the CCA shall treat the variable length number that precedes the "phone-context" parameter as a local E.164 number (for the country identified by the country code, and the area or city identified by the area code or city code).

5.3.2.16.1.4 Use of SIP URI Domain Name with DSN Numbers and E.164 Numbers

The SIP URIs used for VVoIP calls contain both a username (with a numeric Called Party Number and an optional "phone-context" parameter) and a domain name, such as "patch.eur.dsn.mil" or "ysm.pac.dsn.mil". Signaling appliances need some mechanism to accept, reject, or overwrite the domain name values received as part of Called SIP URIs in each VoIP and Video session request.

[Required: LSC, MFSS] Each signaling appliance shall support a configurable per-appliance parameter that indicates how the appliance handles domain names received in VoIP and Video session requests. (Support for this parameter is not a Requirement for UC Spiral 1.)

This parameter, named "Domain Name Treatment for Session Requests," shall support the following values:

- Overwrite with Network FQDN
- Overwrite with Appliance FQDN
- Pass-through

The default value shall be Overwrite with Network FQDN.

To meet this requirement, the appliance must support all three of the above options, and must support the default parameter value of "Overwrite with Network FQDN." The appliance must allow the option selected to be software-configurable.

[Required: LSC, MFSS] When the value of the Domain Name Treatment for Session Requests parameter for the signaling appliance is Overwrite with Network FQDN, the appliance CCA shall discard all domain names received in Called SIP URIs in Session Requests, and overwrite them with the FQDN of the DoD Network that the appliance belongs to. (Support for this parameter value is not a Requirement for UC Spiral 1.)

[Required: LSC, MFSS] The appliance shall support a per-appliance parameter called the "RTS Network FQDN," to be used in overwriting the received domain names in this case. (Support for this additional parameter is not a Requirement for UC Spiral 1.)

The value of this parameter shall be a text string that identifies the FQDN of the DoD Network that the appliance belongs to, for domain name overwriting purposes. At a minimum, the following FQDNs for DoD Networks (i.e., DSN, DRSN) shall be supported: "dsn.mil" and "drsn.mil".

[Required: LSC, MFSS] When the value of the Domain Name Treatment for Session Requests parameter for the appliance is Overwrite with Appliance FQDN, the appliance CCA shall discard all domain names received in Called SIP URIs in Session Requests, and overwrite them with the FQDN of the appliance. (Support for this parameter value is not a Requirement for UC Spiral 1.)

[Required: LSC, MFSS] The appliance shall support a per-appliance parameter called the "Appliance FQDN," to be used in overwriting the received domain names in this case. (Support for this additional parameter is not a Requirement for UC Spiral 1.)

The value of this parameter shall be a text string that identifies the FQDN of the appliance, for domain name overwriting purposes. Examples of possible FQDNs for appliances (i.e., LSCs, MFSSs) are as follows:

- "lsc10.mfss20.patch.germany.eur.dsn.mil" (LSC 10, subordinate to MFSS 20, located at the Patch Barracks in Germany in the European Theater on the DSN)

- "lsc20.lsc30.mfss40.ysm.korea.pac.dsn.mil" (LSC 20, subordinate to LSC 30, subordinate to MFSS 40, located at Yongsan Main in South Korea in the Pacific Theater on the DSN)

- "mfss50.scott.cent.conus.dsn.mil" (MFSS 50, located at Scott Air Force Base in Central CONUS on the DSN)

[Required: LSC, MFSS] When the value of the Domain Name Treatment for Session Requests parameter for the appliance is "Pass-through," the appliance CCA shall transparently pass-through all domain names received in Called SIP URIs in Session Requests, without altering them. (Support for this parameter value is not a Requirement for VVoIP Spiral 1.)

5.3.2.16.1.4.1 SIP URI Domain Names in UC Spiral 1

[Required: LSC, MFSS] For UC Spiral 1, the MFSS or LSC is only required to support one network FQDN for use with SIP URI domain names: "dsn.mil" if that appliance is used for SBU traffic, and "drsn.mil" if that appliance is used for classified traffic.

[Required: LSC, MFSS] For UC Spiral 1, the MFSS or LSC is required to ensure that all AS-SIP session requests entering or leaving that appliance use the network FQDN of that appliance (i.e., "dsn.mil" for SBU traffic, or "drsn.mil" for classified traffic) as the domain name in Called SIP URIs.

In cases where a received Called SIP URI in a received AS-SIP message has a domain name other than "dsn.mil" (for SBU traffic) or "drsn.mil" (for classified traffic), the MFSS or LSC shall either

1. Reject the AS-SIP session request that contained the unexpected domain name, or

2. Accept the AS-SIP session request that contained the unexpected domain name, but overwrite the received domain name with "dsn.mil" (for SBU traffic) or "drsn.mil" (for classified traffic).

Future versions of the UCR document will give additional detail on requirements for the support of SIP URI domain names that are different from "dsn.mil" and "drsn.mil".

5.3.2.16.1.5 Domain Directory

Prior to discussing directories and directory services, it is important to understand that within the IP telephony environment, directories and directory services are not required or used for processing and routing of telephone call requests. Rather, the term directory services refer to the capability of using an IP telephone or other voice and/or video end points for looking up user information directly to obtain a user's telephone numbers (often referred to as "white pages" service). This eliminates the need for dialing an operator or using a hard copy telephone book to obtain this information.

[Required: LSC, MFSS] All voice systems, TDM or IP technology-based, must contain subscriber assignment information.

Traditionally, the subscriber assignment information contained within telephone switching systems consisted of just the subscriber telephone number, line equipment assignment, and subscriber calling classmarks. Typically, data elements, such as the subscriber name, physical address, e-mail address, or department code, were not part of the subscriber line assignment information. An internal table structure, rather than embedded databases, was used by the switching system to store this information.

Most all new IP-based VoIP systems have the capability to store subscriber name, physical address, e-mail address, and/or department code in addition to the basic traditional assignment information as part of the subscriber information. Rather than using a table structure, the new

systems store this information as embedded databases, often referred to as "directories" as part of the LSC complex. An example of the embedded subscriber line database would be a Lightweight Directory Access Protocol (LDAP)-compliant format. This arrangement of a subscriber line database represents a more "open standard" than a current TDM system's unique arrangement of using a table-based internal call processing structure.

The discussion of LDAP-based subscriber line databases here applies to strategic appliances only, and not to tactical appliances. Requirements for subscriber line databases for tactical appliances are candidates for a future version of this document.

When the LSC uses an LDAP (or other open standard)-based structure to store subscriber line data, this data can be imported easily from, or exported to, other external LDAP-based structures. The LDAP-based directories are extensible and multiple entries of "telephony" data can be added in batch mode, or additional attributes can be added to an existing LDAP directory using LDAP Interchange Format (LDIF) files. Consequently, when installing a new VoIP system, a subset of the subscriber line information can be extracted from an existing corporate directory (if it contains subscriber telephone number information) and automatically loaded into a new VoIP system. This represents a labor saving over having to manually build a portion of the subscriber information database.

Pure IP-based systems often have a built-in feature allowing importing and exporting of relevant telephone subscriber information between the VoIP system and an existing external "enterprise directory." Telephony-related data is usually stored in a single branch of the enterprise directory (referred to as the IP Telephony Network Branch). This enterprise directory is often a corporate e-mail directory. To facilitate data transfer, both the VoIP system subscriber database and the external corporate directory conform to a common standard.

Most VoIP systems provide instruments that can provide access to a "directory" function. These telephones have a display where alphanumeric information, such as telephone numbers and subscriber names, can be shown. A user can access the directory function via a dedicated button or via soft keys. Then the VoIP system connects the telephone to the directory portion of the subscriber line database. Then the user can initiate a directory search from the telephone. This search is performed against subscriber data contained within the LSC where the telephone is registered.

Additionally, VoIP systems have a feature allowing their instruments to access a Web browsing capability. Since a VoIP telephone is connected to a LAN to obtain voice services through the LSC, a VoIP telephone also may be allowed to access an external directory server. This opens up possibilities: If the external directory server is accessible from the LAN, the IP telephone user may be allowed to browse to the corporate directory and perform a search of that directory as well as the LSC-contained directory.

A domain directory should allow the following functions:

1. Allow a user assigned to an LSC to look up the telephone numbers of other users assigned to (served by) that common LSC. This function is referred to as "white pages" services and it should not be confused with call routing tables used for forwarding SIP call requests.

2. For security reasons, the Directory Look-Up function will only be available from a user's IP telephone instrument, not via the Internet. The IP telephone instrument will contain a small display and function keys that facilitate the Directory Look-Up function.

3. Access to the Directory Look-Up function shall be controlled by subscriber classmarks. There may be specific reasons for denying this privilege to certain users.

4. The LSC shall allow the system administrator to update the directory database in response to service order activity (i.e., subscriber adds, moves, changes, or removals). The LSC shall update the white pages data automatically as well as subscriber line information contained as part of the Directory Look-Up function.

5. When automatic instrument registration is allowed using Dynamic Host Configuration Protocol (DHCP), a service order "flag" must be sent to the system administrator terminal so the administrator can update the subscriber's location information as necessary.

6. The data elements, shown in Table 5.3.2-54, shall be incorporated as part of the white pages directory portion of the LSC subscriber database.

Table 5.3.2-54. White Pages Directory Data Elements

DATA ITEM	EXAMPLE
USER 10-DIGIT DSN TELEPHONE NUMBER	315-454-1192
USER ORGANIZATION CODE	SCX
ORGANIZATION NAME	1st Comm Squadron
USER GEOGRAPHIC LOCATION	Langley AFB
USER NAME	Civ Bill Smith

7. In the near-term planning horizon, the local directory contained within an LSC will not be required to automatically send updates to a "global directory" database, but planning should allow for this in the future. Then the automatic update shall be performed at a defined interval (e.g., weekly) using an automated electronic transfer of data. The transfer will be under the control of a system administrator responsible for the global directory.

8. It is anticipated that long-range functionality should be provided so that the "telephone part" of the LSC directory can be imported to an external "corporate" (e-mail) directory.

(NOTE: It is anticipated that the external DSN directory will be a branch of the GIG directory under development by the Net-Centric Enterprise Services (NCES) effort.) This function will require that the external directory is based on common standards, for example LDAP, and that the administrator in charge of the external directory extends the directory schema to add new object classes for storing the user telephony information. Likewise, the LSC must have stored the subscriber directory information previously in an LDAP-based system as outlined previously under item 6. Under these conditions, an LDIF file can be used to facilitate the upload of multiple entries in batch mode, or add the telephony attributes to the existing external LDAP directory.

The material here on exporting an LSC directory to an external "corporate" directory (and storing subscriber directory information in an LDAP-based format) applies to strategic appliances only, and not to tactical appliances. Requirements for LSC directory exports for tactical appliances are candidates for a future version of this document.

9. The user should be offered the following ways of searching for local (domain) directory information:

   a. User access to the local domain directory is provided by a "directory" feature available on the VoIP instrument. Directory search will be limited to information contained within the LSC subscriber information.

   b. The basic search may be made based on Last Name, First Name.

   c. The advanced search utility should have a built-in Boolean logic to perform searches using OR with multiple entries in a single field and AND across fields.

5.3.2.16.1.6 Global Directory Services

A global directory service should not be confused with the directory itself, which is the database that holds the information about objects that are to be managed by the directory service. The global directory service is the interface to the directory and provides access to the data that is contained in that directory. It acts as a central authority that can securely authenticate resources and manage identities and relationships between them.

A directory service is highly optimized for reads and provides advanced search on the many different attributes that can be associated with objects in a directory. The data that is stored in the directory is defined by an extendable and modifiable schema. Directory services use a distributed model for storing their information and that information is usually replicated between directory servers.

[Objective: MFSS] A global directory services system shall allow the following functions and interfaces:

1. Allow a DSN user to perform a DSN-wide telephone number look-up for a user assigned anywhere on the DSN. This function is referred to as white pages services, and it should not be confused with call routing tables used for forwarding of SIP call requests.

2. For security reasons, the telephone directory look-up function will only be available from a user's telephone instrument, not via the Internet.

3. Access to the Directory Look-Up function shall be controlled by subscriber classmarks. There may be specific reasons for denying this privilege to certain users.

4. A global search capability will require multivendor interoperability among LSCs. This will be made feasible by using standardized formats (e.g., LDAP-based) for storing directory data within an LSC.

5. A global search capability should allow a user to search using the basic or advanced search methods outlined in UCR 2008, Section 5.3.2.16.1.5, Domain Directory, item 9, as well as by specifying the "name" of an LSC (e.g., patch.eur.dsn.mil). This capability will require that an LSC extend a directory search request through the signaling network.

6. In the near-term planning horizon, the local directory contained within an LSC will not be required to automatically send updates to a "global directory" database, but planning should allow for this in the future. Then the automatic update shall be performed at a defined interval (e.g., weekly) using an automated electronic transfer of data. The transfer will be under the control of a system administrator responsible for the global directory.

7. It is anticipated that long-range functionality should be provided so the "telephone part" of the local directory can be imported to an external local "corporate" e-mail directory. (NOTE: It is anticipated that the external DSN directory will be a branch of the GIG directory under development by the NCES effort.) This function will require that the external directory is based on a common standard, (E.G., LDAP), and that the administrator in charge of the external directory extends the directory schema to add new object classes for storing the user telephony information. Likewise, the LSC must store the subscriber directory information outlined previously under item 6 using a common standard (e.g., LDAP-based). Under these conditions, an LDIF file can be used to facilitate the upload of multiple entries in batch mode, or add the telephony attributes to the existing external directory.

8. In the near-term planning horizon, the domain directories will not be required to automatically send updates to a global directory database, but planning should allow for this in the future. The automatic update shall be provided at a defined interval (e.g., weekly) using an automated electronic transfer of data.

9. The location and administration responsibilities and standard to be used for the global directory database and server have yet to be determined.

5.3.2.17 Management of Network Appliances

Figure 5.3.2-19, Network Appliance Management Model, is a logical view of a network appliance with an emphasis on its management functions. The internal implementations of the management functions are determined by the appliance supplier and may or may not align with Figure 5.3.2-19.

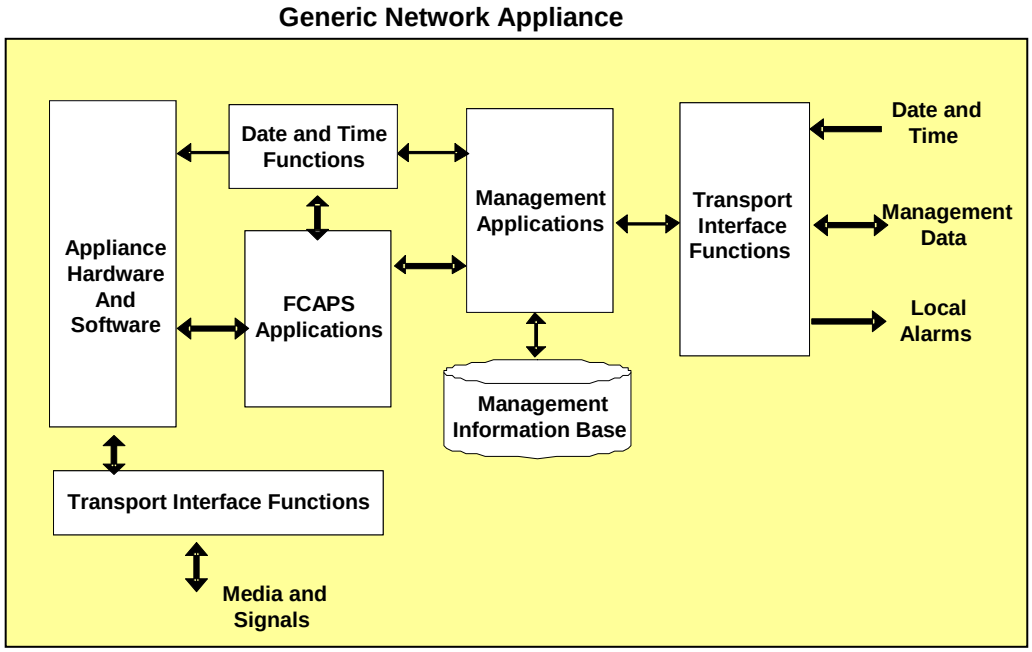


Figure 5.3.2-19. Network Appliance Management Model

This document makes no assumptions about the number of physical components that constitute a network appliance or of the spatial distribution of these components.

All internal interactions are determined by the supplier and are out of the scope of this document.

Figure 5.3.2-19 is a functional model and does not require that the Network Appliance Management functions be internal to the appliance. However, the figure does imply that

interfaces between the management functions and the appliance's hardware and software elements are closed.

In this section, the management requirements are frequently specified in terms of network appliances, or network elements (NEs). It is understood that these requirements refer to the management functions associated with the network appliance, or NE.

5.3.2.17.1 Voice and Video Network Management Domain

End-to-end NM of DISN Voice and Video services will be provided by DISA using the End-To-End RTS Element Management System (E2E RTS EMS). Figure 5.3.2-20, Manager – Managed Device Communications, is a high-level view of the communications network used by the E2E RTS EMS and the managed appliances within the scope of this document.

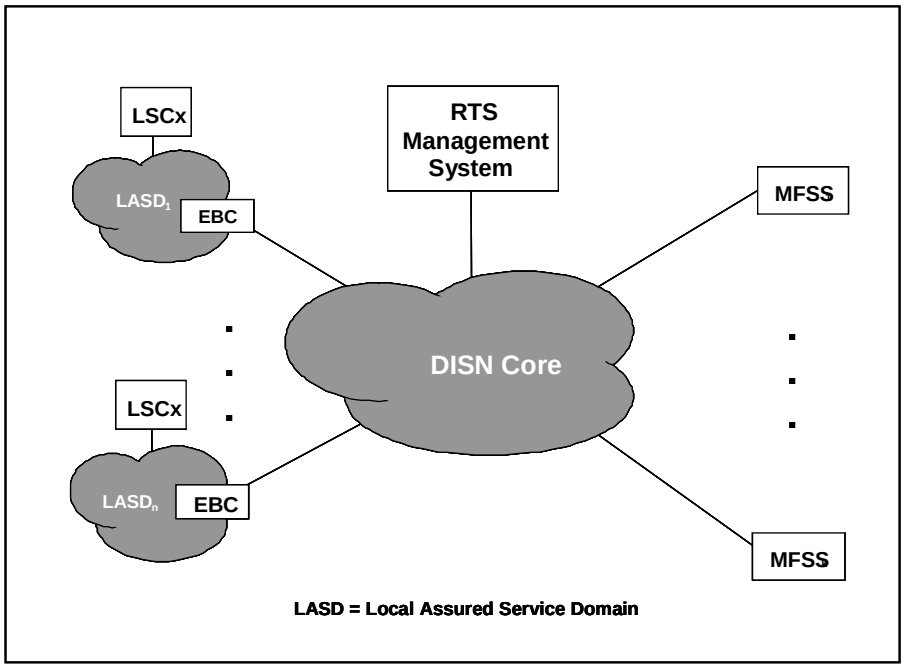


Figure 5.3.2-20. Manager – Managed Device Communications

Figure 5.3.2-20 does not imply that the E2E RTS EMS is a centralized system. In those instances where the E2E RTS EMS is distributed over a number of elements, it is assumed that the managed appliances have been configured with the IP address of the appropriate management element.

5.3.2.17.2 General Management Requirements

This document assumes that all Voice and Video network switching appliances meet the requirement in UCR 2008, Section 5.2.8.1, DISA/DSN Network Management.

Except where otherwise specified, Telcordia Technologies Technical Reference TR-740 shall guide the interface between the network appliances (or components) and the external E2E RTS EMS.

Network and Systems Management are common across all DISN components in the VVoIP solution, including the MFSS and its elements, the LSC and its elements, the CE Router, and the EBC. The MFSS and LSC components shall each have an individual pair of Ethernet interfaces for management purposes, even in cases where the MFSS or LSC component contains multiple physical devices. It is understood that the EBC and the CE Router shall each have their own individual pair of Ethernet management interfaces.

[Required] The MFSS and LSC components shall support one pair of Ethernet management interfaces at the component level (not at the device level). One of these Ethernet management interfaces shall be used for component-level communication with a Local Element Management System (Local EMS). The other Ethernet management interface shall be used for component-level communication with the remote E2E RTS EMS. The MFSS and LSC components shall also support at least one additional Ethernet interface at the component level (not the device level) to carry the signaling and media streams for VVoIP traffic.

[Required] The EBC and CE Router components shall support one pair of Ethernet management interfaces at the component level. One of these Ethernet management interfaces shall be used for component-level communication with a Local EMS. The other Ethernet management interface shall be used for component-level communication with the remote E2E RTS EMS. The EBC and CE Router components shall also support at least one additional Ethernet interface at the component level to carry the signaling and media streams for VVoIP traffic.

[Required] A network appliance shall have Operations interfaces that provide a standard means by which management systems can directly or indirectly communicate with and thus manage the various network appliances in the DISN.

[Required] The physical interface between the Local EMS and the VVoIP network components (i.e., LSC, MFSS, EBC, CE Router) shall be a 10/100 Mbps Ethernet interface. The physical interface between the DCN serving the E2E RTS EMS and the VVoIP network components shall also be a 10/100 Mbps Ethernet interface. The physical interface shall work in either of the two

following modes using auto-negotiation: IEEE, *Ethernet Standard 802.3*, 1993, or IEEE, *Fast Ethernet Standard 802.3u*, 1995.

[Required] There shall be a local craftsperson interface (Craft Input Device (CID)) for Operations, Administration, and Management (OA&M) for all VVoIP network components. The CID is a supplier-provided input/output device that is locally connected to a network component. The CID may be connected to the Local EMS, which is in turn connected to the VVoIP component using the Local EMS Ethernet management interface. The CID may be connected directly to the VVoIP network component also, using the Ethernet management interface on the component that would otherwise be used by the Local EMS (there is no Local EMS in this case). The CID may be connected directly to the VVoIP network component using a separate serial interface.

[Required] The network appliances shall provide NM data to the external E2E RTS EMS.

[Required] A network appliance shall communicate with an external Voice and Video management system by means of a well-defined standards-based management interface using an industry accepted management protocol.

While the majority of management applications will use an interactive mode of communication, there will be some management applications (e.g., transfer of bulk performance information, downloading software generics) will use file-oriented communications.

[Required] Communications between E2E RTS EMS and the VVoIP network appliances shall be via IP.

Where an EMS is the interface with a VVoIP component, the Transmission Control Protocol (TCP)/IP-based communications between the E2E RTS EMS and the EMS shall be via:

- **[Required: NM]** Extensible Markup Language (XML)
- **[Objective FY12: NM]** Multi-Technology Operations System(s) Interface (MTOSI)

[Objective] In order to support file-oriented communications, it is desirable that a network appliance support the File Transfer Protocol (FTP).

[Required] A network appliance shall issue state change notifications for changes in the states of replaceable components including changes in operational state or service status, and detection of new components.

[Required] A network appliance shall be provisioned by the E2E RTS EMS with the address, software, and Open Systems Interconnection (OSI) Layer 4 port information associated with its Core Network interfaces.

[Required] A network appliance shall be capable of maintaining and responding to E2E RTS EMS requests for resource inventory, configuration, and status information concerning Core Network interface resources (e.g., IP or Media Access Control (MAC) addresses) that have been installed and placed into service.

[Required: LSC, MFSS] Network appliances that provide voice and video call service shall have the capability to invoke traffic flow (NM) controls as detailed in UCR 2008, Section 5.3.2.18, Network Management Requirements of Appliance Functions.

[Required] A network appliance shall be capable of setting the Administrative state and maintaining the Operational state of each Core Network interface, and maintaining the time of the last state change.

[Required] A network appliance shall generate an alarm condition upon the occurrence of any of the following failure conditions, as defined in ITU-T Recommendation M.3100:

- Power loss
- Environmental condition not conductive to normal operation
- Loss of data integrity

[Required] A network appliance shall be capable of maintaining and responding to requests for physical resource capacity information for installed components. This information includes the following:

- Component type and model
- Shelf location
- Rack location
- Bay location

5.3.2.17.3 Requirements for FCAPS Management

The requirements for the five general functional areas of FCAPS management involve the CCA, SG, and MG functions. Detailed descriptions of how these functions support the FCAPS management requirements are provided in separate sections of this UCR 2008 as follows:

1. Section 5.3.2.18.1, Management Requirements of the CCA Function, contains management requirement for the CCA function.

2. Section 5.3.2.18.2, Management Requirements of the SG Function, contains management requirements for this SG function.

3. Section 5.3.2.18.3, Management Requirements of the MG Function, contains the management requirements for the MG function.

General requirements for the five management functional areas are defined in the following sections.

5.3.2.17.3.1 Fault Management

Fault Management supports the detection, isolation, and correction of abnormal operating conditions in a telecommunications network and its environment. Fault Management provides the functions to manage service problems, to support customer interactions associated with service troubles, and to support business policies related to service problems.

5.3.2.17.3.1.1 Alarm Messages

[Required: NM] Alarm messages must be distinguishable from administrative log messages.

5.3.2.17.3.1.2 Self-Detection of Fault Conditions

[Required: NM] The Network elements shall detect their own fault (alarm) conditions.

5.3.2.17.3.1.3 Alarm Notifications

[Required: NM] The network elements shall generate alarm notifications.

5.3.2.17.3.1.4 Near-Real Time Alarm Messages

[Required: NM] The network elements shall send the alarm messages in near-real time. More than 99.95% of alarms shall be reported in near real time (NRT). NRT is defined as within 5 seconds of detecting the event, excluding transport time.

5.3.2.17.3.1.5 SNMP Version 2 and Version 3 Format Alarm Messages

The network components shall send alarm messages in:

- **[Required: NM]** SNMP Version 2 (SNMPv2) format
- **[Objective IOC, Required FOC: NM]** SNMP Version 3 (SNMPv3) format

5.3.2.17.3.2 Configuration Management

Configuration Management (CM) exercises control over, identifies, collects data from, and provides data to NEs and the connections between NEs. Configuration Management is responsible for the planning and installation of NEs and their interconnection into a network. Configuration Management includes the establishment of customer services that use the network, all services and product planning, and business policy level functions related to service establishment. Detailed CM support requirements of the CCA, SG, and MG functions are provided in separate sections as follows:

- UCR 2008, Section 5.3.2.18.1, Management Requirements of the CCA Function
- UCR 2008, Section 5.3.2.18.2, Management Requirements of the SG Function
- UCR 2008, Section 5.3.2.18.3, Management Requirements of the MG Function.

5.3.2.17.3.2.1 Read-Write Access to CM Data by the E2E RTS EMS

[Required: NM] Capability to access and modify configuration data by the E2E RTS EMS shall be controllable by using an access privileges function within the network appliance.

5.3.2.17.3.3 Accounting Management

Accounting Management enables the network service usage to be measured and the costs for such use to be determined. It provides facilities to collect accounting records and to set billing parameters for the usage of services and for access to the network. It also includes functionality to exercise control over the proper flow of funds within the enterprise and between the enterprise and its owners and creditors. Detailed requirements for Accounting Management including requirements related to call quality are found in UCR 2008, Section 5.3.2.19, Accounting Management.

5.3.2.17.3.4 Performance Management

Performance Management evaluates and reports the effectiveness with which the network and its NEs support assigned services. Performance Management provides mechanisms to measure service quality and provides the business policy functions for quality control. Detailed requirements for Performance Management interactions by the CCA, SG, and MG functions are provided in separate sections as follows:

- UCR 2008, Section 5.3.2.18.1, Management Requirements of the CCA Function
- UCR 2008, Section 5.3.2.18.2, Management Requirements of the SG Function
- UCR 2008, Section 5.3.2.18.3, Management Requirements of the MG Function.

5.3.2.17.3.4.1 Near Real Time Network Performance Monitoring

Near real time network performance monitoring is a subset of Performance Management. **[Required]** The E2E RTS EMS shall collect alarm messages in real time and selected performance data from the NEs on a near real time basis in 5- or 15-minute intervals. Network control personnel evaluate the alarm and performance data and, to minimize the impact on network traffic caused by a network anomaly, the control personnel implement traffic flow (NM) controls. The NEs must be capable of receiving and responding to NM controls from the E2E RTS EMS. The next section defines requirements for traffic flow (NM) controls.

5.3.2.17.3.4.2 Remote Network Management Commands

[Required: VVoIP NEs] The VVoIP NEs shall be able to receive and respond to remote NM commands. The commands are described in the following sections.

5.3.2.17.3.4.2.1 Comparison of Controls for Circuit-Switched and IP-Based Environments

The IP-based voice solution shall be able to exercise protective and expansive NM controls. (NOTE: Some controls used in the circuit-switched environment are not applicable in the IP-based voice environment because of the fundamental differences in how the two network environments operate.) The set of applicable IP-based traffic control capabilities and actions are outlined in the following paragraphs. The following descriptions and Table 5.3.2-55, Control Function Crosswalk: TDM to IP RTS, indicate which IP control actions (singularly and in combination), across the IP-based Voice solution, are necessary to mitigate or resolve the underlying situation for which each TDM equivalent control exists.

5.3.2.17.3.4.2.2 Automatic Congestion Controls

Within an IP network, the LSC handles only call signaling, while the IP network connecting the two communicating end instruments handles the bearer stream. The LSC congestion resulting from an overload of SIP requests must be detected and controlled. Bearer stream congestion will affect non-real time as well as real time bearer traffic, making it an IP NM concern. While good traffic engineering and the presence of an MPLS router core mitigates much of the traffic

congestion within LAN and WAN environments, congestion at the boundaries between these domains is of concern and needs specific detection and control actions to mitigate the congestion.

Local Session Controller congestion occurs when the volume of AS-SIP messages exceeds the LSC's capacity to process them. While a particular vendor's LSC solution may threshold and alarm on congestion, a simpler approach may be monitoring the CPU utilization on the LSC host. Alarms generated from CPU utilization threshold violations could be the trigger events necessary for the E2E RTS EMS to take the appropriate pre-emptive policy based management action to execute EI destination controls, limiting other LSCs and their EIs from sending SIP messages to the overloaded LSC. From the viewpoint of these other LSCs, in effect, a code control would be executed on them.

Detection of network congestion at the edge of the LANs and WAN (DISN Core) resides with the performance management tools in place over those networks. These performance management tools must detect and report (via SNMP or syslog events) bandwidth utilization threshold violations in each of the CE Router, Unclassified Internet Protocol Router Network (NIPRNet) Aggregation Router (AR)) traffic queues. For the AR Routers, this must be by a southbound (CE connected) interface. From these events, each domain's policy-based management system must take the appropriate (precoordinated) control actions to mitigate the congestion.

Given no change in the physical resources (i.e., a larger bandwidth connection between the LAN and WAN), three basic actions can be taken to reduce congestion at the network edge.

1. Reallocate the queue bandwidth on the CE and PE Routers.

2. Change the call budget on the LSC, with a corresponding change in the RTS queue bandwidths on the CE and PE Routers.

3. A code control could be put on other LSCs to reduce the load of SIP messages sent through the overloaded edge (although this would have minimal effect on reducing the bearer traffic, unless done in conjunction with a call budget and bandwidth change).

4. **[Required: LSC, MFSS**] When ASAC budgets are reduced, by NM action, below the current budget allocation, any previous sessions (regardless of precedence level) in excess of the new budget shall be allowed to terminate naturally. This assumes that the CE Router queue bandwidths would not be reduced until the LSC session count fell below or equal to the newly commanded reduced budget, to prevent the corruption of existing sessions.

In summary, three control actions can help reduce congestion in the IP-based voice network: implementing EI destination controls, call budget changes, and router queue bandwidth allocations. Each of these control actions is described in more detail in the following paragraphs.

5.3.2.17.3.4.2.3 Selective Incoming Load Controls

Like Automatic Congestion Controls (ACCs), Selective Incoming Load Controls (SILCs) are designed to protect the switches and their connecting circuits from overload (congestion) conditions when CCS7 is not available to signal the overload condition to the connected switches.

Within the IP environment, the same two forms of congestion that apply to ACC are of concern: LSC processor congestion and congestion across the LAN/WAN edge. The control solution that applies is similar to that of ACC.

While under SILC, LSC signaling of its congestion state to other LSCs cannot occur. Since LSC congestion can be detected and reported without SIP being involved, alarms generated from CPU utilization threshold violations could be the trigger events necessary for the E2E RTS EMS to take the appropriate policy-based management action to execute call destination controls (i.e., limiting other LSCs and their EIs from sending SIP messages to the overloaded LSC). From the viewpoint of these other LSCs, in effect, a code control would be executed on them. This does not mitigate a mass dialing event on base, where the EI generated AS-SIP messages would fill the base LSC's messaging queue, awaiting processing. This makes its handling effectively the same as under ACC.

Congestion across the LAN/WAN edge is detected and handled the same way as under ACC.

5.3.2.17.3.4.2.4 Trunk Reservation

The primary intent of trunk reservation is to reserve resources for handling specific mission requirements, such as bonding of DS0-level channels to create bandwidth and reserving trunks for a video teleconference.

Reservation of resources in the IP environment is done by controlling the call budget for the class of traffic requiring the reserved resources at the LSC and its associated bandwidth on the LAN CE Router and DISN PE Router queues.

5.3.2.17.3.4.2.5 Precedence Access Threshold

Precedence Access Threshold (which is no longer a requirement in the TDM switch network) does not apply to IP traffic. The number of simultaneous precedence calls onto/off of the base will only be limited by the total call budget for that base.

5.3.2.17.3.4.2.6 Essential Service Protection

Essential Service Protection (ESP), which, in TDM, "guarantees" an EI will get dial tone, even in case of emergency or switch congestion, applies differently to IP real time services.

The EI gets dial tone from itself, not the switch. The EIs are not connected to the LSC, but to the ASLAN, that the LSC is also connected. The first time the LSC knows an EI is "off hook" is when a number is dialed and the SIP INVITE request is sent to the LSC. In the VVoIP design, the LSC has no way of providing a priority queuing of SIP messages from one EI over another. The first time the LSC knows an EI needs service is when the SIP INVITE request is taken from the LSC's signaling queue and processed. If that particular EI has some service guarantee (over other EIs), then that EI really has an increased precedence over the others. NOTE: UCR 2008, Section 5.2.2, Multilevel Precedence and Preemption, already covers EI precedence and preemption.) The LSC signals for the call in accordance with the practices and procedures (P&P) rules. Even if the EI could some how be tagged with an ESP tag, there would be no way of advertising it to the LSC in advance of the SIP INVITE request, thereby providing that guarantee, other than what is already provided through precedence and preemption. Because of this, ESP applies only to service restoral for selected IP users. If an EI needs some level of call guaranteed service, then that EI's precedence level needs to be elevated so the LSC can take the appropriate preemption activity when that EI requests service.

5.3.2.17.3.4.2.7 Destination Code Controls

The TDM code controls are manual protective controls that restrict calls having code prefixes for destinations that have been temporarily designated as difficult or impossible to reach.

[Required: LSC, MFSS] Within the IP environment, Destination Code Control functionality is applied at the LSC or MFSS to prevent or limit the number of calls (session requests) to reach a specific destination. Destination code controls are applied to reduce calls to a specific area or location that have been temporarily designated as "difficult to reach" due to several circumstances

Within the DISN, call completion "difficulties" may include strategic or tactical situations for which a commander may want to minimize traffic to a given destination or set of destinations, such as a theater of operations. Given this, Minimize, (currently a behavioral control to reduce

traffic to a particular destination or region) initiated by a commander's order could be enforced using code controls, and set up to allow only precedence traffic to be passed to the minimized destination.

[Required] Destination Code Controls shall be implemented based on specifying:

- An entire NPA
- A group of specific NNX codes within an NPA (e.g., an example of when this control becomes necessary is when a large military base having multiple NNX codes becomes isolated.)
- A single NNX
- An NNX-D (hundred group within an NNX. Reason. There are locations within CONUS that share an NNX)

[Required] The LSC and MFSS shall have the capability of setting the percentage of calls to be blocked to the designated destination(s).

[Required] FLASH and FLASH-OVERRIDE calls shall not be affected by NM controls.

5.3.2.17.3.4.2.8 SKIP, Cancel To, Cancel From

Within TDM, the protective controls Cancel From (CANF), Cancel To (CANT), and SKIP are those that block traffic from using a trunk group.

Within the IP environment, the analogous functionality is performed within the ASLAN to control traffic (RTS and non-RTS) flows onto and off the base. It presumes there are multiple paths off the base (redundancy) and an ASLAN controlled load balancing or other traffic management capability to maintain appropriate control of all traffic flows. If, for tactical or technical reasons, one or more paths off the base cannot or should not be used, this is controlled within the base's NM and affects all traffic. Since it is applicable to all traffic traversing the ASLAN edge, not just RTS flows, it is not a voice-specific control.

5.3.2.17.3.4.2.9 Total Office Manual Control Removal

The ability to remove all controls that were put in place is equally applicable to TDM and IP-based voice systems.

5.3.2.17.3.4.2.10 Directionalization

Directionalization is intended to control the relative volume of call initiation from on base to off base, or vice versa (i.e., control the sourcing direction). This requirement stems from the Chairman of the Joint Chiefs of Staff Instruction (CJCSI) 6215.01C, Appendix A.

[Required] Within IP, directionalization is controlled by designating all or part of the call budget as inbound (i.e., local destination) and/or outbound (i.e., local origination). The default is no designation (i.e., calls up to the total budget can be inbound or outbound in any combination). It does not change the total budget, only the sourcing direction of the budget; therefore, there is no impact to the router queue bandwidths.

5.3.2.17.3.4.2.11 Reroute (with All Subcontrols)

Within TDM, Reroute restricts offered calls from those routes known to be congested or failed, and provides substitute routes that have a higher probability of call completion.

Within IP, the routing or all traffic (i.e., RTS and non-RTS) is handled via MPLS in the DISN core. The MPLS automatically finds the most effective route for the traffic.

5.3.2.17.3.4.2.12 IP Queue Control Capabilities

An important control unique to the IP-based environment is queue bandwidth allocations. The following requirements are for queue management:

1. Setting the queue bandwidth allocations on the CE Router and its connected port on the Aggregation Router involves setting the amount (or percentage) of bandwidth allocated to each of the (currently) four queues on the CE Router and connected PE Router. Two bandwidth allocation actions/functions can be performed as follows:

    a. **[Required: CE Router, Aggregation Router]** Setting the bandwidth allocations by router queue, and

    b. **[Required: CE Router, Aggregation Router]** Setting the drop probabilities within each Assured Forwarding queue.

5.3.2.17.3.4.2.13 LSC Call Budget Control

Setting the Call Budgets on the LSC involves setting the maximum number of calls (voice and video) that may be in service at one time to/from off the base.

[Required: LSC] Two call budget actions or functions can be performed: Setting the total call budget, and designating all or part of the call budget as inbound (local destination) and/or outbound (i.e., local origination) (to be able to implement an IP equivalent of directionalization). The default for the directionalization is no designation (i.e., calls can be inbound or outbound in any combination).

5.3.2.17.3.4.2.14 EI Origination Capability Control

Setting the EI Origination capability involves setting the parameters for the precedence and destinations of a call that may be originated from an EI.

[Required: LSC] The system shall have the capability of setting an EI's maximum allowed precedence level for originating a call. This is a "subscriber class mark feature," which is controlled by the LSC system administrator.

[Required LSC] The system shall have the capability of controlling the destination(s) an EI is allowed to or restricted from calling. This is a subscriber class mark feature that is controlled by the LSC system administrator. Two actions/functions can be performed by setting:

1. **[Required]** Setting the destinations to which calls are to be blocked by:

    a. **[Required]** NPA/NNX
    b. **[Conditional]** Blocked by a specific seven-digit directory number (NPA-NNX Dxxx)

Table 5.3.2-55, Control Function Crosswalk: TDM to IP RTS summarizes the traffic flow controls that will implemented in the IP environment along with the equivalent TDM-based controls.

5.3.2.17.3.5 Security Management

Security management provides for prevention and detection of improper use or disruption of network resources and services, for the containment of and recovery from theft of services or other breaches of security, and for security administration.

The E2E RTS EMS is required to use the security services of access control, confidentiality, integrity, availability, and non-repudiation as specified in UCR 2008, Section 5.4, Information Assurance Requirements.

[Required] All management interactions shall meet the IA requirements in UCR 2008, Section 5.4, Information Assurance Requirements.

Table 5.3.2-55. Control Function Crosswalk: TDM to IP RTS

	IP REAL TIME SERVICES CONTROL FUNCTIONS			
	ROUTER FUNCTION	**LSC FUNCTIONS**		
Existing TDM Control	CE BW Allocation	ASAC Budget	EI Origination	EI Destination
ACC	**X (bearer stream only)**	**X (bearer stream only)**		**X (from other LSCs/EIs – like Code Controls)**
SILC	**X (bearer stream only)**	**X (bearer stream only)**		
Trunk Reservation	**X**	**X**		
Precedence Access Threshold	**N/A to IP RTS**			
ESP	**N/A to IP RTS**			
Code Controls				**X**
CANT	**Applicable to all ASLAN edge traffic – Handled via base router management**			
CANF	**Applicable to all ASLAN edge traffic – Handled via base router management**			
SKIP	**Applicable to all ASLAN edge traffic – Handled via base router management**			
Total Office Manual Control Removal	**X**	**X**	**X**	**X**
Directionalization		**X**		
Reroute	**N/A to IP RTS – Handled via MPLS Functionality in DISN Core**			
Single via Reroute	**N/A to IP RTS – Handled via MPLS Functionality in DISN Core**			
Multiple via Reroute	**N/A to IP RTS – Handled via MPLS Functionality in DISN Core**			
Overflow vs. Immediate Reroute	**N/A to IP RTS – Handled via MPLS Functionality in DISN Core**			

5.3.2.17.4 Data Classification

This section defines the data types provided by network appliances. The data types can be classified as generated data and parametric data. In addition, data that indicates the condition or state of an appliance is defined as representing operational, usage, and administrative states. In addition to these states, a network appliance utilizes more descriptive status values. Although the data types defined within each category may overlap, they reflect the type of information conveyed by the data, and the urgency with which the data must be presented to the user. These lists are not exhaustive, but cover the most frequently used measurement types and capabilities.

5.3.2.17.4.1 Parametric Data

Parametric data refers to the data that resides in a network appliance and defines its functional mode and its physical resources. Parametric data is composed of criteria data and reference data. Reference data describes the topology, capacity, routing patterns, and other attributes of the components (i.e., switching network appliances, traffic links) that make up a network.

Reference data values do not change as frequently as counts and state indicators and thus, are relatively static. When reference data values changes, the network appliance should notify the appropriate management application. It is desirable for the changed reference data to be sent to the appropriate application when the change occurs. It is acceptable, however, for a state indication to be sent instead alerting the application to the change; this will then cause the application to initiate a request for the changed reference data. In either case, only the reference data that has actually changed should be sent.

Criteria data (also called instruction data) consists of the parameter settings available within the network appliance that govern the various application support functions of the network appliance. This includes, but is not limited to, such parameters as data filters, thresholds, collection schedules, and report generation criteria. The specific parameters may vary across the applications supporting a network appliance. These parameters may be set or modified by the individual supporting applications. Therefore, the network appliance should allow the management system to view and alter these parameters as necessary.

5.3.2.17.4.2 Generated Data

Generated data refers to the data recorded or collected by the NE concerning the traffic it is carrying. This includes traffic counts, data about the use of the NE resources, and noted exceptions. The three data types defined as generated data are event counts, usage counts, and state indications. Counts are cumulative measurements driven by event occurrences. Two types of counts are those based on distinct event occurrences and those based on usage.

5.3.2.17.4.3 Entity States

Access to state information in network appliances provides the current operational, usage, or administrative state of a resource, together with supporting status information.

The following state definitions are from ITU-T Recommendation X.731.

5.3.2.17.4.3.1 Operational State

Two valid Operational states are enabled and disabled.

1. Enabled. The resource is partially or fully operable and ready for use

2. Disabled. The resource is totally inoperable and unable to provide service to users

Generally, Operational states may only be set by the network appliance that houses the resource, and are used to indicate that the resource is experiencing trouble that is impairing functionality.

5.3.2.17.4.3.2 Usage State

Three valid Usage states are idle, active, and busy.

1. Idle. The resource is not currently in use

2. Active. A sharable resource has one or more users and has the ability to serve new users

3. Busy. A non-sharable resource has a user or a sharable user is occupied to capacity with request for use

Generally, Usage states are only able to be set by the network appliance housing the resource whose state is being monitored.

5.3.2.17.4.3.3 Administrative State

Three valid Administrative states are unlocked, shutting down, and locked.

1. Unlocked. The resource is permitted to perform services for users.

2. Shutting down. Use of the resource is allowed to existing users only, and no new users are allowed. After a time period, use of resource to existing users may be terminated.

3. Locked. Resource is administratively prohibited from performing services for its users.

In general, the Administrative state may be set by the E2E RTS EMS, Craft Interface, or the network appliance whose resources are being monitored. Administrative states are used to shut down and restart network appliances or bootable components of the network appliance.

5.3.2.17.4.3.4 Status

In addition to the generic states mentioned earlier, the network appliance utilizes more descriptive status values. An example is Service status.

Applicable values for Service status are as follows:

1. Test. The resource is no longer available for user traffic, as tests are scheduled for this resource.

2. In-service. Use of the resource is allowed.

3. Out-of-service. Resource has been made unavailable for use.

The Service status may be set by the E2E RTS EMS, or Craft Interface, and is used to indicate that tests are being conducted on resource, or the resource is otherwise out of service.

5.3.2.17.5 Management of Appliance Software

Software management must be able to satisfy the following objectives, subject to possible imposed controls and conditions:

1. Request delivery of software to a specific managed system.

2. Control the installation of software on a managed system, including the installation of patches (e.g., upgrades) and control the roll back to a previous version of the software.

3. Initiate the execution of a software program.

4. Request the attributes of the software held on a managed system.

5. Create and delete software held on a managed system.

6. Validate software held on a managed system in order to check its integrity and to terminate validation.

7. Restrict use of software on a managed system for administrative purposes.

8. Back up software and restore software to a previously backed up version.

In all cases, the success or failure of the operation needs to be reported to the managing system.

Software management may use logging, accounting, auditing, and license management at each state of this process.

5.3.2.17.5.1 Management of Software Generics

In this document, a software generic is defined as a non-site-specific software release for a network appliance that encompasses executable instructions, utilities, routines, and application programs. It does not include specific data, such as site-specific equipment configuration and operational parameters.

The management information associated with software generics contains user-settable attributes as well as a pointer to the software generic itself. The management information attributes are entered and edited by users with appropriate user privilege.

The required software management information includes the identities of all the network appliances that used the software modules, the software generic supplier name, the version number or release number of the software, the date and time when the software was received from the supplier, when the last update was made to the software generic, a program executability attribute that represents the state of the software generic, and a program accessibility attribute that governs the security access to the software generic.

[Required] A network appliance shall maintain management information associated with the software generics it is holding including the following elements:

- Software generic ID (e.g., supplier name, software type, version number, date of last update)
- Program size
- Location
- Program executability
- Program accessibility (e.g., privilege codes)
- Date and time loaded.

The Location attribute can be thought of as the pointer (e.g., file system path) to the software generic.

The program Accessibility attributes specifies the management systems, personnel, and other programs that may invoke the execution of the software generic.

The software generic ID uniquely identifies a software generic within the network appliance. The version of a software generic (e.g., new software generic, software update, software patch) labels the software generic release and its subsequent software updates and software patch releases so they can be unambiguously identified and related. The labeling scheme for software and for documentation should be the same for each type of software generic.

The program Executability attribute is used to indicate that a program is available for invocation and execution; in a testing state; unavailable for invocation or execution; and does not exist currently in a network appliance file store.

5.3.2.17.5.2 Software Installation

When software is initially installed, it may be necessary to have technicians present on site to monitor and control the installation. Therefore, a network appliance is required to support on-site installation of software generics. When this method is used, the network appliance shall inform the management operating system that the installation has taken place. Typically, only the first software generic is installed on site. Future releases are downloaded from a remote location under the direction of a management system.

[Required] A network appliance shall provide functionality to support the on-site installation of software generics, using portable storage media, with control of the installation process accessible over a local CID.

[Required] A network appliance shall be capable of accepting remote downloads of software generics.

[Required] The network appliance verifies any new software generic to ensure that the new software generic was loaded error free.

[Required] In response to a request, a network appliance shall report the management information associated with all loaded software generics.

[Required] A network appliance shall autonomously inform a managing system of the status of its software download activities.

[Objective] The network appliance should activate a new software generic load upon receiving a request to do so from a managing system.

[Objective] The software generic should be automatically activated on the network appliance once the correctness of it has been verified. This activation may occur immediately or at a predefined time.

[Objective] If a new software generic fails to activate, a network appliance shall back out of the software generic, re-establish its previous software generic, and indicate the reason for the back-out.

[Required] The process of loading software generics, including updates and patches, in a network appliance shall cause no disruption to the Appliance's functionality, or alter any existing option settings or configuration data.

5.3.2.17.5.2.1 Data Backup and Recovery

[Required] Programs, including application software and protocol software, and the corresponding software generic management information shall be subject to the backup and recovery requirements.

5.3.2.17.5.2.2 Service Impacts

An established (stable) call is a call that is in the connected state (i.e., voice, video or data is being transmitted), and no transient call activity is being initiated. A transient call is a call that is in a state of potential change.

[Required] During a software cutover, the network appliance shall preserve all stable calls.

[Objective] It is desirable that the software cutover process limit the duration of effects on transient calls for any size switching network appliance to less than one minute.

5.3.2.17.5.2.3 Databases/Directories

A network appliance may contain a Database Manager for its Management Information Base (MIB).

Occasionally, the data associated with newly loaded software generic will be sufficiently different from that of the older software generic that the Database Manager will have to restructure the MIB. General database reconfiguration generic requirements are discussed in Telcordia Technologies GR-2932-CORE.

[Required] In the case where a newly loaded software generic requires restructuring of MIB data, a mechanized method shall be provided for reconfiguring the MIB from the older software generic configuration database to a structure that is compatible with the new software generic.

5.3.2.18 Network Management Requirements of Appliance Functions

[Required: LSC, MFSS] The NM requirements for the various functions of the LSC and the softswitch part of the MFSS are contained in this section. Requirements are defined for the following functions:

- CCA function
- SG function
- MG function

5.3.2.18.1 Management Requirements of the CCA Function

A complete description of the CCA function is provided in UCR 2008, Section 5.3.2.9, Call Connection Agent.

5.3.2.18.1.1 CCA Support for Configuration Management

This section addresses CM under the following three topics:

- Capacity installation
- Service activation
- Status and control

5.3.2.18.1.1.1 CCA Support for Capacity Installation

Capacity installation supports the placement of equipment in the network. This includes the extension or reduction of resources, loading software, and coordination of changes.

The CCA needs to be able to access configuration data that it maintains about itself and other network appliances.

[Required] A Switching network appliance shall acquire, activate, and manage a CCA software download as directed by the E2E RTS EMS. The CCA software may be managed on a per CCA hardware component basis.

NOTE: The CCA software is managed as a software generic described in UCR 2008, Section 5.3.2.9, Call Connection Agent.

The CCA is provisioned with a CCA Identification parameter that uniquely identifies the CCA to the Billing Agent. See UCR 2008, Section 5.3.2.19, Accounting Management, for the

accounting requirements. The CCA is provisioned with a Recording Office Identification parameter that uniquely identifies the Billing Agent to the CCA.

[Required] The CCA shall be able to manage the following parameters in the CCA from the E2E RTS EMS:

- CCA Identification parameter
- Recording Office Identification parameter

5.3.2.18.1.1.1.1 MG-Related Configuration

This section specifies the data needed by the CCA to support access lines. This data is organized into the data the CCA needs to communicate with the MG, voice grade analog line-specific data, ISDN-related data, trunk-related data, and trunk circuit-related information.

[Required] The CCA shall manage the IP address of an MG from the E2E RTS EMS upon installation or removal of an MG or associated trunk equipment.

[Required] The CCA shall manage configuration data supporting voice grade analog lines upon installation of CCA or MG access equipment.

[Required] The CCA shall support provisioning of MG ISDN interface resources.

[Required] The CCA shall be capable of managing trunk-related provisioning information for associated MGs.

[Required] The CCA shall be capable of managing provisioning information related to trunk circuits associated with its assigned MGs.

5.3.2.18.1.1.1.2 SG-Related Data

[Required] The CCA shall accept manage configuration information about the set of SGs associated with the CCA.

5.3.2.18.1.2 CCA Support for Service Activation

Service activation focuses on the interactions with and functional requirements of the CCA in order to activate, modify, and discontinue services based on customer or traffic demands.

[Required] The CCA shall manage the activation and deactivation of service features.

[Required] The CCA shall maintain data for the media server and UFS functions it interacts with.

[Objective] It is desirable that activation of a new service feature not cause the CCA to disrupt customer services or operations support.

The CCA needs to be able to restore its configuration database to the last validated stable condition in the case of the corruption of configuration data.

[Required] The CCA shall be able to create a backup and manage restoration of configuration data by placing its stable data and changes to the latest configuration in a nonvolatile storage device.

5.3.2.18.1.3 CCA Support for Fault Localization

It is the responsibility of fault localization to determine the root cause of a fault. Fault localization may need to acquire data or perform tests to determine the root cause.

Generic maintenance requirements for trouble isolation in switching systems are found in Telcordia Technologies GR-474-CORE. These requirements shall apply to a CCA.

[Required] A CCA shall meet all applicable Operations Technology Generic Requirements (OTGR) for switching system NE trouble isolation in Telcordia Technologies GR-474-CORE.

[Required] A CCA shall perform root cause analysis for any faults within its purview, report the root cause, and suppress the reporting of non-root cause conditions.

The preceding requirement implies that if a single fault or abnormality results in the impairment of multiple generic functions, the CCA shall generate a single alarm message that reports the fault or abnormality and that identifies all such impaired functions.

5.3.2.18.1.4 CCA Support for Testing

Testing is concerned with the testing of connections directly related to customer services or with transmission facilities and the related resources within affected functional elements. Testing is performed for the purpose of acceptance of newly provisioned connections, new installation of physical facilities or network appliances, validating trouble reports, providing additional information to fault localization, or to verify a network repair.

[Required] A CCA shall support the ability to perform internal diagnostics on its call processing functionality and internal resources, initiated either locally or upon request by the E2E RTS EMS.

5.3.2.18.1.5 CCA Support for Performance Management

Performance management criteria are used to evaluate and report on the behavior and effectiveness of the CCA as well as the physical and logical entities it supports. Performance management includes gathering and analyzing statistical data for both performance monitoring (for network maintenance) and Network Traffic Management purposes.

Performance monitoring provides non-intrusive collection, analysis, and reporting of network performance information and traffic statistics. This data is used to assess and maintain the network as well as to document the quality of service to customers. Indications of service affecting degradation are forwarded to Fault Management applications.

5.3.2.18.1.5.1 The MG-MGC Protocol and Traffic Monitoring

Protocol and traffic monitoring requirements shall apply to the Gateway Control interface. This interface refers to the control interface between the CCA's internal MGC function and an MG. NOTE: The MG-MGC protocol may be H.248 or may be a priority protocol. The specific protocol to be used is a supplier/vendor decision.

The terminology used in this section for describing the communication between a CCA and an MG is briefly reviewed in the next paragraph.

A Command provides the ability to manipulate the logical entities of the protocol connection model. Examples are an Add Command that adds a Termination to a Context or a Subtract Command that removes a Termination from a Context. Commands between the CCA and an MG are grouped into Transactions. Transactions consist of one or more Actions. An Action consists of a series of Commands that are limited to operating within a single Context. In addition, multiple Transactions can be concatenated into a Message.

Traffic counts will only be performed on Commands and Transactions.

[Required] The CCA shall provide counters for the following on each MG interface supporting the MG-MGC protocol:

- Number of requests sent
- Number of responses received
- Number of retransmits

- Number of received error conditions
- Number of service changed commands
- Count of termination ID related errors
- Count of context related errors
- Count of descriptor related errors
- Count of action related errors
- Count of package related errors
- Count of transaction related errors
- Count of command related errors
- Count of digit map related errors
- Count of gateway related errors

[Required] The CCA shall count each of the following specific command error codes on interfaces supporting the MG-MGC protocol (Thresholds on these counts shall be set on a per-interface basis.):

- Bad Request
- Protocol Errors
- Unauthorized
- Insufficient Resources
- Not Implemented
- Not Ready
- Service Unavailable
- Insufficient Bandwidth
- Internal Hardware Failure

[Required] The CCA shall log information on a service change command each time it generates this Command. The log for a service change shall contain the following information:

- Service change reason.

- Service change method.

- Date and time of service change. The time shall be accurate to within 1 second, with respect to the CCA's local clock.

5.3.2.18.1.5.2 Call-Related Performance Monitoring

The CCA needs to monitor internal call-related procedures, as well as performance associated with call processing.

[Required] The CCA shall provide a counter for each of the following to support monitoring of call processing:

1. No responses. The CCA fails to receive a response to a request or message that requires a response.

2. Incorrect messages. The CCA receives a message that cannot be understood or does not permit a valid response to be formed and sent to a specific MG.

3. Invalid messages. The CCA receives a transaction request or message that is invalid or cannot be successfully acted upon, but for which a valid response can be directed to the transmitting MG.

4. Sending error messages. The CCA receives a number of responses with error codes indicating a malformed request or message that suggests a problem in the CCA or in the sending entity.

[Required] The CCA shall provide basic switch-related traffic measurements as specified in Telcordia Technologies GR-477-CORE, Section 4.1.1. In particular, the CCA shall support the following GR-477-CORE requirement:

- Telcordia Technologies GR-477-CORE related to CCA processor performance:
  - Call processing capacity

- Telcordia Technologies GR-477-CORE call direction measurements:
  - Total originating calls
  - Originating line to terminating line calls
  - Originating line to outgoing trunk calls
  - Total incoming calls
  - Incoming trunk to terminating line calls
  - Incoming trunk to outgoing trunk calls

- Telcordia Technologies GR-477-CORE Basic failure to match and no circuit measurements:

  - Originating to terminating matching loss
  - Originating to outgoing matching loss
  - Incoming to terminating matching loss
  - Incoming to outgoing matching loss
  - Originating to outgoing calls encountering No Circuit (NC)

  - Incoming to outgoing calls encountering NC
  - Originating to terminating calls to line busy
  - Incoming to termination call to line busy

- Telcordia Technologies GR-477-CORE Additional ineffective machine attempt measurements:

  - Final handling overflows
  - Incoming trunk permanent signaling time-outs
  - Outgoing trunk start signaling time-out
  - Miscellaneous equipment-related ineffective machine attempts
  - Vacant code treatments

[Required] The CCA shall provide trunk group-related traffic measurements as specified in Telcordia Technologies GR-477-CORE, Section 4.1.3. In particular, the CCA shall support absolute requirement of GR-477-CORE, providing basic trunk group measurements including the following:

- Access attempts for trunk group
- Overflow for trunk group
- Total usage for trunk group
- Incoming attempts for trunk group

[Required] For all calls originating at a CCA, the CCA shall monitor call set-up delay statistics, including delay incurred as part of the set-up of the core network bearer connection.

5.3.2.18.2 Management Requirements of the SG Function

The requirements identified in this section are **[Conditional: MFSS, LSC],** since an SG is also conditional.

The SG interacts with the Management function by:

1. Making changes to its configuration in response to commands from the Management function that request these changes.

2. Returning information to the Management function on its FCAPS, in response to commands from the Management function that request this information.

3. Sending information to the Management function on a periodic basis (e.g., on a set schedule), and keeping the Management function up-to-date on SG activity. An example

of this update would be a periodic transfer of audit reports from the SG to the Management function, so that the Management function could either store the report locally or transfer it to a remote NMS for remote storage and processing.

A complete description of the SG is provided in UCR 2008, Section 5.3.2.13, Signaling Gateway Requirements.

5.3.2.18.2.1 SG Support for Configuration Management

This section addresses CM under the following three topics:

- Identifiers
- Protocol Management – CCS7 Layers
- Status Monitoring

5.3.2.18.2.1.1 Identifiers

[Conditional] The SG shall allow the E2E RTS EMS to configure the set of adjacent and remote CCS7 destinations in the CCS network. For each CCS7 destination, the SG shall allow the E2E RTS EMS to configure the CCS7 destination address.

[Conditional] The SG shall allow the E2E RTS EMS to configure its unique CCS7 primary Signaling Point Code (SPC), in terms of the decimal equivalents of its Network Identifier (NI), Network Cluster, (NC), and Network Cluster Member (NCM) codes.

5.3.2.18.2.1.2 Protocol Management – CCS7 Layers

The SG is required to support the provisioning via the E2E RTS EMS of various resources associated with the SG's CCS7 network interfaces. Requirements are presented for the various types of CCS7 resources or functional parameter profiles.

5.3.2.18.2.1.2.1 CCS7 Link Interface Equipment Ports

[Conditional] The SG shall maintain the following management information for each configured CCS7 link interface equipment port:

- Link equipment port identifier
- Port equipment options/settings

5.3.2.18.2.1.2.2 CCS7 Link Sets

[Conditional] The SG shall allow the E2E RTS EMS to configure its CCS7 link set terminations, including the specification of the following link set attributes:

- Network link set identifier
- Far-end point code
- Far-end node identifier
- Local link set identifier (optional)

5.3.2.18.2.1.2.3 CCS7 Signaling Routes

The configured link sets are to be regarded as the "signaling routes" to the CCS7 configured destinations. As two A-link link sets are assumed for the initial SG implementations, there are no requirements for the explicit provisioning of ordered (primary and alternate or loadshared) signaling routes to each CCS7 destination address. Equal loadsharing via the SLS code mechanism is implied for outbound signaling traffic distributed over the links in the configured A-link sets.

5.3.2.18.2.1.2.4 CCS7 Links

[Conditional] The SG shall allow the E2E RTS EMS to configure its CCS7 link terminations, including the creation of member links within link sets and their assignment to CCS7 link equipment ports, along with the specification of the following link attributes:

- Network link set identifier
- Link member number/signaling link code (SLC)
- Link equipment port identifier
- Associated CCS7 MTP-Level 2 timer profile (optional)
- Associated CCS7 MTP link transmit congestion thresholds profile

Up to 16 links per link set are allowed by the size of the SLC and SLS codes used for A-link sets.

5.3.2.18.2.1.2.5 CCS7 MTP Level 2 Timer Profiles

[Conditional] The SG shall provide default values and allow the E2E RTS EMS to configure one or more Level-2 parameter profiles described in T1.111.3 (i.e., T1, T2, T3, T4n, T4e, T5, T6, T7), each assignable to individual MTP2-based signaling links.

5.3.2.18.2.1.2.6 CCS7 MTP Link Transmit Congestion Threshold Profiles

[Conditional] The SG shall provide default values and allow the E2E RTS EMS to configure one or more congestion-threshold parameter profiles (i.e., Level 1, Level 2 and Level 3), each assignable to individual MTP2-based signaling links.

The default values and configurable ranges for the CCS7 link transmit congestion thresholds should be selected by the SG supplier to maximize link throughput and minimize expected link output delays, subject to capacity and design constraints of the implementation's signaling message handling process and the capacity of its transmit and retransmit buffers. The latter constraints are implementation-specific considerations.

5.3.2.18.2.1.2.7 CCS7 MTP3 Timer Profile

[Conditional] The SG shall provide default values and allow the IP network to configure a profile of MTP3 timer values to be used by the SG in its interactions across all CCS7 signaling links. The profile shall contain values of the parameters described in T1.111.4 (i.e., timers T1, T2, T3, T4, T5, T6, T10, T12, T13, T14, T15, T16, T17, T19, T20, T21, T22, T23, T26, T26, T27, T28, T29, T31) and T1.111.7 (i.e., timers T1, T2), changeable on a per-node (per-SG) basis.

[Conditional] The SG shall support configurable ranges for the CCS7 MTP3 timers as specified in Telcordia Technologies GR-246-CORE, Tables 4-2, *Provisional Values for Signaling Link Test Timers*, and 4-3, *Provisional Values for MTP Level 3 Timers*.

5.3.2.18.2.1.2.8 CCS7 Provisioning Operations

[Conditional] The SG shall support provisioning of the following CCS7 resources by the E2E RTS EMS:

- Assign or change the self-identity SPC.
- Add CCS7 destinations.
- Change existing CCS7 destination attributes.
- Retrieve CCS7 destination attributes.
- Delete/remove CCS7 destinations.
- Retrieve link port attributes.
- Modify link port equipment settings.
- Create/add link sets.
- Modify link set attributes.
- Retrieve link set attributes.
- Remove/delete link sets with no member links.
- Assign/add member links to existing link sets.

- Modify link attributes.
- Retrieve link attributes.
- Delete/remove inactive signaling links.
- Create CCS7 MTP Level 2 timer profiles.
- Modify CCS7 MTP Level 2 timer profiles.
- Retrieve CCS7 MTP Level 2 timer profiles.
- Delete CCS7 MTP Level 2 timer profiles.
- Create CCS7 MTP link transmit congestion threshold profiles.
- Modify link transmit congestion threshold profiles.
- Retrieve link transmit congestion threshold profiles.
- Delete link transmit congestion threshold profiles.
- Create CCS7 MTP3 timer profile.
- Modify CCS7 MTP3 timer profile.
- Retrieve CCS7 MTP3 timer profiles.
- Delete CCS7 MTP3 timer profile.
- Set or change MTP3 control indicators.
- Retrieve MTP3 control indicators.

[Conditional] It shall be possible for the E2E RTS EMS or local management to initially configure each CCS7 signaling link at the SG as follows:

1. Requesting an "inactive" state, so the link terminal may be activated at a later time when provisioning activity may be coordinated with the far-end NE (STP) and with interoffice facility systems.

2. Requesting an "active state," under which the SG shall attempt to immediately activate, align, and prove in the signaling link, subject to prevailing network conditions.

5.3.2.18.2.1.3 Status Monitoring

The SG is expected to support Status Management functions via its interface with the E2E RTS EMS. A CID may be supported for direct control of the interface of the SG. References to the configuration interface in this document shall be meant to correspond to either interface.

5.3.2.18.2.1.3.1 General State Variables

[Conditional] The SG shall be capable of monitoring the following states for each of its configured resources:

- Operational state
- Usage state

- Administrative state
- Service status
- Procedural status

The preceding requirement does not imply that all these states and their values need to be applied to each configured resource or component at the SG. In fact, the definitions of these states are likely to apply to only certain types of resources or traffic-carrying components. When applied to specific SG resources, they will be subject to interpretation. Nor are these states exhaustive in terms of all the relevant state information that needs to be monitored for the SG's resources.

5.3.2.18.2.1.3.2 SG CCS7 Signaling Point States

[Conditional] An SG shall maintain its own (local) CCS7 MTP3 signaling point status, X.731 administrative state, and X.731 operational state.

5.3.2.18.2.1.3.3 CCS7 Link Equipment Port States

[Conditional] For each CCS7 link port detected by the SG's Management function, the SG shall maintain the following states:

- Equipage state: Unequipped or Equipped
- Provisioning state: Assigned or Spare

5.3.2.18.2.1.3.4 CCS7 Link States

[Conditional] For each configured CCS7 signaling link, the SG shall maintain the status variables with indicated state values as recognized by the MTP3 of the CCS7 protocol, per Telcordia Technologies GR-246-CORE, Section T1.111.4, Section 3.2, *Status of Signaling Links*.

[Conditional] For each configured CCS7 signaling link, the SG shall maintain the following status information:

- Link Activity Status: Inactive or Active

- Management-Inhibit Status: Locally, Remotely, Both, or Not

- Transmit Congestion Status: Level 1 onset, Level 1 discard, Level 2 onset, Level 3 discard, Level 3 onset, Level 3 discard, or Not

- Service Status: In-Service or Out-of-Service

- Local Processor Outage Status: Spontaneous outage, Interworking-induced outage, Management-induced outage, or None
- Remote Processor Outage Status: Remotely blocked or Not remotely blocked
- Receiving Congestion Status: Congested or Not-congested
- Link Terminal Status: Active or Inactive

5.3.2.18.2.1.3.5 CCS7 Link Set States

[Conditional] For each configured CCS7 signaling link set, the SG shall maintain a Link Set Availability indicator: Available or Unavailable

5.3.2.18.2.1.3.6 CCS7 Destination/Route-Set States

[Conditional] For each configured CCS7 destination, the SG shall maintain the status of that destination's signaling route-set. This status variable shall convey one of the following values: Unavailable, Available, Congested-Level-1, Congested-Level-2, or Congested-Level-3.

5.3.2.18.2.1.3.7 CCS7 Signaling Route States

[Conditional] For each configured CCS7 signaling route (destination/link set combination), the SG shall maintain the status of that route. This status variable shall convey one of the following status values: Allowed, Prohibited, or Restricted.

5.3.2.18.2.1.3.8 Status Retrieval–- General

[Conditional] The SG shall support query capabilities from the E2E RTS EMS to retrieve current SG status information regarding installed major components and process at the SG.

5.3.2.18.2.1.3.9 Autonomous Notification of State Changes

The SG needs to be able to provide the E2E RTS EMS notification of changes of state as the result of recognition that a state has changed such as a change from "enabled" to "disabled" in the event of a failure.

[Conditional] The SG shall be capable of providing to the E2E RTS EMS notification of changes to the Operational and Administrative states of major components and other monitored resources associated with the SG.

5.3.2.18.2.1.3.10 Status Management Actions – General

[Conditional] The SG shall be capable of placing components in or out of service in a graceful manner when instructed to do so by the E2E RTS EMS.

5.3.2.18.2.1.3.11 Status Management Actions for CCS7 Interfaces

[Conditional] The SG shall support the following state management interactions for the specified CCS7 resources as initiated by the E2E RTS EMS:

1. Request local management inhibiting of a signaling link not yet locally inhibited.

2. Request local management un-inhibiting of a locally inhibited signaling link.

3. Request activation of an inactive signaling link.

4. Deactivate (render inactive and remove from service) a signaling link already unavailable to MTP user part message traffic for other reasons.

5. Unconditionally force a manually induced local processor outage condition in a signaling link.

6. Clear a manually induced local processor outage condition for a manually blocked link set or member link, allowing link restoration (subject to prevailing network conditions).

7. Unconditionally deactivate a signaling link and remove it from service regardless of its current MTP3 availability status or the status of its supported route sets.

5.3.2.18.2.2 SG Support for Fault Management

Fault management for the SG includes the following:

- Alarm surveillance
- Fault localization
- Testing

The focus of these requirements will be on alarm and event surveillance, in terms of the reporting by the SG of detected alarm and event conditions. Fault localization and testing capabilities are addressed only on a best effort basis at this time.

5.3.2.18.2.2.1 SG Alarm Surveillance

Alarm surveillance provides the capability to monitor failures detected in network appliances in near real time. This information, along with other information allows Voice network management personnel to determine the nature and severity of the fault. The term "alarm" actually refers to all types of events that are associated with specific events. Although most alarms are associated with specific events, some alarms are based on a cumulative count of specified events exceeding a preset threshold during a designated time period.

[Conditional] The SG shall conform to all applicable objectives for trouble detection, verification, and notification in a switching network appliance, as specified in Telcordia Technologies GR-474-CORE, Section 4, *Network Maintenance: Alarm and Control for Network Elements*. Specifically, the applicable GR-474-CORE requirements are R3-1 through R3-3, R3-6, R3-8, R3-10, and R3-11.

[Conditional] Upon detection of or clearing of an alarm condition, the SG shall generate an alarm event notification. Each alarm notification generated by the SG shall contain the following information:

1. SG Identity. The unique identifier of the SG generating the event notification.

2. Event Type Identifier. A unique identifier or code conveying the specific type of event reported (e.g., the failure of a specific type of component or resource).

3. Sequence Number. A unique sequence number for the reported alarm/ event notification, so that the notification may be properly sequenced by the E2E RTS EMS and so missing or discarded notifications may be detected.

4. Timestamp. The date, time, and time zone at which the event was detected by the SG based on its internal system clock.

5. Alarm Severity. Conveying the seriousness of the reported alarm/ event condition and the intended priority of management action to address the alarm. Applicable values include the following:

    a. Critical
    b. Major
    c. Minor
    d. Information only (non-alarmed)
    e. Recovery – Critical
    f. Recovery – Major

g. Recovery – Minor
h. Recovery – Non-Alarmed

6. Impacted Resource. A locally or globally unique identifier identifying the specific instance of the impacted NE component or resource, or external network resource, for which the fault or trouble condition was detected.

The alarm severity and impacted resource(s) will differ according to the specific alarm/event type. Requirements for additional output parameters may apply on an alarm/event-type specific basis, such as the detected or probable cause of a fault condition, results of diagnostic procedures run on the resource, and supporting information that may be used to support trouble verification, localization, and isolation.

[Conditional] The SG shall support queries for alarm status and state information.

[Conditional] The SG shall monitor, detect, and generate alarm conditions and states associated with hardware. The minimum faults monitored are as follows:

- Link interface line card out of service
- Control CPU out of service

5.3.2.18.2.2.2 Notification Retention

[Objective] It is desirable for the SG to log alarm/event notifications in a local database, in case the operations interface or the E2E RTS EMS is unavailable for a period of time.

5.3.2.18.2.2.3 Alarm Surveillance for CCS7 Interfaces

An SG is expected to generate an alarm or event notification concerning its CCS7 interfaces and associated resources.

[Conditional] The SG shall generate an alarm notification to the E2E RTS EMS immediately when one of the following situations occurs:

1. The SG becomes isolated from both member STPs of its serving STP pair (Critical).

2. The SG becomes isolated from an adjacent STP (Major).

3. A CCS7 destination (i.e., signaling point or network cluster), other than the adjacent STP's unique DPC, becomes unavailable (Major).

4. A route set to a CCS7 destination (i.e., signaling point or network cluster), other than the adjacent STP's unique DPC, becomes unavailable (Major).

5. A CCS7 route set to a remote (non-adjacent) CCS7 point code destination becomes congested or increases its congestion level (Minor).

6. All links comprising a CCS7 link set have become unavailable to MTP user-part message traffic (Major).

7. A previously available CCS7 signaling link has become unavailable to CCS7 user part message traffic, as perceived by MTP3 (Minor).

8. A CCS7 link previously regarded as in-service at MTP2 has failed (Minor).

9. A failed CCS7 link, or a previously inactive CCS7 link for which activation has been initiated by MTP3, has failed its first alignment attempt following the link failure or attempted activation, or that alignment is not possible due to prevailing network conditions (Minor).

10. A failed CCS7 link, or a previously inactive CCS7 link for which activation has been initiated by MTP3, has failed one or more alignment and proving attempts and has remained out of service for a duration exceeding the MTP3 Failed Link Craft Referral Timer (Minor).

11. A CCS7 signaling link has been remotely blocked due to MTP3 or higher level processor outage at the far end (Minor).

12. A CCS7 signaling link has been locally blocked due to a spontaneous or induced local processor outage (Minor).

13. A CCS7 signaling link is deactivated and removed from service by Operations management (Minor).

14. The SG's own local CCS7 MTP3 has become unavailable (Critical alarm).

15. A thresholded number (value to be set by network control personnel) of incoming CCS7 messages that fail MTP message discrimination.

16. A thresholded number (value to be set by network control personnel) of outgoing CCS7 messages that fail MTP routing procedures.

[Conditional] The SG shall generate an alarm recovery notification to the E2E RTS EMS immediately when it recovers from a reported alarm condition.

[Conditional] The SG shall allow the E2E RTS EMS to suppress reporting of the alarm and event notification.

5.3.2.18.2.2.4 SG Fault Localization

Fault localization determines the root cause of a failure. Where the initial failure information is insufficient for fault localization, it has to be augmented with information obtained by additional failure localization routines.

5.3.2.18.2.2.4.1 General

[Conditional] An SG shall on request or on a predefined schedule, run diagnostics on hardware checks on software, and report the result to the E2E RTS EMS.

5.3.2.18.2.2.4.2 For CCS7 Interfaces

The SG, as a CCS7 network node, should provide capabilities by which it can assist network maintenance personnel in distinguishing faults associated with local Signaling Link Terminal Equipment (SLTE), from faults that may be attributed to link transmission facilities or far-end SLTE.

[Conditional] If a failed signaling link or an inactive signaling link for which activation has been initiated fails to align and correct after a period of T19/GR-426-CORE T1.111.4 (provisional value 8 minutes), the SG shall temporarily suspend the restoration or activation attempt and automatically run diagnostics on the SLTE. After the diagnostics are completed, the SG shall generate an output message (i.e., event notification) to inform management of the sustained failure and convey the results of the diagnostics.

5.3.2.18.2.3 SG Support for Testing

Testing is concerned with the testing of transmission facilities and related resources within the SG. Testing may be carried out for the following purposes:

1. Testing connecting facilities in preparation for installation of new equipment.

2. Accepting newly installed facilities or service circuits.

3. Validating trouble reports.

4. Supporting fault localization.

5. Verification of repair.

5.3.2.18.2.3.1 General

[Conditional] The SG shall provide both local and remote loopback capabilities for the signals that terminate at the SG physical ports.

The SG shall support the ability to perform internal diagnostics on its internal resources.

[Conditional] The SG shall provide diagnostics that can examine the state of each significant element of hardware, and that can identify faults and isolate failures to within the smallest replaceable unit of hardware.

[Conditional] The SG shall permit the E2E RTS EMS to initiate diagnostics.

[Conditional] The SG shall provide test access to external test equipment for passively monitoring the traffic through the SG interfaces. This passive monitoring shall not degrade the performance of traffic.

5.3.2.18.2.3.2 For CCS7 Interfaces

[Conditional] The SG shall support the initiation, via the E2E RTS EMS and the CID, of CCS7 Signaling Data Link Test Procedures to be performed over its DS0 interfaces, including loopback test procedures, as specified in Telcordia Technologies GR-246-CORE, Chapter T1.111.7, Section 2.1, and the reporting of test results via those interfaces.

5.3.2.18.2.4 SG Support for Performance Management

This section addresses the performance management criteria used to evaluate and report on the behavior and effectiveness of the SG as well as the physical and logical entities it supports.

The main focus will be on traffic and performance monitoring. Traffic and performance monitoring provides a systematic assessment of a particular entity's ability to carry out its assigned function through the continuous collection and analysis of appropriate performance measurement data. Traffic and performance monitoring procedures are intended to quantify the traffic offered to and handled by a network appliance and its components, as well as capture intermittent error conditions and troubles resulting from the gradual deterioration of network equipment. Proactive maintenance techniques, such as traffic and performance monitoring, enable the network provider to detect troubles early before they escalate in severity.

5.3.2.18.2.4.1 General Monitoring Requirements (Common)

This section defines some common requirements for performance management including counters and monitoring intervals, and generation of threshold crossing alerts.

5.3.2.18.2.4.1.1 Counters and Monitoring Intervals

All counters need to be designed so they remain at their maximum value, so that they do not "roll over" to "000...000." It is stressed that the term "counter" does not imply an implementation. For example, if three counts are required as well as an associated sum of errors counter, this could be implemented as two registers for two simple counts and one register for the sum of errors. The third simple count could be inferred from the other two.

[Conditional] Upon receiving a request from the E2E RTS EMS, the SG shall provide a report of a parameter's present or past history counters.

Most traffic and performance measurement data collected by the SG for performance management purposes (e.g., for traffic engineering and planning and performance monitoring) shall be collected on a 15-minute accumulation interval. The following requirement applies to the storage and accuracy of those measurements.

[Conditional] For all counters, the SG shall store 8.25 hours worth of 15-minute data; the current 15-minute interval plus the past thirty-two 15-minute intervals.

5.3.2.18.2.4.2 SG Traffic and Performance Monitoring

This section provides requirements and objectives for the SG's collection, monitoring, and reporting of traffic and performance measurements, which includes the following:

1. Scheduled measurements are to be collected routinely by the SG and made available to the E2E RTS EMS on an ongoing basis, some of which shall be thresholded for the purposes of exception reporting and Threshold Crossing Alerts (TCAs).

2. Exception measurement reports are to be generated and reported only when key measurement counters are non-zero or exceed specified thresholds.

3. Threshold Crossing Alerts are generated as event notifications when thresholds are first crossed for key performance measurements.

   For each applicable resource type, measurements are specified in terms of the measurement definition, the accumulation basis (e.g., per component type), and the applicable

accumulation interval (e.g., 5, 15, 60 minutes, or 24 hours) based on the specific intended use in Performance Management functions. The following abbreviations are used within the stated measurement requirements (enclosed within square brackets) to denote the appropriate measurement accumulation intervals, and the typical uses for such measurements:

a. [5] = 5 minutes. Typically used for near-real time Network Traffic Management (NTM) surveillance,

b. [15] = 15 minutes. Typically used for traffic engineering/capacity monitoring and short-term performance monitoring.

c. [h] = hourly. Typically used for network maintenance surveillance.

d. [m] = hourly-marginal. Typically used for exception-oriented performance management, reported only when key marginal performance indicators are exceeded.

e. [d] = daily. Typically used for network maintenance surveillance, including longer term trending of traffic measurements and those performance measurements indicating faults and error conditions.

When no interval is specified, the 15-minute accumulation interval is implied by default.

5.3.2.18.2.4.2.1 SG System Totals

[Conditional] The SG shall support the collection and reporting of the following performance measurements on a total system basis for the indicated intervals:

- SG availability {15,d}
- CCS7 MTP3 user part messages discarded due to SG node internal failures {15,d}
- CCS7 MTP3 user part messages discarded due to SG node internal congestion or overload {15,d}
- Duration of SG node internal failure, defined as the total time that messages could not be switched to the appropriate interface for transmission, independent of interface failures {15,d}.

5.3.2.18.2.4.3 CCS7 Interface Measurements

The requirements in this section and objectives address measurements concerning the SG's CCS7 interfaces and associated resources.

5.3.2.18.2.4.3.1 CCS7 Link Measurements

[Conditional] The SG shall support the collection and reporting of the following traffic and performance measurements on a per-CCS7-link basis for the indicated intervals:

- MSUs received {15,d,m}
- MSUs transmitted (including retransmissions) {15,d,m}
- MSUs retransmitted {m}
- MSU octets received {15,d}
- MSU octets transmitted (including retransmitted MSUs) {15,d}
- MSU octets retransmitted {m}
- Signal Units (SUs) received in error {15,m,d}
- Number of hourly marginal performance thresholds exceeded for SUs received in error {d}
- Negative acknowledgements received from the far end {15,m,d}
- Number of hourly marginal performance thresholds exceeded for negative acknowledgements received {d}
- Duration of link unavailability to MTP3 user part message traffic (seconds) {5,15,m,d}
- Duration of link out-of-service at MTP2 (seconds) {15,m,d}
- Link Maintenance Usage: duration of link unavailability attributed to management action, including inhibiting (local or remote), management-induced local processor outage, or deactivation/removal from service (seconds) {15,m,d}

- Number of automatic link changeovers {15,m,d}
- Number of hourly marginal-performance thresholds exceeded for automatic changeovers {d}
- Event count for entry into level 1 transmit congestion (onset threshold crossings) {15}
- Event count for entry into level 2 transmit congestion (onset threshold crossings) {15}
- Event count for entry into level 3 transmit congestion (onset threshold crossings) {15}
- MSUs discarded due to local link transmit congestion (all priorities) {15}
- Priority 0 MSUs discarded due to local link transmit congestion {15}
- Priority 1 MSUs discarded due to local link transmit congestion {15}
- Priority 2 MSUs discarded due to local link transmit congestion {15}
- Priority 3 MSUs discarded due to link transmit buffer overflow {15}
- Link transmit buffer maximum observed occupancy {15}
- Link transmit buffer average occupancy {15}
- Duration of receipt of Status Indication “Busy” (SIB) Link Status Signaling Units (LSSUs) (remote receiving congestion) (seconds) {15}
- Duration of transmission of SIB LSSUs (local receiving congestion) (seconds) {15}
- Duration of receipt of SIPO LSSUs (remote processor outage) (seconds) {15}
- Duration of transmission of SIPO LSSUs (local processor outage) (seconds) {15}

5.3.2.18.2.4.3.2 Performance Reporting of TCAs

[Conditional] The SG shall allow the E2E RTS EMS to set performance thresholds, and if a performance threshold is defined for a specific measurement, the SG shall compare the counter values of the indicated measurement to the corresponding thresholds. Whenever the threshold is exceeded during an interval, the SG shall report to a TCA to the E2E RTS EMS.

5.3.2.18.2.4.3.3 CCS7 Link Set Measurements

[Conditional] The SG shall support the collection and reporting of the following traffic and performance measurements on a per-CCS7-link-set basis for the indicated intervals, aggregated across member links where necessary:

- MSUs received {15}
- MSUs transmitted (including retransmissions) {15}
- MSUs retransmitted {15}
- MSU octets received {15}
- MSU octets transmitted (including retransmitted MSUs) {15}
- MSU octets retransmitted {15}
- Duration of link set outage (all links unavailable to MTP3 user-part message traffic) {15}
- Duration of member link unavailability (summed across member links) {15}
- Number of assigned links in the link set {15}

5.3.2.18.2.4.3.4 CCS7 Destination/Route-Set Measurements

[Conditional] The SG shall support the collection and reporting of the following traffic measurements for the indicated intervals aggregated on a per configured-CCS7-destination/route-set basis (i.e., per configured DPC and cluster destination) (For network cluster destinations, counts shall be aggregated over cluster members.):

- MTP3 user part messages received (from matching OPC) {15}
- MTP3 user part messages transmitted (to matching DPC) {15}

- MTP3 MTP NM messages received (from matching OPC) {5,15}
- MTP3 MTP-NM messages transmitted (to matching DPC) {15}

5.3.2.18.2.4.3.5 MTP3 and Interworking Measurements

[Conditional] The SG shall support the collection and reporting of the following traffic and performance measurements concerning its CCS7 Network Interface functions and their interactions with the SG's Interworking function (These measurements are to be aggregated across all CCS7 interfaces for the indicated intervals.):

- Incoming CCS7 MTP3 messages received from the CCS7 network {15,d}
- Incoming invalid CCS7 MTP3 messages from the CCS7 network failing message discrimination due to invalid DPC (not matching the SG's primary SPC) or network indicator {15}
- Incoming valid CCS7 MTP3 messages submitted by MTP3 to the interworking function {15}
- Incoming valid CCS7 MTP Network Management (MTP-NM messages) {15}
- Incoming valid CCS7 Testing and Maintenance (T&M) messages {15}
- Outbound CCS7 MTP3 messages submitted to MTP3 by the interworking function {15}
- Outbound CCS7 MTP3 messages discarded due to routing translation failures (unknown DPC or unrecognized network indicator) {15}
- Outbound CCS7 MTP3 messages discarded due to inaccessible CCS7 destinations {15}
- Outbound CCS7 MTP3 messages discarded due to CCS7 route-set congestion (local or remote) {15}
- Duration of SG isolation from serving STP pair {15,d}
- Unavailability of the SG's local CCS7 MTP3 to user part message traffic (seconds) {15,d}

5.3.2.18.3 Management Requirements of the MG Function

The MG interacts with the Appliance Management function by:

1. Making changes to its configuration and to its trunks' configuration, in response to commands from the Management function that request these changes.

2. Returning information to the Management function on its FCAPS, in response to commands from the Management function that request this information.

3. Sending information to the Management function on a periodic basis (e.g., on a set schedule), and keeping the Management function up-to-date on MG activity. An example of this update would be a periodic transfer of trunk media error logs from the MG to the Management function, so the Management function could either store the records locally or transfer them to a remote NMS for remote storage and processing.

A complete description of the MG is provided in UCR 2008, Section 5.3.2.12, Media Gateway Requirements.

5.3.2.18.3.1 MG Support for Configuration Management

The requirements in this section apply to MGs in general.

[Required] An MG shall manage logical and physical resource inventory information.

[Required] An MG shall issue an autonomous notification to the E2E RTS EMS whenever a new inventory or capabilities are added or configuration is changed through local management activity.

[Required] An MG maintains the information related to service features and data, including the management of service logic.

5.3.2.18.3.1.1 Status and Control

An MG shall be capable of managing and reporting the operational state and administrative state information for associated components that will include, at least, all hosts and processes.

5.3.2.18.3.1.2 Core Network Interface Resources

[Required] An MG shall manage current MG state and status information regarding its installed major components, line and plug-in cards, and processes.

[Required] An MG shall conform to all applicable OTGR requirements for trouble detection, verification, and notification in a switching system NE given in Telcordia Technologies GR-474-CORE. Specifically, the requirements from GR-474-CORE are R474-83 through 0474-85, 0474-88, R474-90, R474-92, and R474-93. .

5.3.2.18.3.2 MG Support for Fault Management

5.3.2.18.3.2.1 MG Alarm Surveillance

[Required] Upon the detection or clearing of alarm conditions, the MG shall generate and forward, based on filtering criteria, a notification to the E2E RTS EMS.

[Required] An MG shall support queries for alarm status, state, and current problem information.

[Required] An MG shall monitor, detect, and generate alarm conditions and states associated with hardware, functional components, system interfaces, and logical resources (e.g., trunk terminations, tone and announcement generators, media content detectors, signal processors, echo control devices).

5.3.2.18.3.2.2 MG Fault Localization

Fault localization determines the root cause of a failure. Where the initial failure information is insufficient for fault localization, it has to be augmented with information obtained by additional failure localization routines.

[Required] An MG shall perform root cause analysis for any faults within its purview, report the root cause and suppress the reporting of non-root cause conditions.

5.3.2.18.3.2.3 MG Support for Testing

Testing is concerned with the testing of transmission facilities and related resources within the MG. Testing may be carried out for the following purposes:

- Testing connecting facilities in preparation for installation of new equipment
- Accepting newly installed facilities or service circuits
- Validating trouble reports
- Supporting fault localization
- Verification of repair

[Required] An MG shall on request or per a pre-established schedule run diagnostics on internal resources, hardware, or software and report the result to the E2E RTS EMS.

[Required] An MG shall provide both local and remote loopback capabilities for the digital interfaces that terminate at the MG ports.

[Objective] It is desirable that an MG provide test access to external test equipment for passively monitoring the traffic through the MG interfaces. This passive monitoring shall not degrade the performance of traffic.

5.3.2.18.3.3 MG Support for Performance Management

This section addresses the performance management criteria used to evaluate and report on the behavior and effectiveness of the MG, which includes gathering and analyzing of statistical data on interfaces that the MG supports.

5.3.2.18.3.3.1 Counters and Monitoring Intervals

All counters need to be designed so they remain at their maximum value, so that they do not "roll over" to "000...000." It is stressed that the term "counter" does not imply an implementation. For example, if three counts are required as well as an associated sum of errors counter, this could be implemented as two registers for two simple counts and one register for the sum of errors. The third simple count could be inferred from the other two.

[Required] Upon receiving a request from the E2E RTS EMS or by an established schedule, an MG shall provide a report of a parameter's present or past history counters.

[Required] For all counters, the MG shall store the current interval and 8 hours of history data.

5.3.2.18.3.3.2 Generation of Threshold Crossing Alerts

This section contains general requirements on the generation of TCAs. A particular count should generate a TCA if the requirement defining the count indicates that the count should be thresholded.

[Required] An MG shall generate TCAs to notify the E2E RTS EMS when a thresholded count exceeds its threshold during a measurement interval.

5.3.2.18.3.4 Trunk Configuration Requirements

[Required] The MG shall manage interexchange trunk (between MG and SSP), trunk group, trunk, and physical resource inventory and configuration data.

[Required] The MG shall manage MG termination-related status information. This information includes the following:

- Context-ID Operational and Service status
- Trunk Administrative, Operational, and Service status
- Termination ID Administrative, Operational, and Service status

5.3.2.18.3.5 MG Trunk Fault Management

[Required] The MG shall include in the alarm notifications sufficient information to isolate failed replaceable units.

[Required] **The** MG shall support queries for alarm status, state, and current problem information.

[Required] The MG shall generate an alarm condition when any of the following failure conditions:

- Power loss
- Environmental condition not conducive to normal operation
- Loss of data integrity
- Interface faults (core, trunk, MG-CCA)
- Hardware and line card faults
- Functional Component and Resource faults
- Protocol alarm conditions

[Required] An MG shall, on request or on schedule, run diagnostics on internal resources, hardware and checks on software, and report the result to the E2E RTS EMS.

The MG shall provide both local and remote loopback capabilities for the physical signals that terminate at the MG ports.

[Required] The MG shall provide test access to external test equipment for passively monitoring the traffic through the MG interfaces. This passive monitoring shall not degrade the performance of traffic.

5.3.2.18.3.6 Trunk Performance Management (MG)

All Trunk Performance Management requirements are covered by the MG requirements.

5.3.2.18.3.7 Access Configuration Requirements

[Required] The MG shall receive voice grade analog line configuration data from the E2E RTS EMS upon service activation.

5.3.2.18.3.7.1 Conventional DS1 Interface to PBX

[Required] The MG shall receive digital signal 1 (DS1) Interface configuration data from the E2E RTS EMS upon service activation.

5.3.2.18.3.7.2 ISDN PRI Trunks

[Required] The MG shall receive ISDN PRI trunk configuration data from the E2E RTS EMS upon service activation.

5.3.2.18.3.7.3 Interface Status Parameters

[Required] The MG shall set the status parameters necessary for support of ISDN digital subscriber lines basic rate and DS1 interfaces.

5.3.2.18.3.8 Access Fault Management

Many circuit troubles are detected by the customer, but others may be detected by per-call or automatic routine tests.

[Required] The MG shall provide diagnostic tests to detect and verify faults, such as low loop resistance or ground conditions, or any other faults within the MG that could cause false ring trip or false answer.

The actual tests needed to satisfy the previous requirement depend on the MG implementation, and hence are not specified in this generic requirements document.

[Required] The Integrated Digital Terminal (IDT) function in the MG shall support all the protection switching requirements as specified in Telcordia Technologies GR-303-CORE.

[Required] An MG providing DS1 interfaces shall detect line and path defects as specified in Telcordia Technologies GR-820-CORE, Section 4.1.2, *DS1 Performance Defects*.

DS1 defects include Loss of Signal (LOS), Out of Frame (OOF), Severely Errored Frame (SEF), Alarm Indication Signal (AIS), and Alarm Indication Signal - Customer Installation (AIS-CI). The AIS-CI defect detection is not applicable to an Integrated Digital Loop Carrier (IDLC) DS1 interface. See Telcordia Technologies GR-303-CORE, Sections 4.7 and 4.9, for additional IDLC-related criteria.

[Required] An MG providing DS1 interfaces shall support the DS1 failure declaration process (i.e., line, near end path, far end path) specified in Telcordia Technologies GR-820-CORE, Section 4.

DS1 failures include LOS, OOF, AIS, AIS-CI, Remote Alarm Indication (RAI), and Remote Alarm Indication - Customer Installation (RAI-CI). The AIS-CI and RAI-CI failure detections are not applicable to an IDLC DS1 interface. See Telcordia Technologies GR-303-CORE, Sections 4.7 and 4.9, for additional IDLC-related criteria.

[Required] An MG providing DS1 interfaces shall generate DS1 trouble notifications (i.e., alarms) upon the declaration of a DS1 failure condition. Trouble notifications shall be consistent with the DS1 line and path trouble notification criteria specified in Telcordia Technologies GR-474-CORE, Section 8.2.

[Required] The MG shall generate alarm conditions for digital signal 3 (DS3) signals by monitoring the paths and lines for failures, as specified in Telcordia Technologies GR-820-CORE, Section 5.

5.3.2.18.3.8.1 IDLC Trouble Management

A trouble notification alerts a technician, either directly or through the E2E RTS EMS, to the existence and severity of IDLC system troubles. Trouble indications aid the technician to restore service using spare facilities, to sectionalize the trouble for efficient scheduling and dispatch of repair personnel, and to determine the nature of the trouble and the units likely to be the cause of the trouble.

Trouble verification is the process of confirming the existence of a trouble once a trouble has been detected. Trouble verification is needed to verify that the trouble still exists before dispatching a technician and to verify that the trouble has been cleared after a repair has been made.

Trouble isolation is performed after trouble detection, verification, and automatic service recovery in an attempt to determine the source of the trouble. Trouble isolation attempts to isolate the source to a minimum number of replacements. The replaceable elements are reported

in the order of most likely element first to the least likely element last. Trouble isolation does not affect regular service.

[Required] The MG shall conform to all applicable requirements and objectives for trouble detection, verification, and notification in an IDLC system, if it is supported by the MG, as given in Telcordia Technologies GR-303-CORE.

[Required] The MG shall provide a 102 Type Test Line function as specified in Telcordia Technologies GR-822-CORE, Section 6.

[Required] The MG shall conform to all requirements specified for Test Access Units (TAUs) and Test System Controller/Remote Test Unit (TSC/RTU) features and functions for supporting metallic loop test access, in Telcordia Technologies GR-844-CORE.

[Required] The MG shall conform to all test initiating, generic loop testing, all related test commands and test measurement, and all special TSC/RTU calculation requirements as specified in Telcordia Technologies GR-844-CORE.

[Required] When metallic testing via a metallic bypass pair (or digital equivalent) is not being provided at the MG, the MG shall allow channel testing to be provided.

[Required] The MG shall meet the Digital Test Access criteria in Telcordia Technologies GR-303-CORE, Section 5.4.3.2.3, Circuit Testing, with “LDS” and “IDT” replaced with “MG.”

The Digital Test Access criteria in Telcordia Technologies GR-303-CORE, Section 5.4.3.2.3, allows for a built-in channel test capability or the use of an external TSC/RTU Channel Test function. The interface with an external channel test TSC/RTU is via a Digital Test Access Unit (DTAU) function in the MG.

[Required] An MG providing a built-in channel testing capability should provide a No Test Trunk interface to embedded test systems.

Some service providers may require an MG with a built-in channel test capability to be compatible with existing No Test Trunk-based test systems.

[Required] An MG providing a built-in channel testing capability shall meet the TSC1/RTU1 general and IDLC-specific criteria of Telcordia Technologies GR-822-CORE, Section 3.2, TSC/RTU Testing Requirements.

The Line Unit (LU) Test subsection in Telcordia Technologies GR-303-CORE Section 5.4.3.2.3, Circuit Testing, also describes the transmission and single party signaling tests that constitute channel testing.

For single party service, the signaling tests consist of verification of Remote Digital Terminal (RDT) off-hook detection and RDT ringing generation. In both cases, test results are conveyed to the TSC/RTU function via the robbed bit signaling bits associated with the channel under test. The detection of a power ringing signal generated by the LU under test is conveyed by the RDT via a transition from a Loop Open (LO) to a Loop Closure (LC) ABCD codeword.

The TSC/RTU transmission measurements are described in the LU Test subsection in Telcordia Technologies GR-303-CORE, Section 5.4.3.2.3. These tests consist of (1) echo return loss, (2) two-way channel loss, and (3) idle channel noise.

[Required] An MG providing a built-in channel testing capability shall provide the E2E RTS EMS with provisionable values of echo return loss, two-way channel loss, and idle channel noise that should be measured to indicate satisfactory performance of the LU under test.

[Required] The MG shall support Telcordia Technologies GR-303-CORE Embedded Operations Channel (EOC) messages to connect and release test access.

Telcordia Technologies GR-303-CORE EOC is used to disconnect an RDT LU from the distribution facilities, connect the output of an RDT LU to a specified test response circuit, and to provide test access to the distribution facility if metallic testing is being performed.

5.3.2.18.3.8.2 ISDN PRA Testing

There are multiple ways by which test accesses are provided to the MG to support ISDN Primary Rate Access (PRA) testing. They are as follows:

- Monitor Access function
- Split Access function
- Digital Test Unit (DTU) Loopback function

The MG shall conform to the test access, access supervision, and test signal and bit error insertion, line loopback control, signal monitoring and measuring, and service state control requirements as specified in TR-NWT-001219.

5.3.2.18.3.9 MG Access Performance Management

The following requirement applies to all interfaces from the MG to the MFSS or LSC ASLAN.

In addition, the DS1 physical layer protocol monitoring requirements shall apply to the MG ISDN PRI interfaces, Telcordia Technologies GR-303-CORE IDLC interfaces, and non-ISDN PBX trunk interfaces supported by DS1 transport.

[Required] The MG shall support the collection of the standard DS1, DS3, Physical Layer Convergence Protocol (PLCP), synchronous optical network (SONET), and ISDN BRI line performance monitoring requirements, as defined in Telcordia Technologies GR-820-CORE, for applicable interfaces.

5.3.2.19 Accounting Management

This section provides the minimum set of requirements to capture the basic call information for accounting purposes. Additional information on this call accounting is contained in Telcordia Technologies GR-3058-CORE.

Accounting management identifies a set of events during which call detail information is collected. These events are call connect, call attempt, and call disconnect. When these events are detected, specific call data will be provided by the network appliances that were involved in the event. Each appliance has a certain function within the network, and thus will be in the natural position to have knowledge of particular call data. It is the collections of this call information from all appliances that will provide the data necessary to formulate a billing record.

The requirements provided in this section allow for the functional elements to be individual components within the network, or packaged together in an integrated system solution. In either case, each component will have a certain role in the call, and be privy to specific call data that is needed to construct a billing record.

This section assumes that the Media Server function, the UFS function, and the Directory function together provides the necessary information and services needed for billing and jointly provide the functional equivalent to a Services Agent (SA). A Service Agent is defined as follows:

- The SA supports the execution of service logic both for transactions that occur completely within the IP network, and those that require signaling to CCS7 SEPs (e.g., SG, SCP) that are external to the IP network. The SA may be part of the network appliance that provides CCA functionality, or may be deployed in a separate appliance that communicates with the CCA.

It is further assumed that an LSC and an MFSS each has its own means of gathering call information (e.g., originating party, terminating party, time of call, date of call, call answered,

call unanswered) and process them into a call record. This function is equivalent to that of a Billing Agent (BA). A Billing Agent is defined as follows:

- A BA supports much of the billing functionality needed in the VoIP network. It collects the necessary call data from the CCAs and other network appliances, and processes them for use by downstream billing systems.

This section assumes that the E2E RTS EMS will provide the same functionality as that of the BA. Therefore, throughout the remainder of this document, reference to the BA should be viewed as the functional equivalent that resides within the E2E RTS EMS. As such, the communications between the functional entities (e.g., CCA, MGC) and the BA will be internal to the appliance, and all the necessary accounting data is assumed to be made readily available to the BA.

However, there may be network appliances that are externally linked to the softswitches (e.g., an external MG connecting into the MGC of the LSC). Depending on the purpose of these network appliances, they may be in the best position to obtain specific accounting data on calls that involve the use of this external network appliance. As such, this data should be provided to the BA (whether this information is passed to the BA directly, or passed to the CCA or MGC, which then passes it to the BA).

The following section presents the requirements for accounting data that should be provided by the functional entities to the BA. Section 5.3.2.19.2, Processing of Data Sets, applies to external network appliances (e.g., MG) that need to provide accounting data to the BA. As mentioned before, functional entities within a network appliance are assumed to have their own means of sharing accounting data; however, the requirements in the following section can be used to ensure that the specific data is made available to the BA (within the internal communications and sharing) so that the proper accounting can be accomplished.

5.3.2.19.1 Accounting Data

[Objective] It is desirable for a network appliance to support the data sets described in this section for supplying accounting information to the necessary functional entity that will generate call detail recordings.

The call data captured for calls that are detected by the CCA and other functional entities are the individual pieces of data that, when logically assembled by the BA, provide the details required to account for the use of a service. Some of this call data is captured based on call events, usually determined from the content of received signaling messages. Other call data is determined from local information maintained at the CCA.

Whenever the CCA or other functional entities generate call data, the CCA or other functions would package the call data into what is known as a Data Set (DS), which is then transmitted to the BA. Data set is another name for Telcordia Technologies GR-3058-CORE's Protocol Data Unit (PDU). It should be noted that the term DS (or PDU) is used in the generic sense to describe a unit of related information, and is not meant to imply the use of any specific protocol for the communications between the functional entities and the BA. The actual protocol for communications between the functional entities and the BA is considered to be a vendor decision.

The functional entities generate the data sets based on an event. Currently, three events generate the data sets as follows:

- Call Connect
- Call Disconnect
- Call Attempt (e.g., call was attempted, but unsuccessful)

Correspondingly, the three data sets are as follows:

1. Call Connect Data Set. Used for call data that represents a call connection event.

2. Call Disconnect Data Set. Used for call data that represents a call disconnection event.

3. Call Attempt Data Set. Used for call data that represents a call attempt event.

A successful voice call would have two events (each of which would result in data sets): the Call Connection event and the Call Disconnection event. For unsuccessful voice calls, the call event would result in the generation of the Call Attempt Data Set(s). This can also apply to a Video session. For example, when a user wants to open a Video session, a connection attempt will need to be made to the application that will provide the video.

Thus, either a Call Connection Data Set (if the video connection is made) or a Call Attempt Data Set (if the video connection is attempted, but is not successfully connected) would be generated. If a video connection is made and the video is played, a Call Disconnect Data Set will be generated once the video connection is over.

The following subsections will provide the formatting and the field definitions for the Call Connect Data Set (The Call Attempt Data Set has the same format as the Call Connect Data Set.) and the Call Disconnect Data Set. The formatting will be provided in a table with the following column headings:

1. The first column identifies the call data.

2. The second column identifies whether this data is conditionally required or optional for the DISN.

3. The third column specifies the call data as either fixed or variable in length.

4. The fourth column identifies the section in Telcordia Technologies GR-3058-CORE that provides more information on the fields.

5. The fifth column provides a summary of how the field is populated.

6. The sixth column reflects what is currently believed to be the most appropriate network component for each data element. "Pri" indicates the NC network appliance that is considered to be the "primary" source for the data element.

7. The seventh column reflects what is currently believed to be the "secondary" source or source of the data for that particular element. It is labeled as "Sec."

The fifth column does not necessarily preclude the vendor from using the CCA as the sole source of the data elements and have all other functional elements provide data to the CCA for population in the PDUs sent to the BA. The data elements in the PDU need to arrive at the BA to generate an accurate, timely, and verifiable CDR. The choice of the particular method to get the data elements to the BA is left to the vendor.

NOTE: For a field that has been designated as conditionally required, the field should be populated with the appropriate data if that data is available and applicable to the call. For example, if a call originates from the PSTN and terminates into the VoIP network, the MGC would be utilized in completing this call. This means that information (e.g., the Ingress Trunk Group number) would be available. Since the Data Set field for the Ingress Trunk Group number is required, that field should be populated with the trunk group number.

5.3.2.19.1.1 Call Connect Data Set

Table 5.3.2-56, Call Connect Data Set Information, provides the formatting and fields for the Call Connect Data Set.

Table 5.3.2-56. Call Connect Data Set Information

USAGE DATA ELEMENT	DEPEND REQ'D/ OPTIONAL	FIXED/ VARIABLE	REFERENCE SECTION IN GR-3058-CORE	POPULATION SUMMARY	PRI	SEC
Call Event Type	R	F	3.3.6.	1 = Call Completion 3 = Call Attempt	CCA	MG MGC
Correlation ID	R	F	3.3.6.2	UUID = 128 bits (Variable depending on implementation) Unique value for each call composed of: 1. Network Component Network Appliance ID 2. Timestamp 3. Random Number	CCA	MG MGC
Element Identifier	R	F	3.3.6.	Range of 000001 through 999999	CCA	MG MGC
Directional Indicator	R	F	3.3.6.4	1 = Egress (originating) 2 = Ingress (terminating) 3 = Transiting (MGC) 4 = Intra-gateway (AGW)	CCA	MG MGC
Study/Test Indicator	R	F	3.3.7.1	Default = zeros (or null-value)	CCA	MG MGC
Timing Guard	R	F	3.3.7.1	0 = no timing irregularities detected 2 = timing irregularities detected	CCA	MG MGC
Customer Connect Date Customer Connect Time	R	F	3.3.7.2	MMDDYYYY - Month, Day, and Full Year HHMMSSms – Hours, Minutes, Seconds, and milliseconds (depending on implementation).	MG	CCA MGC
Incoming Destination Number	R	V	3.3.8.7	For services other than toll-free – destination routing address (if NANP based, this is pre-NP query – NOT the LRN) For toll-free – NANP routing number (pre-NP query – NOT the LRN) returned from toll-free query	MG	CCA MGC
Destination Address [IN and AIN queries only]	R	V	3.3.9.1	For toll-free – NANP routing number (pre-LNP query – NOT the LRN) returned from toll-free query	CCA	SA MGC

USAGE DATA ELEMENT	DEPEND REQ'D/ OPTIONAL	FIXED/ VARIABLE	REFERENCE SECTION IN GR-3058-CORE	POPULATION SUMMARY	PRI	SEC
Calling Station ID	R	V	3.3.7.6	Used for CPN	MG	CCA MGC
Called Station ID up to 15 digits	R	V	3.3.7.7 3.3.10.4	Egress calls Ingress calls dealing with NP	MG	CCA MGC
Overseas Indicator	R	F	3.3.7.7	0 = North America World Zone 1 1 = International (01 or 011 prefix dialed)	MG	CCA MGC
Operator Involvement	R	F	3.3.7.7	0 = No Involvement 1 = 0+ or 0- dialed	MG	CCA MGC
Dialing Indicator	R	F	3.3.7.7	0 = No CAC 1 = 10XXXX dialed	MG	CCA
Dialed Carrier Identification Code	R	F	3.3.7.7	Carrier Identification Code (if dialed) Default = zeros (or null-value)	MG	CCA MGC
Presubscription Indicator	R	F	3.3.7.7	0 = No presubscription on line 1 = PIC present	MG	CCA
PIC - Presubscribed Carrier Identification Code	R	F	3.3.7.7	Carrier Identification Code when PIC = 1 Default = zeros (or null-value)	MG	CCA MGC
ANI (Charge Number)	R	F	3.3.7.9	ANI for Originating Call ChN received for transiting and terminating calls	MG	MGC
Service Provider Identification – Switching System ID	R	V	3.3.7.10	Operating Company Number of CCA owner	MG	CCA MGC
Service Provider Information – Account Owner	R	V	3.3.7.10	Operating Company Number of the Calling Station's Service Provider	MG	CCA MGC

USAGE DATA ELEMENT	DEPEND REQ'D/ OPTIONAL	FIXED/ VARIABLE	REFERENCE SECTION IN GR-3058-CORE	POPULATION SUMMARY	PRI	SEC
Service Feature	R	F	3.3.7.11	Reference Table 12 of GR-1100-CORE for representative list of service features that could be provisioned on a line at the AG. A few notable features of importance are: 7 Call Forwarding 8 Call Hold 9 Call Transfer 10 Call Waiting 11 Conference Call	MG	CCA MGC
Calling Station Porting Status	R	F	3.3.10.1	0 = Not Ported 1 = Ported 2 = Not on AG	MG	CCA MGC
Called Number Porting Status	R	F	3.3.10.1	0= Not Ported 1 = Ported 2 = Not on AG	MG	SA
Incoming Calling Party Number	R	V	3.3.7.9	CPN parameter in CCS7 or functional equivalent	MGC	CCA MGC
Facility Allocation Date Facility Allocation Time	R	F	3.3.7.3	MMDDYYYY – Month, Day, and Full Year HHMMSSms – Hours, Minutes, Seconds, and milliseconds (depending on implementation)	MGC	CCA
Service Type	R	F	3.3.7.5	1 = No CS-PSTN Interface 2 = Interface to CS-PSTN (via MGC)	MGC	CCA
Called Party Offhook	R	F	3.3.7.8	0 = Called Party Offhook detected 1 = Called Party Offhook not detected	MGC	CCA
Egress Trunk Group Number	R	F	3.3.8.1	Provisioned TG number at MGC (TG)	MGC	CCA
Egress Trunk Group Designation	R	F	3.3.8.1	See Table 3-3 in GR-3058-CORE	MGC	CCA
Egress Signaling Protocol	R	F	3.3.8.4	See Table 3-4 in GR-3058-CORE	MGC	CCA
Egress Interfacing Network ID	R	V	3.3.8.2	Operating Company Number assigned to the interfacing Network Provider	MGC	CCA

USAGE DATA ELEMENT	DEPEND REQ'D/ OPTIONAL	FIXED/ VARIABLE	REFERENCE SECTION IN GR-3058-CORE	POPULATION SUMMARY	PRI	SEC
Egress Trunk Group Billing Number	R	F	3.3.8.2	Billing Number assigned to the facility	MGC	CCA
Egress QoS Statistics	R	F	3.3.8.5	Variable – See Table 3-5 in GR-3058-CORE	MGC	CCA
Ingress Trunk Group Number	R	F	3.3.8.1	Provisioned TG number at MGC (TG)	MGC	CCA
Ingress Trunk Group Designation	R	F	3.3.8.1	See Table 3-3 in GR-3058-CORE	MGC	CCA
Ingress Signaling Protocol	R	F	3.3.8.4	See Table 3-4 in GR-3058-CORE	MGC	CCA
Ingress Interfacing Network Id	R	V	3.3.8.2	Operating Company Number assigned to the interfacing Network Provider	MGC	CCA
Ingress Trunk Group Billing Number	R	V	3.3.8.2	Billing Number assigned to the facility	MGC	CCA
Ingress QoS Statistics	R	V	3.3.8.5	Variable – See Table 3-5 in GR-3058-CORE	MGC	CCA
Release Cause	R	V	3.3.8.6	Variable – See Table 3-6 in GR-3058-CORE for examples	MGC	CCA
Jurisdiction Designation of MGC	R	F	3.3.8.3	NPA-NXX representative of the Jurisdiction of the MGC	MGC	CCA
CCA-LRN	R	F	3.3.10.2	When Directional Indicator = 1, then LRN of the originating CCA-MGC-AG combination When Directional Indicator = 2 or = 3, then zeros	MGC	CCA
Incoming JIP	R	F	3.3.10.3	When Directional Indicator = 2 or = 3, then the digits contained in the JIP parameter (CCS7) or equivalent	MGC	CCA
Toll-Free Query Indicator	R	F	3.3.9.1	141 = Handoff to IC 142 = LEC Transport	SA	CCA
Toll-Free CIC	R	F	3.3.9.1	Toll-Free Transport provider	SA	CCA
LRN – DB	R	F	3.3.10.2 3.3.10.3 3.3.10.4	Ported = LRN of destination switch Non-Ported – Called Number	SA	CCA

USAGE DATA ELEMENT	DEPEND REQ'D/ OPTIONAL	FIXED/ VARIABLE	REFERENCE SECTION IN GR-3058-CORE	POPULATION SUMMARY	PRI	SEC
LNP Query Status	R	F	3.3.10.2 3.3.10.3 3.3.10.4	See Table 3-7 in GR-3058-CORE	SA	CCA
Originating Customer/ Business Group Identification	R	F	7.1.1.1	10-Digit Originating Customer/Business Group Identification number	MG	CCA MGC
Terminating Customer/ Business Group Identification	R	F	7.1.1.2	10-Digit Terminating Customer/Business Group Identification number	MG	CCA MGC
CCA IPv4 Address	R	F	3.3.7.10	IPv4 address assigned to the CCA	CCA	CCA
CCA IPv6 Address	R	F	3.3.7.10	IPv6 address assigned to the CCA	CCA	CCA
Bearer Capability/Call Type	R	V	3.3.7.12	Bearer call type and bearer capabilities delivered to the user	MG	CCA MGC
Network Interworking	R	V	3.3.7.12	Identifies the different interworking situations encountered by the user's call	MGC	CCA
Signaling or Supplementary Service Capabilities Usage	R	V	3.3.7.12	Records the use of signaling or supplementary service capabilities on a yes/no or other outcome basis, and it is designed to record one, all, or any combination of these capabilities in a single record.	MGC	CCA
Call Characteristic	R	F	7.1.1.3	1 = Voice 2 = Video	MG	CCA MGC
Bandwidth Reservation	R	V	7.1.1.4	Used to indicate the rate (in kbps/sec) that is reserved for this session (e.g., a voice call or a Video session may have a fixed amount of bandwidth).	MGC	CCA AGW
Service Level Priority	R	F	3.3.7.14	Value used to indicate the service level of the call	MGC	CCA AGW

[Objective] For every call attempt, call completion, and transiting call detected by the CCA, the CCA and any other functional entities (if applicable) shall provide information to properly populate the Call Connect Data Set following the rules outlined in Table 5.3.2-56, Call Connect Data Set Information.

5.3.2.19.1.2 Originating Customer/Business Group Identification

The Originating Customer/Business Group identification identifier is a 10-digit value that identifies the Customer or Business Group associated with a service. This ID is usually provided through some service application or some database. If this is available, it will be populated in the Originating Customer/Business Group Identification field.

[Objective] If an Originating Customer/Business Group Identification number is available, it will be populated in the Originating Customer/Business Group Identification field.

5.3.2.19.1.3 Terminating Customer/Business Group Identification

The Terminating Customer/Business Group Identification identifier is a 10-digit value that identifies the customer or business group associated with a service. This ID is usually provided through some service application or some database. If this is available, it will be populated in the Terminating Customer/Business Group Identification field.

[Objective] If a Terminating Customer/Business Group Identification number is available, it will be populated in the Terminating Customer/Business Group Identification field.

5.3.2.19.1.4 Call Characteristic

The Call Characteristic identifies how a particular call is set up. For example, the Call Characteristic will identify whether the call is a voice call or a video call.

[Objective] The Call Characteristic field will be populated with a value of one to indicate that this particular data set represents a Voice call.

[Objective] The Call Characteristic field will be populated with a value of two to indicate that this particular data set represents a Video session.

5.3.2.19.1.5 Bandwidth Reservation

On VoIP voice calls or calls that utilize video calls, there is a need to record the bandwidth that is allocated for the type of service call. This information can be used for maintenance or for projections on future usage and growth. This field bandwidth is measured in units of kbps.

[Objective] The Bandwidth Reservation field will be populated with the amount of bandwidth reserved in kbps.

5.3.2.19.1.6 Call Disconnect Data Set

Table 5.3.2-57, Call Disconnect Data Set, provides the formatting and fields for the Call Disconnect Data Set.

Table 5.3.2-57. Call Disconnect Data Set

USAGE DATA ELEMENT	REQUIRED/ OPTIONAL	FIXED/ VARIABLE	REFERENCE SECTION IN GR-3058-CORE	POPULATION SUMMARY	PRI	SEC
Call Event Type	R	F	3.3.6.1	1 = Call Completion 2 = Call Disconnect 3 = Call Attempt	CCA	MG MGC
Correlation ID	R	F	3.3.6.2	UUID = 128 bits (Variable depending on implementation) Unique value for each call composed of: 1. Network Component Network Appliance Id 2. Timestamp 3. Random Number	CCA	MG MGC
Element Identifier	R	F	3.3.6.3	Range of 000001 through 999999	CCA	MG MGC
Directional Indicator	R	F	3.3.6.4	1 = Egress (originating) 2 = Ingress (terminating) 3 = Transiting (MGC) 4 = Intra-gateway (AGW)	CCA	MG MGC
Service Type	R	F	3.3.7.5	1 = No CS-PSTN Interface 2 = Interface to CS-PSTN (via MGC)	CCA	MG MGC
Timing Guard	R	F	3.3.7.1	0 = no timing irregularities detected 2 = timing irregularities detected	CCA	MG
Disconnect Detection Date Disconnect Detection Time	R	F	3.3.7.4	MMDDYYYY – Month, Day, and Full Year HHMMSSms – Hours, Minutes, Seconds, and Milliseconds (depending on implementation).	CCA	MG MGC
Release Cause	R	V	3.3.8.6	Variable – See Table 3-6 for examples	CCA	MG MGC

[Objective] For every call disconnect detected by the CCA, the CCA and any other network appliances (if applicable) shall provide information to properly populate the Call Connect Data Set following the rules outlined in Table 5.3.2-57.

5.3.2.19.1.7 Billing Agent

The functions of the Billing Agent are to provide processing, formatting, storage, and outputting of usage records for delivery to downstream processing systems. In the VoIP system design, it may be so the functional entities (e.g., CCA, MGC) of a network appliance are responsible for generating the call data, and transmitting them this data to the BA in the form of a data set or through network appliances internal means of communication and data sharing (assuming all these functional entities are internally connected). It is then up to the BA to gather all the accounting data and process it to determine the proper recording format.

The BA may be a separate entity within a network; or it may be internally connected to the other functional entities within a network appliance. In either case, the BA should be able to process, format, store, and output generated usage records based on either the data sets or the accounting data that it will receive. If the network utilizes data sets as defined in UCR 2008, Section 5.3.2.19.1, Accounting Data, the Dependent Requirements in UCR 2008, Section 5.3.2.19.2.1, Call Data, and the requirements in the rest of UCR 2008, Section 5.3.2.19.2.2, Record Format, shall apply. Otherwise, only the requirements in UCR 2008, Section 5.3.2.19.2.2, Record Format, and so forth shall apply.

5.3.2.19.2 Processing of Data Sets

To process data sets, the BA must have the capability to match and correlate multiple data sets (generated from multiple functional entities) that are associated with the same call. In addition, a Call Connect Data Set will often have a corresponding Call Disconnect Data Set that will be delivered at one point or another. The BA must be able to correlate these sets of records together. The ability to correlate all these data sets is made possible by the use of the Correlation ID. Telcordia Technologies GR-3058-CORE has additional information regarding the format and use of the Correlation ID.

As the BA processes the data sets, it basically assembles the call data from the various data sets and formats it into an appropriate record, and stores it in the appropriate format. Processing of assembled call data for a particular call is activated immediately upon receipt of the Call Disconnect Data Set for that call. The following requirements are taken from Telcordia Technologies GR-3058-CORE and they pertain to the processing and assembling of the call data:

1. **[Objective]** The BA shall activate usage assembly within 250 ms of receiving a disconnect Data Set from the network component network appliances.

2. **[Objective]** The BA shall correlate all usage measurements related to a single VoIP call to produce the appropriate usage record(s).

5.3.2.19.2.1 Call Data

Regardless of the recording format that is chosen, there is information that is important for proper billing and accounting. Also, there is information that may be necessary for one type of call, but may not be necessary for another type of call. The following requirement lists the call data that are needed in the recording (Of course, there are other call data that are also desired and thus should be captured in the record; however, the data items listed in the following requirement are the call data that must be provided.):

[Required] For the selected recording format that is chosen of all the call information that will be provided, the following call data shall be provided in the record data:

1. Host Name of the CCA controlling the call processing

2. Start Date of call (In Julian or Calendar)

3. Start Time of Call (Hour + Minuet + Second)

4. Elapsed Time of Call and/or Stop Time of call

5. Calling Number

6. Called Number (included all dialed digits)

7. **[Conditional]** Call Answered/Unanswered Indicator

8. Precedence level of call (NOTE: This may be accomplished either by a specific precedence level designation field in the call or by providing the dialed precedence level access digits in the called number field.)

9. **[Conditional]** Indication of either a VoIP or Video over IP “call”

10. **[Conditional]** Indication of the assigned bandwidth for the entire duration of the Video over IP “call”

[Required] For the selected recording format that is chosen, of all the call information that will be provided, the following call data shall be provided in the record data if it applies to the call:

1. **[Required]** Conference Call Indicator

2. **[Conditional]** Customer/Business Group Identification

The Conference Call Indicator is used to identify callers that are participants in a conference call, which will be useful for tracking purposes, or if there is special billing associated for conference calls.

For Customer/Business Group identification, the originating party (or even the terminating party) may be part of a customer or business group. Special billing or charges may apply to a member of a particular group; and thus for calls where the originating party and/or terminating party is assigned a Customer/Business Group Identification, the Customer/Business Group Identification information should be provided in the CDR as per the previous requirement.

The following subsections describe the types of VoIP calls (e.g., PSTN to IP, IP to PSTN), and provide additional call information that should be captured in the CDR.

5.3.2.19.2.1.1 Quality of Service

For VoIP calls, compression of voice traffic is used to conserve bandwidth. However, compression at one end and decompression at the other end usually results in a degradation of voice quality. Since stronger compression usually results in further degradation of voice quality, service providers need to find a balance between the two. In order to determine if the voice quality is sufficient enough to warrant the level of compression, there needs to be some means by which the quality of the call can be measured.

The "system" in the requirements below is the combination of the LCS or MFSS and the set of End Instruments that it serves.

[Required: LSC, MFSS] The system shall provide a voice quality record at the completion of each voice session. The voice quality record shall be included in the CDR that the LSC or MFSS generates for that session and shall conform to the E-Model, as described in TIA TSB-116-A, and ITU-T Recommendation G.107. The voice quality record shall contain the calculated R-Factor for the Voice session per TSB-116-A. The allowable error for the voice quality calculations shall be +/- 3 in accordance with TIA TSB-116-A. NOTE: This requirement is only related to VoIP EIs and is not applicable to MGs.

[Required: LSC, MFSS] As part of the voice quality record, the system shall provide the raw voice session statistics that are used to provide the R-Factor calculation to include, as a minimum, the latency, packet loss, Equipment Impairment Factor (Ie), and the TCLw. (Definitions of latency and packet loss are found in UCR 2008, Appendix A, Definitions,

Abbreviations and Acronyms, and References, and the methods of calculation are described in UCR 2008, Section 5.3.3, Network Infrastructure End-to-End Performance Requirements.)

[Required: LSC, MFSS] The system shall provide the jitter for the session. (See UCR 2008, Appendix A, Definitions, Abbreviations and Acronyms, and References, for the definition of jitter. The method of calculation is described in UCR 2008, Section 5.3, Network Infrastructure End-to-End Performance Requirements.)

For example, the EI can generate an initial voice quality record at the end of an EI Voice session, which contains the latency, packet loss, Ie, TCLw, and jitter, but not the R-factor. The EI can use the Voice media packets that it sent and received over the duration of the Voice session to compute these values. The EI can send this initial Voice quality record to its LSC or MFSS as part of the EI signaling that ends the Voice session.

The LSC or MFSS can use this initial Voice quality record to calculate the R-Factor for the session. The LSC or MFSS can generate a final voice quality record containing the latency, packet loss, Ie, TCLw, and jitter values received from the EI, and the R-Factor that it calculated. Then the LSC or MFSS can generate a CDR for the session that contains the final Voice quality record.

This example shows how the EI and LSC/MFSS can jointly generate the Voice quality record and CDR, and meet the previous system requirements.

[Required: LSC, MFSS] The system shall generate an alarm to the E2E RTS EMS when the session R-Factor calculation in the CDR fails to meet a configurable threshold. By default the threshold shall be an R-Factor value of 80, which is equivalent to an MOS value of 4.0.

5.3.2.19.2.1.2 VoIP to PSTN

VoIP to PSTN calls refers to calls routed to the PSTN from a VoIP network. An example of this is a call that originates in the VoIP network and utilizes the PSTN to complete the call. Another example could be a call that originates from another network (be it a PSTN or another VoIP network), enters this VoIP network, and transits out to the PSTN.

For the transiting case, there may be two CDRs that are generated. One CDR would represent the incoming call into the VoIP network, and the other CDR would represent the outgoing call to the PSTN. For information on what call data to capture for the incoming portion of the call, please refer to UCR 2008, Section 5.3.2.19.2.1.3, PSTN to VoIP, for incoming calls from the PSTN, and UCR 2008, Section 5.3.2.19.2.1.4, VoIP to VoIP, for calls incoming from a VoIP network.

When a call originates in the VoIP network and continues into the PSTN for completion; there is certain information related to the PSTN that should be captured in the CDR, which is generated in the VoIP network. The following requirement indicates the specific call information:

1. **[Required]** In addition to the call data as specified previously, the following call data must be provided in the record data for calls that are routed to the PSTN from the VoIP network:

    a. IP address of originating subscriber (if the call originated from the subscriber on the VoIP network)

    b. IP address of the gateway connecting to the PSTN

    c. Outgoing trunk group of the call

    d. Outgoing trunk group member of the call

In the PSTN environment, calls are routed from one network to another via a trunk. A trunk group is a group of trunks and normally identified by a specific number. Similarly, a member of a trunk group is identified by another specific number. Identification of these trunk groups and trunk group members may be important for billing purposes (depending on the tariffs agreed between the VoIP service providers and the PSTN service providers) as well as for troubleshooting purposes.

5.3.2.19.2.1.3 PSTN to VoIP

PSTN to VoIP refers to the type of call where the call that originates in the PSTN network enters the VoIP network for completion. An example of this would be a call that originates from the PSTN network and terminates to a subscriber in the VoIP network. Another example would be a call from the PSTN enters the VoIP network, but transits to another VoIP network or back out to the PSTN. For these cases, there may be two separate CDRs. One CDR would represent the incoming call into the VoIP network, and another CDR would represent the call outgoing call to the PSTN or to another VoIP network.

This section addresses the incoming part of the call to the VoIP network. For the call data related to the outgoing part of the call, refer to UCR 2008, Section 5.3.2.19.2.1.2, VoIP to PSTN, for calls to the PSTN, and to UCR 2008, Section 5.3.2.19.2.1.4, VoIP to VoIP, for calls to another VoIP network.

As was the case for VoIP to PSTN scenario calls, there is certain information related to the PSTN that should be captured in the CDR that is generated in the VoIP network. The following requirement indicates the specific call information:

1. **[Required]** In additional to the call data as specified above, the following call data must be provided in the record data for calls that are routed from the PSTN to the VoIP network:

    a. IP address of terminating subscriber (if the call terminates to a subscriber on the VoIP network)

    b. IP address of the gateway connecting to the PSTN

    c. Incoming trunk group of the call

    d. Incoming trunk group member of the call

In the PSTN environment, calls are routed from one network to another network on a trunk. A trunk group is a group of trunks, and is identified by a specific number. Similarly, a member of a trunk group is identified by a specific number. Identification of these trunk group and trunk group members may be important for billing purposes (depending on the tariffs agreed between the VoIP service providers and the PSTN service providers) as well as troubleshooting purposes.

5.3.2.19.2.1.4 VoIP to VoIP

A VoIP to VoIP call can be one of the following three basic scenarios:

1. Subscriber in this VoIP network originates a call to another VoIP network

2. Subscriber in this VoIP network originates a call and terminates in the same VoIP network

3. Call from another VoIP network that terminates a call to a subscriber that belongs in this VoIP network

The first scenario could result in a CDR that captures originating type information. The second scenario could result in a CDR that captures terminating type information. Finally, the third scenario could result in two separate CDRs (i.e., one for originating, and another for terminating), or one CDR that captures both the originating and terminating information.

The next requirement identifies the call information that should be captured in the CDR that is generated for the originating call.

[Required] In addition to the call data specified previously, the following call data must be provided in the record data for calls that originate from the VoIP network and terminate to another VoIP network:

- IP Address of Originating Subscriber
- IP Address of the Gateway connecting to the other VoIP network (if applicable)

The following requirement identifies the call information that should be captured in the CDR that is generated for incoming calls from another VoIP network:

1. **[Required]** In addition to the call data specified previously, the following call data must be provided in the record data for calls that originate in one VoIP network, and terminates in another VoIP network:

   a. IP address of terminating subscriber
   b. IP address of the gateway connecting to the other VoIP network (if applicable)

For the third scenario, if there are two separate CDRs generated, one CDR would represent the originating part of the call, and the other CDR would represent the terminating part of the call. In this case, the originating CDR would contain the same call information as required previously for calls that originate in the VoIP network. The terminating CDR would contain the same call information as defined previously for calls that terminate in the VoIP network.

However, if the third scenario resulted in one CDR to capture both the originating and terminating information of the call, then the following requirement identifies the call information that should be captured in that singular CDR:

1. **[Required]** In addition to the call data specified previously, the following call data must be provided in the CDR (that captures both the originating and terminating information) for calls that originate from the VoIP network and terminate within the same VoIP network:

   a. IP address of originating subscriber
   b. IP address of terminating subscriber

5.3.2.19.2.2 Record Format

The actual format of the CDRs that the BA will create (either based on the call data acquired from the processing and assembly of the data sets or through internal call date sharing between functional entities) will be the format that is agreed upon between the DoD Network and the vendors of the BA. If the agreed upon format is Bellcore AMA Format (BAF), then the requirements in Telcordia Technologies GR-3058-CORE on the use of BAF will apply. For further information on the use of BAF, please refer to GR-3058-CORE, Section 4.3. The following subsections will provide some of the basic formatting found in GR-3058-CORE.

[Objective] If BAF is chosen as the Call Detail Recording format, the BAF requirements in GR-3058-CORE shall apply, with THE noted exception in the following subsections.

5.3.2.19.2.2.1 BAF Structure 0625

Originating and terminating calls (whether they are voice or video) that originates in another service provider's network or terminates in another service provider network or calls that utilize the PSTN would result in a Structure Code 0625. From For calls that originate and terminate from in the PSTN made to the VoIP network, to and for calls that both originate and terminate within the VoIP network, Structure Code 0625 is used to capture the call information. Table 5.3.2-58, BAF Structure 0625 and Field Populations, shows the format of Structure Code 0625 and the requirements on the field population. Further details on field population can be found in Telcordia Technologies GR-3058-CORE.

Table 5.3.2-58. BAF Structure 0625 and Field Populations

FIELDS OF THE STRUCTURE	REFERENCE SECTION IN GR-3058-CORE	BAF TABLE	POPULATION SUMMARY
Record Descriptor Word	4.3.3.1	000	Populate as described in GR-1100-CORE
Hexadecimal Identifier	4.3.3.2	00	Populate as described in GR-1100-CORE
Structure Code	4.3.3.3	0	00625 if no Module Codes are appended to this Structure 40625 if Module Codes are appended to this Structure
Call Type	4.3.6 4.3.7 4.3.8 4.3.9 4.3.15	1	Use the following: 110 = Originating Access Service 119 = Terminating Access Service 589 = Originating Connecting Network Access Service 720 = Terminating Connecting Network Access Service 060 = Basic Long Distance Service - Ingress 529 = VoIP Unidentified Call
Sensor Type	4.3.3.4	2	Sensor Type value associated with the network appliance
Sensor Identification	4.3.3.5	3	Populate character 1 as described in GR-1100-CORE Populate Characters 2-7 with the value of the Element Identifier in the Element Identifier usage element of the network component that is identified in the Sensor Type.

FIELDS OF THE STRUCTURE	REFERENCE SECTION IN GR-3058-CORE	BAF TABLE	POPULATION SUMMARY
Recording Office Type	4.3.3.6	4	Value assigned for the specific network appliance that contains the BA functionality that generated this record.
Recording Office Identification	4.3.3.7	5	Populate Character 1 as described in GR-1100-CORE Populate Characters 2-7 with the value of the Recording Office ID.
Connect Date	4.3.3.8	6	Populate Character 1 with the least significant digit of the year represented in the date the connection is made by the customer. Populate Characters 2-3 with the month represented in the date the connection is made by the customer. Populate Characters 4-5 with the day represented in the date the connection is made by the customer.
Timing Indicator	4.3.3.9	7	If timing irregularities have been detected, the BA shall populate Timing Indicator (Table 7) to indicate that a Timing Guard condition exists.
Study Indicator	4.3.3.10	8	Populate Characters 1 through 4 with the value of the Study/Test Indicator usage element Populate Character 5 with 0 Populate Character 6 as follows: — with 0 if complete originating and terminating numbers were received — with 1 if an all-zero originating number and a non-all-zero terminating number were received — with 3 if an all-zero terminating number and a non-all-zero originating number were received — with 4 if an all-zero originating number and an all-zero terminating number were received — with 5 if a terminating number with an all-zero station number and an originating number with a non-all-zero station number were received — with 6 if an originating number with an all-zero station number and a terminating number with a non-all-zero station number were received

FIELDS OF THE STRUCTURE	REFERENCE SECTION IN GR-3058-CORE	BAF TABLE	POPULATION SUMMARY
			— with 7 if a terminating number with an all-zero station number and an originating number with an all-zero station number were received. Populate Character 7 with 0.
Called Party Off-Hook Indicator	4.3.3.11	9	Populate Called Party Off-Hook (Answer) Indicator (Table 9) with 0 if call was completed and 1 if call was not completed.
Service Observed/Traffic Sampled	4.3.3.12	10	Populate Service-Observed/Traffic-Sampled Indicator (Table 10) with the "default" value per GR-1100-CORE.
Operator Action	4.3.3.13	11	Populate Operator Action (Table 11) to indicate no operator involvement per GR-1100-CORE.
Service Feature	4.3.3.14	12	Populate Service Feature Code (Table 12) with the value in Table 12 of GR-1100-CORE that maps to the service that applies to the call (e.g., 012 for Call Forwarding, 056 = Call Waiting, 605 = Call Hold, 160 = Call Transfer, etc.)
Originating NPA	4.3.3.15 4.3.9	13	Populate Originating NPA (Table 13) as follows: — NPA of the ANI (Charge Number) if non-zero, otherwise use the NPA of the Calling Station Id. This is when the ANI (or the CPN if ANI is not available) is 10 or less digits — per fill procedures described in GR-1100-CORE if the ANI (or CPN if ANI is not available is 11 digits or higher). See the section related to Ingress Trunk Group Billing number in GR-3058-CORE for when using the Ingress Trunk Group Billing Number usage element.

FIELDS OF THE STRUCTURE	REFERENCE SECTION IN GR-3058-CORE	BAF TABLE	POPULATION SUMMARY
Originating Number	4.3.3.16 4.3.9	14	Populate Originating Number (Table 14) as follows: — NXX-XXXX of the ANI if non-zero, other use the CPN (this is when ANI (or CPN if ANI is not available) is 10 digits or less — per fill procedures described in GR-1100-CORE if the ANI (or CPN if ANI is not available) is 11 digits or higher. See the section related to Ingress Trunk Group number in GR-3058-CORE for when using the Ingress Trunk Group
Overseas (International Call) Indicator	4.3.3.17	15	Populate Overseas Indicator (Table 15) with the value: 0 = North America World Zone 1 1 = International (01 or 011 prefix dialed)
Terminating NPA	4.3.3.18	16	Populate Terminating NPA (Table 16) as follows: —If the value is 12 digits or less, the Called Station Id as per GR-1100-CORE —per fill, procedures described in GR-1100-CORE if the Called Station Id is 13 digits or more.
Terminating Number	4.3.3.19	17	Populate Terminating Number (Table 17) as follows: — If the value is 12 digits or less, the Called Station Id as per GR-1100-CORE —per fill procedures described in GR-1100-CORE if the Called Station Id is 13 digits or more.

FIELDS OF THE STRUCTURE	REFERENCE SECTION IN GR-3058-CORE	BAF TABLE	POPULATION SUMMARY
Connect Time	4.3.3.20	18	Populate Characters 1-2 with the hour represented in the rounded value of the Customer Connect Time or Circuit Seizure Time usage element Populate Characters 3-4 with the minute represented in the rounded value of the Customer Connect Time or Circuit Seizure Time usage element Populate Characters 5-6 with the second represented in the rounded value of the Customer Connect Time or Circuit Seizure Time usage element Populate Character 7 with the tenth-of-second represented in the rounded value of the Customer Connect Time or Circuit Seizure Time usage element
Elapsed Time	4.3.3.21	19	Populate Character 1 with 0 Populate Characters 2-6 with the number of minutes of the rounded value of the customer elapsed time of the call Populate Character 7-8 with the number of seconds of the rounded value of the customer elapsed time of the call Populate Character 9 with the number of tenths-of-seconds of the rounded value of the customer elapsed time of the call
IC/INC Prefix	4.3.6.1	57	Populate Characters 1-4 with the value of the CIC that was used in the call. If there is no CIC available, then the fill procedure in GR-1100-CORE shall be implemented. Populate Character 5 with the value of: 0 if operator was involved 1 if operator was not involved
Carrier Connect Date	4.3.6.2	6	Populate Character 1 with the least significant digit of the year represented in the date the call attempt is made by the customer. Populate Characters 2-3 with the month represented in the date the call attempt is made by the customer Populate Characters 4-5 with the day represented in the date the call attempt is made by the customer

FIELDS OF THE STRUCTURE	REFERENCE SECTION IN GR-3058-CORE	BAF TABLE	POPULATION SUMMARY
Carrier Connect Time	4.3.6.3	18	Populate Characters 1-2 with the hour represented in the rounded value of the call attempt time or Circuit Seizure Time usage element Populate Characters 3-4 with the minute represented in the rounded value of the call attempt time or Circuit Seizure Time usage element Populate Characters 5-6 with the second represented in the rounded value of the call attempt time or Circuit Seizure Time usage element Populate Character 7 with the tenth-of-second represented in the rounded value of the call attempt time or Circuit Seizure Time usage element
Carrier Elapsed Time	4.3.6.4	19	Populate Character 1 with 0 Populate Characters 2-6 with the number of minutes of the rounded value of the carrier elapsed time of the call Populate Characters 7-8 with the number of seconds of the rounded value of the carrier elapsed time of the call Populate Character 9 with the number of tenths-of-seconds of the rounded value of the carrier elapsed time of the call
IC/INC Call Event Status	4.3.6.5	58	Populate as follows: — If the call has been completed, the BA shall populate BAF Table 58 with the value = 010. — If the call has been attempted, but not completed; the BA shall populate BAF Table 58 with the value = 007.
Trunk Group Number	4.3.6.6	83	Populate Character 1 with the value = 9 to indicate Signaling type not specified Populate Characters 2-5 with the value of the Trunk Group Number. If there no Trunk Group Number available, this table should use the BAF fill procedure (e.g., Hex-F).

FIELDS OF THE STRUCTURE	REFERENCE SECTION IN GR-3058-CORE	BAF TABLE	POPULATION SUMMARY
Routing Indicator	4.3.6.7	59	If the call involved the PSTN, this table shall be populated with the value -0 = if the call was direct to the PSTN -1 = if the call was Tandem. Otherwise, the BAF fill procedure should be used for this table (e.g., Hex-F).
Dialing and Presubscription Indicator	4.3.6.8	85	Used to indicate whether the calling party dialed a Carrier Access Code. The BA shall populated Table 85 with the values that best match the dialing pattern as per GR-1100-CORE.
ANI/CPN Indicator	4.3.6.9	60	Populate as per - 0 = Neither ANI nor CPN was provided in the signaling - 1 = Only ANI was provided in the signaling - 2 = Only CPN was provided in the signaling - 3 = Both ANI and CPN were provided in the signaling.

[Objective] The BA shall generate BAF Structure 0625 and populated the fields as per Table 5.3.2-58, BAF Structure 0625 and Field Populations, for the following types of calls:

- Calls that terminates into another service provider's network
- Calls that originated from another service provider's network
- Calls that utilized the PSTN
- IP calls that cannot be identified

Toll-free calls are calls that are placed to toll-free numbers (in the format that have the form 8YY-NXX-XXXX, where YY = 88, 77, 66) and they will cause the CCA to launch a query to the toll-free database for determining how to transport the call. For the purposes of these requirements, in this section, it is assumed that an IN/1 query/response format is used following the requirements found in Telcordia Technologies GR-533-CORE.

However, it is the assumption that the DISN voice network will not be providing toll-free queries using the IN/1 query/response, instead it will be sending the calls to toll-free numbers to the PSTN to determine the final routing information. Calls to toll-free numbers should generate the Structure Code 0625 as if the toll-free number was a typical normally dialed number.

5.3.2.19.2.2.1.1 Precedence Level of a Call

As identified in the previous section, one of the required items to be provided in an Automatic Message Accounting (AMA) record is the precedence level of the call. The precedence level can be identified in one of two ways: viz. 1) a specific Precedence Level Designation field in the call and 2) providing the dialed precedence level access digits in the called number field.

If the first method is used to identify the precedence level, then this information can be contained in Module Code 616.

[Objective] Module Code 616 shall be used to capture the precedence level if there is a specific Precedence Level Designation field in the call. In Module Code 043:

1. Table 569 will be populated with the value that indicates precedence level of a call in Characters 1-2, and Characters 3 will give the number of significant digits in Table 803.

2. Table 803 will be populated with either the precedence level designation or the dialed precedence level access digits.

5.3.2.19.2.2.2 VoIP/Video over IP

[Objective] In the VoIP environment, a call can be a VoIP or a Video over IP. For Video over IP calls, the BA would append Module Code 610 to the BAF Structure 0625 and populate it as per the following dependent requirements.

[Objective] Module Code 204 shall be used to indicate that the BAF record represents a Video over IP "call." As such, BAF Table 610 of Module Code 204 shall be populated with a value in Telcordia Technologies GR-1100-CORE that indicates a Video call.

For Video calls, the BA may have the option to of appending a Module Code 611 that will identify the assigned bandwidth of the Video call.

[Objective] The BA may have an option to provide an indication in the AMA record that will identify the assigned bandwidth of a Video call.

[Objective] If the call is a Video call, then the BA shall append Module Code 611 to indicate the assigned bandwidth of the Video call. The BA shall populate:

1. BAF Table 237 of Module Code 611 with a value code in Telcordia Technologies GR-1100-CORE is that indicates the assigned bandwidth values

2. BAF Table 126 of Module Code 611 with the corresponding assigned bandwidth value code

5.3.2.19.2.2.3 Customer/Business Group Identification

It may be necessary to capture the Customer/Business Group Identification information related to a call. For this, Module Code 027 should be used to capture this information.

[Objective] Module Code 027 shall be used to capture the Customer/Business Group Identification. In Module Code 027, Table 87 shall be populated according to Telcordia Technologies GR-1100-CORE.

5.3.2.19.2.2.4 BAF Structure 0588

BAF Structure 0588 is used to capture the usage information (e.g., the name of the service provided) when a service is activated, deactivated, or has an instance of use by the SA. Additional information on the generation and population rules can be found in Telcordia Technologies GR-3058-CORE.

[Objective] If a functional entity equivalent to the SA has usage information to be recorded, the BA shall generate BAF Structure 0588 according the requirements defined in Telcordia Technologies GR-3058-CORE. The population of BAF Structure 0588 shall follow the population requirements in GR-3058-CORE.

5.3.2.19.2.2.5 BAF Structure 9000

If there is a need to generate AMA records for time changes (e.g., Daylight savings), then the BA should use BAF Structure 9000.

[Objective] If there is a need to record time changes, the BA shall generate BAF Structure 9000. The population of BAF Structure 9000 shall follow the population requirements in Telcordia Technologies GR-3058-CORE.

5.3.2.19.2.3 Storage

Once the BA has generated the call records of a chosen format, it may need to retain or store those records until it is time to provide them to the downstream processing. Normally, these records are stored together as files and wait to be transported for downstream processing. The process of transporting or sending the records to downstream processing systems is left to be agreed on between the DoD and the vendors.

While in retention, additional CDRs may accumulate in this storage area. The BA must have enough storage capacity to store a reasonable quantity of CDRs. In addition, the storage device must be non-volatile, so the CDRs are protected from power disturbances and other transient conditions.

[Required] The mass storage in the BA must be non-volatile.

[Required] The mass storage in the BA must be able to retain at least five average-busy season business days of AMA data. (NOTE: This is needed to provide adequate capacity for high-volume storage of CDRs.)

5.3.2.19.2.4 Outputting Records

Once the BA has the records stored in files, there will come a time when these files will need to be outputted for downstream processing. Outputting the call records is the process of delivering those files to a processing center within the network that specializes in processing the record for billing and accounting purposes. Electronic transfer of those records would provide the most convenient method of transfer. However, electronic transfer must have security measures to prevent unauthorized access to the record during transfer. One security measure is to transfer the file over a secured protocol, such as SSHv2.

[Required] The BA should be able to electronically output the records over a secured connection. (NOTE: This is needed to allow transfer of CDRs from one location to another in a secure manner (e.g., to prevent intruder detection, theft, and/or manipulation of CDRs).)

In addition to electronic transfer, it may become necessary to transfer the records to a physical media that is also removable, such as a tape or CD. Such situations may include a third party that requires access to the records, but an electronic transfer to that third party is not an option. Thus, the following requirement should apply.

[Required] The BA should have the ability to transfer the records to a removable physical storage media that is also removable. (NOTE: This is needed to allow manual transfer of CDRs from one location to another in the case where automated electronic transfer is not available (e.g., there is an IP network outage between the CDR source and the CDR destination).)

THIS PAGE INTENTIONALLY LEFT BLANK

TABLE OF CONTENTS

SECTION **PAGE**

5.3.3 Network Infrastructure End-to-End Performance Requirements 749
5.3.3.1 End-to-End Network Infrastructure Description. 749
5.3.3.1.1 Customer Edge (CE) Segment 749
5.3.3.1.2 Network Edge Segment 750
5.3.3.1.3 DISN Service Delivery Nodes 751
5.3.3.1.4 Network Core Segment 751
5.3.3.1.5 Expanded Customer Edge Segment: COINs .752
5.3.3.2 VVoIP Characteristics 752
5.3.3.3 General Network Requirements.....753
5.3.3.3.1 Compression 754
5.3.3.3.2 VVoIP Differentiated Services Code Point ...754
5.3.3.3.3 VVoIP PHB Requirements 755
5.3.3.3.4 Traffic Conditioning Requirements 756
5.3.3.4 VVoIP Latency 758
5.3.3.4.1 VVoIP E2E Latency 758
5.3.3.4.2 VVoIP CE Latency 759
5.3.3.4.3 VVoIP Aggregation Router-to-Aggregation Router Latency.....761
5.3.3.4.4 VVoIP Customer Edge Router-to-Customer Edge Router Latency.....762
5.3.3.5 VVoIP Jitter 763
5.3.3.5.1 VVoIP End-to-End Jitter.....763
5.3.3.5.2 VVoIP Aggregation Router-to-Aggregation Router Jitter.....764
5.3.3.5.3 VVoIP CE Router-to-CE Router Jitter 765
5.3.3.5.4 VVoIP CE Jitter 766
5.3.3.6 VVoIP Packet Loss.....766
5.3.3.6.1 VVoIP E2E Packet Loss 766
5.3.3.6.2 VVoIP AR-to-AR Packet Loss 767
5.3.3.6.3 VVoIP CE Router-to-CE Router Packet Loss 768
5.3.3.6.4 VVoIP CE Packet Loss 769
5.3.3.7 Internet Protocol Version 6 (IPv6).....769
5.3.3.8 VVoIP Network Infrastructure Network Management 770
5.3.3.9 System Quality Factors.....770
5.3.3.9.1 End-to-End Availability.....770

5.3.3.10 Design and Construction.....774
5.3.3.10.1 Materials 774
5.3.3.11 Provisioning.....775
5.3.3.12 Interchangeability 777
5.3.3.13 Voice Grade of Service.....777
5.3.3.14 VVoIP Network Infrastructure Survivability 778
5.3.3.15 Voice Service Quality.....778

5.3.3 Network Infrastructure End-to-End Performance Requirements

Section 5.3.3 contains E2E performance requirements for the network infrastructure that supports the IP-based VVoIP. The focus of this section is on the network performance aspects. The requirements for the various APL-approved products that make up the network infrastructure are provided in the respective UCR 2008 sections as follows: The requirements for LAN products (LAN Core, Distribution and Access switches), including LAN design guidance are provided in UCR 2008, Section 5.3.1, requirements for the Network Infrastructure products (DISN Router, DISN Switch, and DISN Access Elements) are provided in UCR 2008, Section 5.5, Network Infrastructure Product Requirements.

This section is written for converged networks, but does not address the impact of prioritized voice on data and video services, which will be addressed in a subsequent revision of this document. The network infrastructure E2E performance requirements in this version are focused on voice applications. Subsequent versions of this section will address video and data E2E performance requirements. Finally, this section addresses a wired WAN, but does not address wireless WANs.

5.3.3.1 End-to-End Network Infrastructure Description.

The E2E network infrastructure consists of three network segments. The network segments are the CE, Network Edge, and Core Segments. Figure 5.3.3-1, GIG E2E VVoIP Network Infrastructure Segments and Measurement Reference Points, illustrates a high-level overview of the three-segment network infrastructure. The CE Segment is connected to the Core Segment by the Network Edge Segment. The description of each segment is provided in the following paragraphs.

5.3.3.1.1 Customer Edge (CE) Segment

The CE Segment may consist of LAN, a Campus Area Network (CAN), or a Metropolitan Area Network (MAN). The boundary of the CE Segment is the CE router. The Network Edge Segment connects the CE router to the AR (AR) via a DISN SDN. The CE router is owned and maintained by the B/P/C/S. The CE Segment is considered robust and the LAN/CAN/MAN characteristics include high bandwidth, diversity, and redundancy. CE Segment Quality of Service (QoS) is provided predominately by the use of robust bandwidth. Design guidance and requirements for the LAN portion of the CE Segment are provided in UCR 2008, Section 5.3.1.

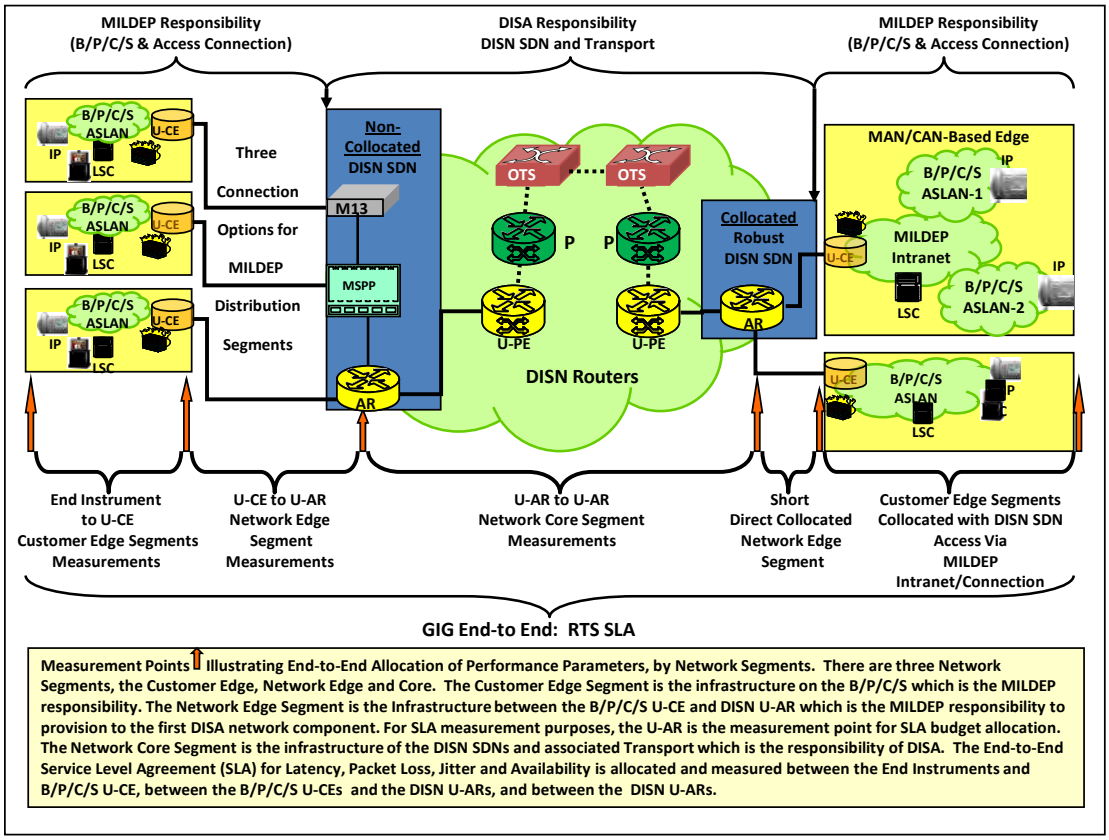


Figure 5.3.3-1. GIG E2E VVoIP Network Infrastructure Segments and Measurement Reference Points

5.3.3.1.2 Network Edge Segment

The Network Edge Segment is measured between the following two demarcation points: network side of the CE router to the access port of the AR. Depending on the specific class of DISN Service Delivery Node (SDN), the Network Edge Segment may consist of several configurations. The simplest configuration, which has an extremely low packet delay, is encountered when the CE router and AR are collocated. In this case, the Network Edge Segment is a direct, short Ethernet (i.e., 100BT or 1000BT) connection between the CE router and an AR. Figure 5.3.3-2, High-Level Illustration of End-to-End Network Segments, illustrates short-delay and longer-delay Network Edge Segment configurations.

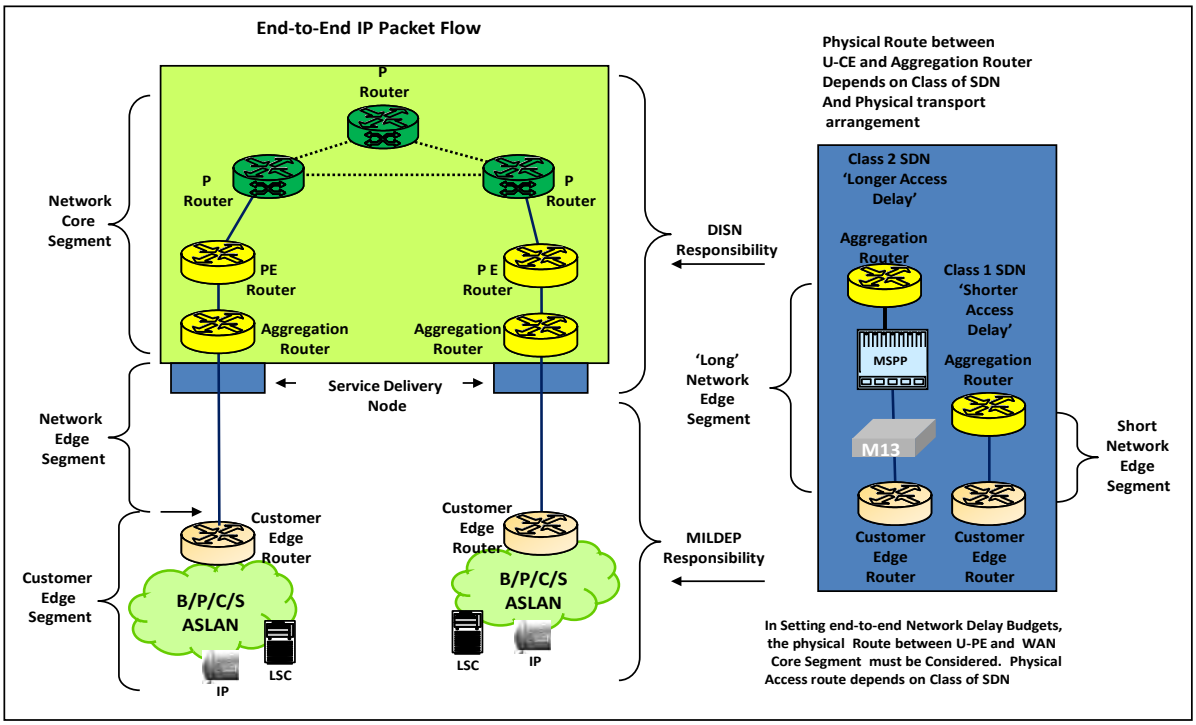


Figure 5.3.3-2. High-Level Illustration of End-to-End Network Segments

5.3.3.1.3 DISN Service Delivery Nodes

A DISN SDN is the access point where traffic to-from the CE Segment (or "customer") enters the DISN WAN via the Network Edge Segment. There are several classes of Service delivery nodes depending on whether the SDN has a M13, Multi-Service Provisioning Platform (MSPP), Provider (P), Provider Edge (PE), and/or AR. The CE Segment CE Router connects to the SDN via the Network Edge Segment using one of three connection options as shown in Figure 5.3.3-2, High-Level Illustration of End-to-End Network Segments. Each connection option will introduce different transport delays between the CE router and the AR depending on the physical connection string (data path) between the CE router and the AR. The DISA is responsible for the DISN SDN-to-SDN performance.

5.3.3.1.4 Network Core Segment

The Network Core Segment provides IP-based transport services over a high-speed network infrastructure and consists of the SDNs and the DISN Transport between the SDNs. The DISN

Transport between the SDNs typically consists of a high-speed optical transport network that starts and terminates at the PE Router. The PE Routers are connected by a series of Provider (P) Routers to form a reliable and robust IP core network. The ARs are typically subtended to the PE Router via a high-speed Ethernet connection. Figure 5.3.3-1, GIG E2E VVoIP Network Infrastructure Segments and Measurement Reference Points, shows the different network segments. Due to the different types of system deployments, the network infrastructure may be categorized according to whether it is deployed in a tactical environment or within a strategic environment. Since the performance of the network infrastructure is impacted by the type of deployment, the network infrastructure is categorized as F-F (F-F), Fixed-to-Tactical (F-T), and Tactical-to-Tactical (T-T). F-F deployments are associated with strategic-to-strategic network infrastructure connections and are provided by terrestrial transport (wireline) connections serviced by the DISN. F-T deployments are associated with tactical-to-strategic connections where the strategic point of presence is the Standardized Entry Point (STEP)/Teleport, Joint Network Node (JNN) Regional Hub, the Naval Computer and Telecommunications Area Master Station (NCTAMS) or some other Teleport. This section covers only the strategic requirements unless specifically noted otherwise. T-T deployments are associated with tactical-to-tactical connections and may or may not transit a strategic point of presence.

5.3.3.1.5 Expanded Customer Edge Segment: COINs

Figure 5.3.3-1, GIG E2E VVoIP Network Infrastructure Segments and Measurement Reference Points, addresses the use of MANs or CANs to create Communities of Interest Networks (COINs) or MILDEP Intranets. It must be noted that an entire MAN or CAN-type of arrangement falls under the CE Segment of the E2E network infrastructure. Therefore, the requirements specified for the CE Segment apply to the entire MAN/CAN arrangement.

5.3.3.2 VVoIP Characteristics

The Inelastic Real-Time aggregate service class category is composed of granular service classes that support applications sensitive to delay. The Inelastic Real-Time aggregate service class is associated with applications that require low latency (also called One-Way IP Packet Transfer Delay (IPTD)), jitter (also called IP Packet Delay Variation- IPDV), and packet loss (called One-Way IP Packet Loss Ratio (IPLR)). The traffic sources in this aggregate service class category do not have the ability to reduce their transmission rate based on feedback received from the receiving end. Typically, applications in this service class are configured to negotiate the setup of a Real Time Protocol (RTP)/User Data Protocol (UDP) session using some type of signaling (i.e., AS-SIP, H.323, H.248, etc.). When a user or end-point has been authorized to start a new session, the admission procedure should verify that the newly admitted data rates are within the engineered capacity. The following granular service classes are classified as Inelastic/Real-Time Services:

- Voice
- Circuit Emulation
- Short Messages
- Interactive Video Teleconferencing (VTC) (i.e., DVS)
- Command and Sensor Messages

5.3.3.3 General Network Requirements

The primary performance driver for voice systems (SBU and voice components of DVS) used in the DISN is the E2E voice quality. The voice quality is calculated E2E from handset to handset. For voice applications, the measurement model for the EI is the E-Model as described in the Telecommunications – IP Telephony Equipment – Voice Quality Recommendations for IP Telephony (TIA/TSB-116-A), which is based on the International Telecommunications Union – Telecommunication Standardization Sector (ITU-T) Recommendation G.107. The E-Model uses an R-Factor rating that is correlated to the MOS rating. The detailed EI voice quality calculation requirements are found in Section 5.3.2.19.2.1, Call Data.

The performance requirements specified in this section are network infrastructure related and include routers, asynchronous transfer mode (ATM) switches, MSPP and optical interfaces to ensure that the handset-to-handset requirements are achievable. The following assumptions were used in determining the performance requirements necessary to achieve acceptable service:

- IP version 4

- Wireline Strategic Network (A=0)

- G.711 CODEC with 20 ms samples (Ie=0)

- Bearer packet size = 242 bytes
  - Calculated for SRTP encrypted bearer packets
  - Includes SRTP Tag, and Ethernet Interframe Gap

- Weighted Terminal Coupling Loss (TCLw) = 52 dB (in accordance with American National Standards Institute (ANSI)/Telecommunications Industries/Industry Association (TIA)-810-B

- Latency due to EI (voice to IP and IP to voice) is 50 ms
  - Latency due to de-jitter buffer in EI is 20 ms
  - Includes Packet loss Concealment delays

5.3.3.3.1 Compression

[Conditional] If the system supporting VVoIP uses compression, the compression approach shall be reversible.

NOTE: The preferred codec used for E2E F-F voice sessions is a G.711 Pulse-Code Modulation (PCM) (Uncompressed) with 20 ms samples. Other CODECs are allowed and a minimum list of CODECs that must be supported by all EIs is found in Section 5.3.2, EI requirements.

5.3.3.3.2 VVoIP Differentiated Services Code Point

[Required] The system shall support the plain text DSCP plan as shown in Table 5.3.3-1.

Table 5.3.3-1. VVoIP DSCP Assignments

AGGREGATED SERVICE CLASS	GRANULAR SERVICE CLASS	PRIORITY/ PRECEDENCE	DSCP BASE10	DSCP BINARY	DSCP BASE8
Network Control	Network Signaling (OSPF, BGP, etc.)		48	110 000	60
Inelastic Real-Time	User Signaling (AS-SIP, H.323, etc.)		40	101 000	50
	Voice (Includes SRTCP)	FO	41	101 001	51
		F	42	101 010	52
		I	43	101 011	53
		P	45	101 101	55
		R	46	101 110	56
	Interactive VTC includes all sessions associated with VTC (voice, video, and data)	FO	33	100 001	41
		F	34	100 010	42
		I	35	100 011	43
		P	37	100 101	45
		R	38	100 110	46
Preferred Elastic	Multimedia Streaming	FO	25	011 001	31
		F	27	011 011	33
		I	29	011 101	35
		P	31	011 111	37
		R	26	011 010	32
	Low-Latency Data (OA&M (SNMP, Telnet, SSHv2, etc.))		18	010 010	22
	High Throughput Data (OA&M (Syslog Files, CDRs, etc.))		16	010 000	20

AGGREGATED SERVICE CLASS	GRANULAR SERVICE CLASS	PRIORITY/ PRECEDENCE	DSCP BASE10	DSCP BINARY	DSCP BASE8
Elastic	Best Effort		0	000 000	0

LEGEND:
AS-SIP Assured Services Session Initiation Protocol
BGP Border Gateway Protocol
CDR Call Detail Recording
DSCP Differentiated Services Code Point
F Flash
FO Flash Override
I Intermediate
OA&M Operations, Administration, and Maintenance
OSPF Open Shortest Path First
P Priority
R Routine
SNMP Simple Network Management Protocol
SSHv2 Secure Shell Version 2

5.3.3.3.3 VVoIP PHB Requirements

[Required] The system routers supporting VVoIP shall support the 4-queue PHBs as defined in Table 5.3.3-2.

NOTE: The 8-queue model is preferred, but may not be feasible in FY2008.

NOTE: This assumes that AR and CE router PHB coordination occurs to prevent asymmetrical performance since the routers may be different on the ends of the connection. The LSC session budget must be less than or equal to the equivalent CE router bandwidth budget. The CE router bandwidth budget per queue must be less than or equal to the AR bandwidth budget per queue. For example, if the LSC session budget is ten voice sessions, then the CE router bandwidth budget for the EF queue must be greater than or equal to 1,100 kbps (10 * 110 kbps). In this scenario if the CE router bandwidth budget was 1400 kbps to account for expected growth, surge or other EF traffic, then the AR bandwidth must be greater than or equal to the CE router bandwidth budget.

NOTE: For AF and EF PHBs refer to UCR 2008, Section 5.3.2.14.3, Per Hop Behavior Support.

Table 5.3.3-2. 4-Queue PHB Approach

AGGREGATED SERVICE CLASS	GRANULAR SERVICE CLASS	PRIORITY/ PRECEDENCE	DSCP BASE10	QUEUE	PHB
Control	Network Signaling (OSPF, IS-IS, etc.)		48	3	EF
Inelastic Real-Time	User Signaling		40		
	Voice (Includes SRTCP)	FO	41		
		F	42		
		I	43		
		P	45		
		R	46		

AGGREGATED SERVICE CLASS	GRANULAR SERVICE CLASS	PRIORITY/ PRECEDENCE	DSCP BASE10	QUEUE	PHB
	Interactive VTC	FO	33	2	AF41
		F	34		
		I	35		
		P	37		
		R	38		
Preferred Elastic	Multimedia Streaming	FO	25		AF42
		F	27		
		I	29		
		P	31		
		R	26		
	Low-Latency Data	FO	17	1	AF31
		F	19		
		I	21		
		P	23		
		R	18		
	High Throughput Data	FO	9		AF32
		F	11		
		I	13		
		P	15		
		R	10		
	OA&M	R	16		
Elastic	Default		0	0	Default

[Conditional] The system routers supporting VVoIP shall support the 8-queue PHBs as defined in Table 5.3.3-3, 8-Queue PHB Approach.

NOTE: This assumes that AR and CE router PHB coordination occurs to prevent asymmetrical performance since the routers may be different on the ends of the connection. The LSC call budget must be equal to the equivalent CE router bandwidth budget. The CE router bandwidth budget per queue must equal to the AR bandwidth budget per queue. For example, if the LSC call budget is ten calls then the CE router bandwidth budget for the EF queue must be equal to 1,100 kbps (10 * 110 kbps). In this scenario if the CE router bandwidth budget was 1400 kbps to account for expected growth, surge or other EF traffic, then the AR bandwidth must be equal to the CE router bandwidth budget.

5.3.3.3.4 Traffic Conditioning Requirements

[Required] All CE router and/or AR interfaces toward the CE router shall support traffic conditioning on an aggregate granular service class basis on the input interface.

[Required] The system routers shall be able to traffic condition using IP addresses, virtual LAN (VLAN) tags, protocol port numbers, and DSCPs as discriminators, as a minimum.

Table 5.3.3-3. 8-Queue PHB Approach

AGGREGATED SERVICE CLASS	GRANULAR SERVICE CLASS	PRIORITY/ PRECEDENCE	DSCP BASE10	QUEUE	CE ROUTER PHB
Control	Network Signaling		48	3	EF
Inelastic Real-Time	User Signaling		40		
	Voice (Includes SRTCP)	FO	41	7	
		F	42		
		I	43		
		P	45		
		R	46		
	Interactive VTC	FO	33	6	AF41
		F	34		
		I	35		
		P	37		
		R	38		
Preferred Elastic	Multimedia Streaming	FO	25	5	AF31
		F	27		
		I	29		
		P	31		
		R	26		AF32
	Low-Latency Data	FO	17	4	AF21
		F	19		
		I	21		
		P	23		
	OA&M	R	18		AF22
	High Throughput Data	FO	9	2	AF11
		F	11		
		I	13		
		P	15		
	OA&M	R	10		AF12
Elastic	Default		0	0	Default

LEGEND:
AF Assured Forwarding
CE Customer Edge (route)r
DSCP Differentiated Services Code Point
EF Expedited Forwarding
F Flash
FO Flash Override
IS-IS Intermediate System-Intermediate System
I Intermediate
OA&M Operations, Administration, and Maintenance
P Priority
PHB Per Hop Behavior
R Routine
VTC Video Teleconferencing

NOTE: The definition of traffic engineering is found in UCR 2008, Section A1, Definitions, Abbreviations and Acronyms, and References.

[Required] All CE routers and/or AR interfaces toward the CE router shall support traffic conditioning on a granular service class basis on the output interface.

5.3.3.4 VVoIP Latency

Latency is defined in UCR 2008, Appendix A, Section A2, Glossary and Terminology Description and the term is used interchangeably with the term Internet Protocol Packet Transfer Delay (IPTD). For the purposes of this UCR, the one-way latency metric is reported as the arithmetic mean of several (specified) single measurements over a 5-minute period. Errored packets and lost packets are excluded from the calculation. The metric is reported to 1ms accuracy, rounded up, with a minimum value of 1 ms.

[Required] All routers shall have a latency of 2 ms or less (≤) as measured from the input interface to output interface under congested (as described in the UCR 2008, Section 5.3.1, ASLAN) conditions.

5.3.3.4.1 VVoIP E2E Latency

[Required] The E2E System supporting VVoIP shall ensure that the one-way E2E latency (handset to handset) for F-F locations is 220 ms or less (≤) for VVoIP sessions between theaters (intertheater) as averaged over any 5-minute period. Figure 5.3.3-3, Fixed-to-Fixed End-to-End Latency, illustrates the measurement points for calculating the F-F E2E latency.

NOTE: Due to the large number of satellite connections to South West Asia (SWA) the latency SLAs may not be met to that theater. The requirement for 220 ms is due to the limits of talk over. This latency may not be feasible for all scenarios, but the requirement as stated is necessary to avoid talk over for the scenarios that are feasible.

[Required] The E2E System supporting VVoIP shall ensure that the one-way E2E latency (handset to handset) for F-F locations is 150 ms or less (≤) for VVoIP sessions within a theater (intratheater) as averaged over any 5-minute threshold period. Figure 5.3.3-3, Fixed-to-Fixed E2E Latency, illustrates the measurement points for calculating the F-F E2E latency.

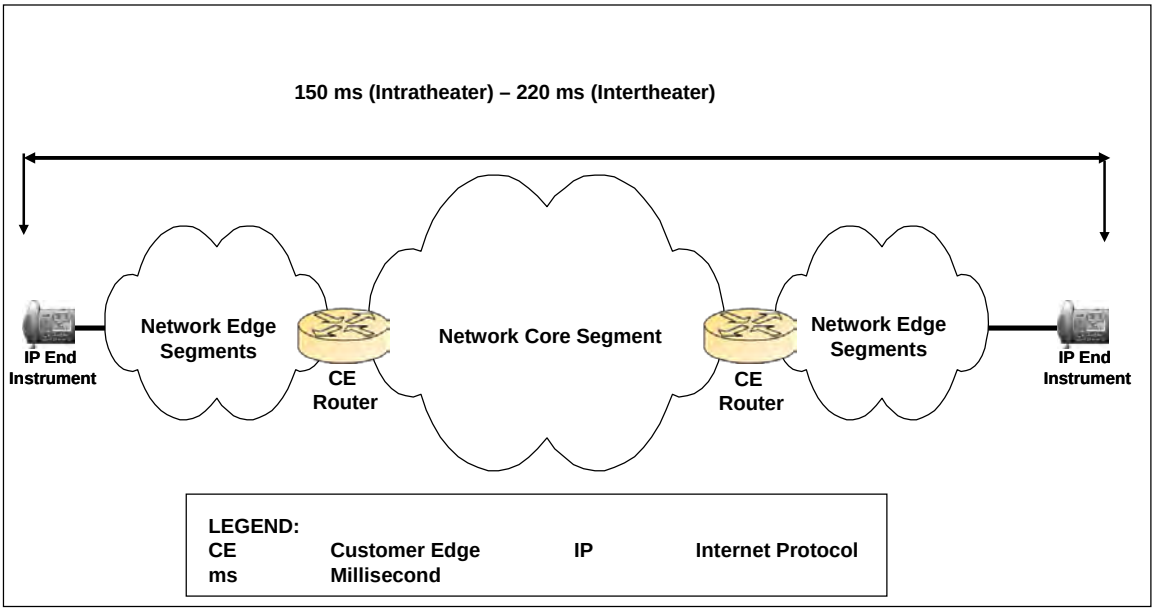


Figure 5.3.3-3. Fixed-to-Fixed End-to-End Latency

5.3.3.4.2 VVoIP CE Latency

[Required] The CE System supporting VVoIP shall ensure that the one-way latency from the IP handset to the CE router within the CE Segment is less than or equal to (≤) 35 ms (≤ 44 ms if the CE router is collocated with a AR) for VVoIP sessions as averaged over any 5-minute period. Figure 5.3.3-4, CE Segment Outbound Latency, illustrates the delays associated with calculating the CE Segment outbound latency. The measurements shall include the latency associated with the CE router switching.

[Required] The CE System supporting VVoIP shall ensure that the one-way latency from the CE router to the IP handset within the CE Segment is (≤) 35 ms (≤ 44 ms if the CE router is collocated with an AR) for VVoIP sessions as averaged over any 5-minute or period. Figure 5.3.3-5, CE Segment Inbound Latency, illustrates the delays associated with calculating the CE Segment inbound latency. The measurements shall include the latency associated with the CE router switching.

NOTE: This assumes the latency associated with the de-jitter buffer is 20 ms.

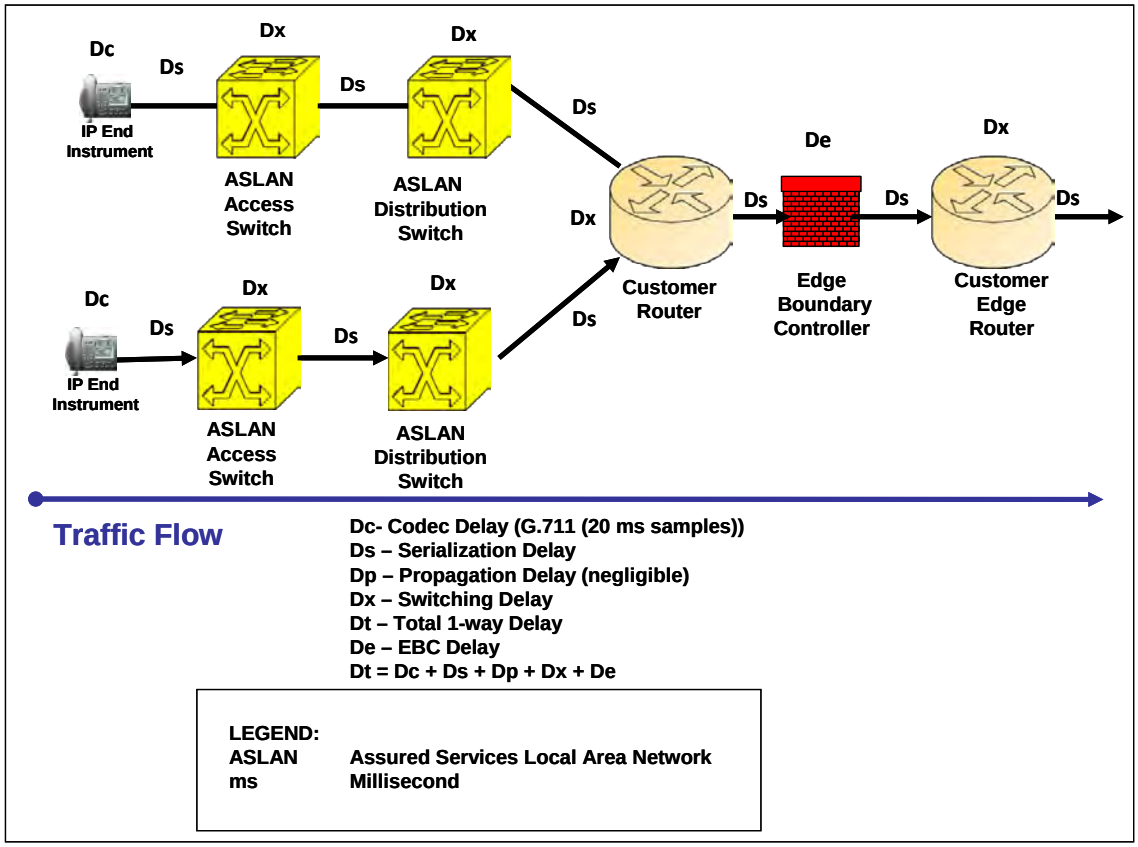


Figure 5.3.3-4. Customer Edge Segment Outbound Latency

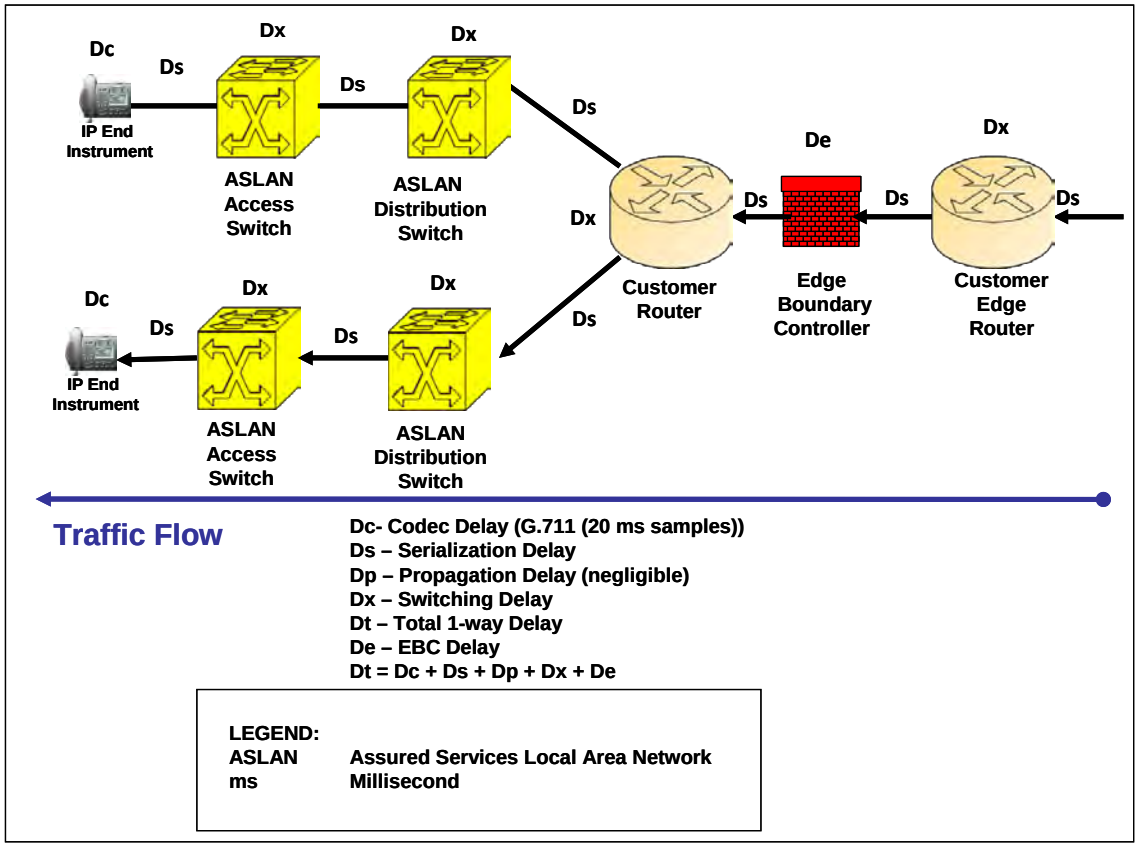


Figure 5.3.3-5. CE Segment Inbound Latency

5.3.3.4.3 VVoIP Aggregation Router-to-Aggregation Router Latency

[Required] The Network Infrastructure supporting VVoIP shall ensure that the one-way latency from the AR to AR across the DISN WAN for F-F nodes is 130 ms or less (≤) for VVoIP sessions between theaters (intertheater) as averaged over any 5-minute period. Figure 5.3.3-6, F-F AR-to-AR Latency, illustrates the measurement points for calculating the F-F AR-to-AR latency. The measurements shall occur at the AR output ports to the CE router to incorporate the switching delays through the AR.

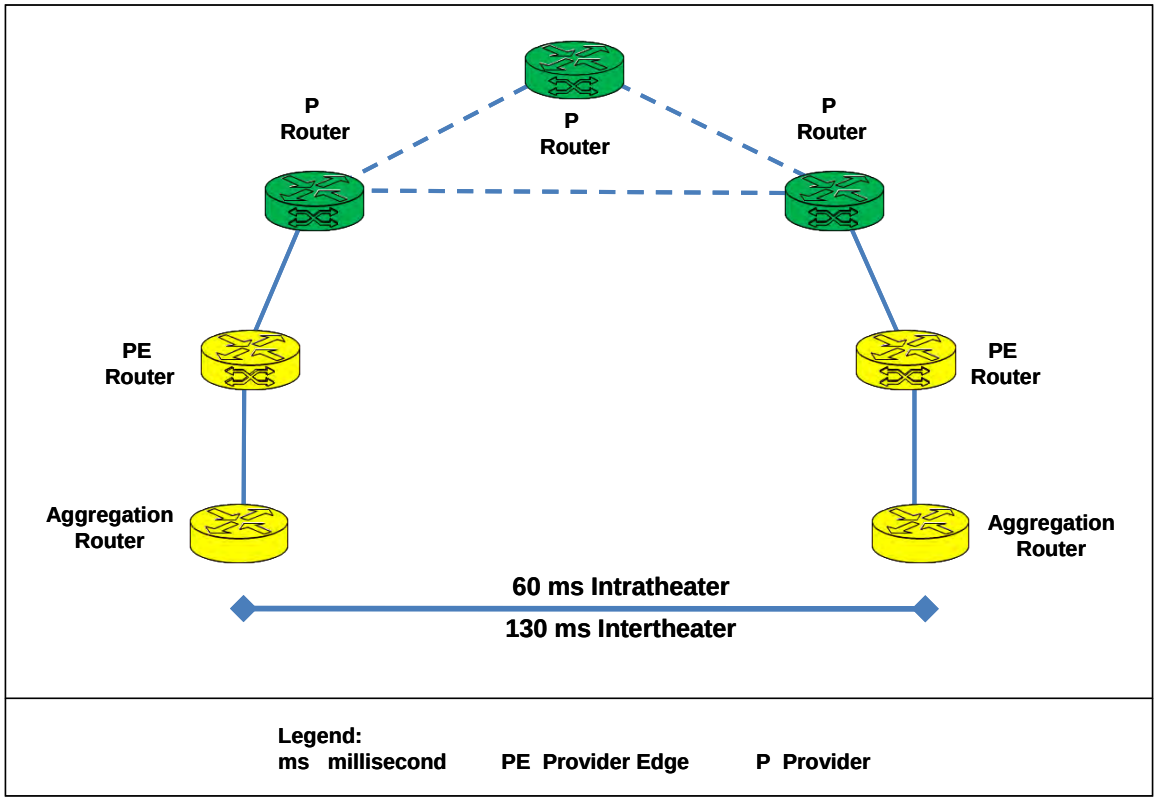


Figure 5.3.3-6. Fixed-to-Fixed Aggregation Router-to-Aggregation Router Latency

[Required] The DISN SDN and Transport System supporting VVoIP shall ensure that the one-way latency from the AR to AR across the DISN for F-F nodes is 60 ms or less (≤) for VVoIP sessions within a theater (intratheater) as averaged over any 5-minute period. Figure 5.3.3-6 illustrates the measurement points for calculating the F-F AR to AR latency. The measurements shall occur at the AR output ports to the CE router to incorporate the switching delays through the AR.

5.3.3.4.4 VVoIP Customer Edge Router-to-Customer Edge Router Latency

[Required] The DISN Network Infrastructure System supporting VVoIP shall ensure that the one-way latency from the CE router to CE router across the DISN Network Infrastructure for F-F nodes is 150 ms or less (≤) (132 ms or less (≤) if the CE router is collocated with a AR) for VVoIP sessions between theaters (intertheater) as averaged over any 5-minute period. Figure 5.3.3-7, Fixed-to-Fixed CE Router -to-CE Router Latency, illustrates the measurement points for calculating the F-F CE router to CE router latency. The measurements shall occur at the router output ports to the ARs because the CE Segment incorporates the switching delay through the CE router.

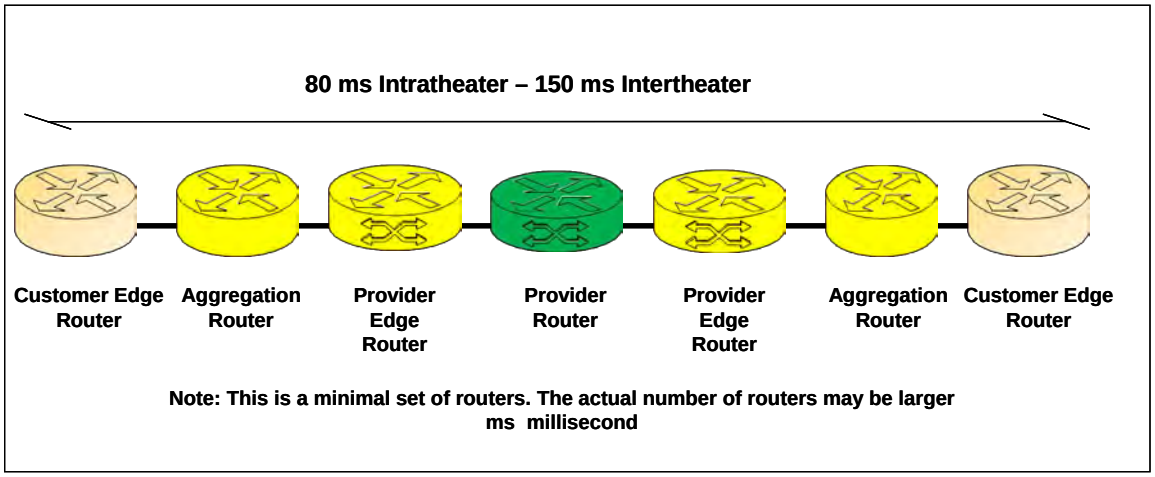


Figure 5.3.3-7. Fixed-to-Fixed CE Router-to-CE Router Latency

[Required] The Network Infrastructure System supporting VVoIP shall ensure that the one-way latency from the CE router to CE router across the DISN for F-F nodes is 80 ms or less (≤) (62 ms or less (≤) if the CE router is collocated with a AR) for VVoIP sessions within a theater (intratheater) as averaged over any 5-minute period. Figure 5.3.3-7 illustrates the measurement points for calculating the F-F CE router to CE router latency. The measurements shall occur at the router output ports to the SDN because the CE Segment incorporates the switching delay through the CE router.

5.3.3.5 VVoIP Jitter

Jitter is defined in Appendix A, Section A2, Glossary and Terminology Description and the term is used interchangeably with the term Internet Protocol Packet Delay Variation (IPDV). The jitter numbers specified in this section are based on the minimum latency jitter model defined in ITU-T Y.1540, November 2007. The one-way jitter is defined as the 99th percentile measurement of the distribution of singleton jitter (n) measurements over a 5-minute measurement interval.

5.3.3.5.1 VVoIP End-to-End Jitter

[Required] The E2E System supporting VVoIP shall ensure that the E2E jitter (handset to handset) for F-F locations is 20 ms or less (≤) for VVoIP sessions between theaters (intertheater) during any 5-minute period. Figure 5.3.3-8, E2E Fixed-to-Fixed Jitter, illustrates the measurement points for calculating the F-F E2E network jitter.

NOTE: Dynamic de-jitter buffers are allowed, but for the purpose of these performance measurements are assumed to be 20 ms.

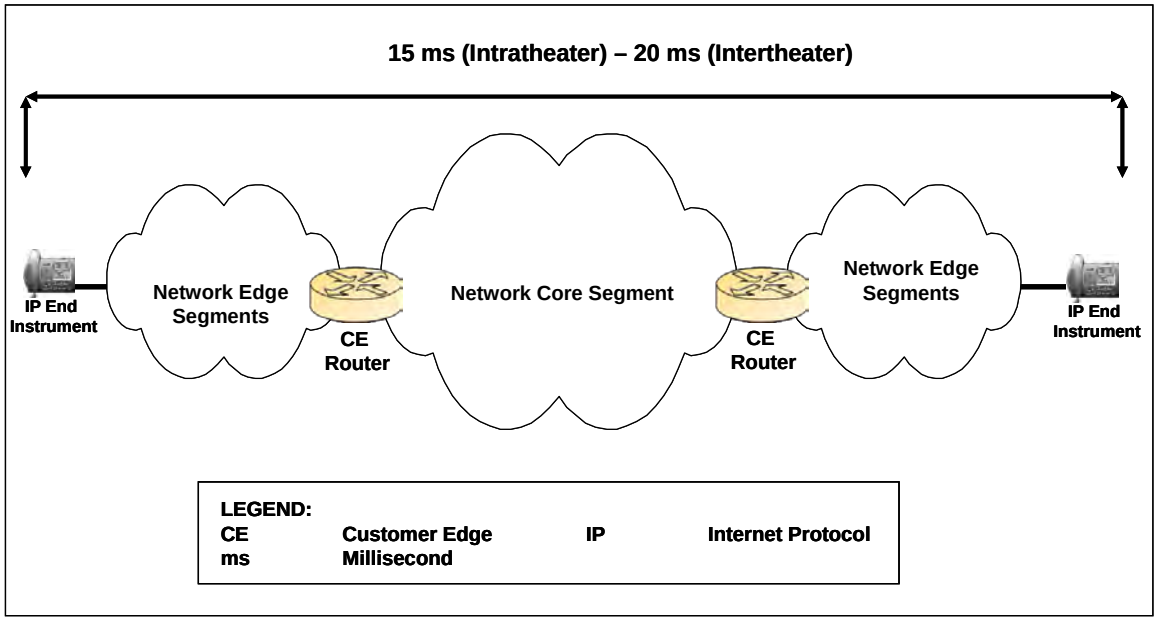


Figure 5.3.3-8. End-to-End Fixed-to-Fixed Jitter

[Required] The E2E System supporting VVoIP shall ensure that the E2E jitter (handset to handset) for F-F locations is 15 ms or less for VVoIP sessions within a theater (intratheater) during any 5-minute period. Figure 5.3.3-8 illustrates the measurement points for calculating the F-F E2E jitter.

NOTE: Dynamic de-jitter buffers are allowed, but for the purpose of these performance measurements are assumed to be 20 ms.

5.3.3.5.2 VVoIP Aggregation Router-to-Aggregation Router Jitter

[Required] The Network Infrastructure from AR-to-AR supporting VVoIP shall ensure that the jitter for F-F nodes is 10 ms or less (≤) for VVoIP sessions between theaters (intertheater) during any 5-minute period. Figure 5.3.3-9, Fixed-to-Fixed AR-to-AR Jitter, illustrates the measurement points for calculating the F-F AR-to-AR jitter. The measurements shall occur at the AR output ports to the CE router to incorporate the jitter through the AR.

[Required] The Network Infrastructure from AR-to-AR supporting VVoIP shall ensure that the jitter for F-F nodes is 5 ms or less (≤) for VVoIP sessions within a theater (intratheater) during any 5-minute period. Figure 5.3.3-9 illustrates the measurement points for calculating the F-F AR-to-AR jitter. The measurements shall occur at the AR output ports to the CE router to incorporate the jitter through the AR.

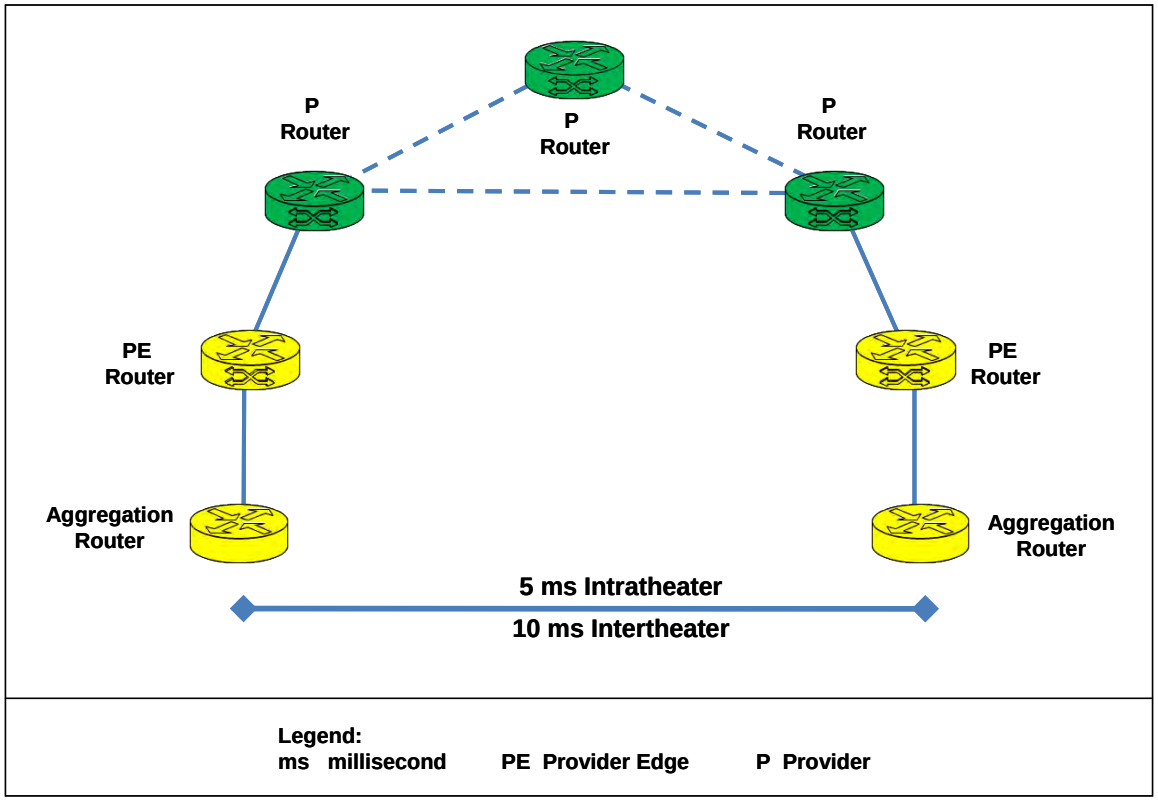


Figure 5.3.3-9. Fixed-to-Fixed AR-to-AR Jitter

5.3.3.5.3 VVoIP CE Router-to-CE Router Jitter

[Required] The DISN Network Infrastructure System supporting VVoIP shall ensure that the one-way jitter from the CE router to CE router across the DISN Network Infrastructure for F-F nodes is 14 ms or less (≤) (10 ms or less (≤) if the CE router is collocated with the AR) for VVoIP sessions between theaters (Intertheater) during any 5-minute period. Figure 5.3.3-10, Fixed-to-Fixed CE Router-to-CE Router Network Infrastructure jitter, illustrates the measurement points for calculating the F-F CE Router-to-CE Router Network Infrastructure jitter. The measurements shall occur at the router output ports to the ARs because the CE Segment incorporates the jitter through the CE Router.

[Required] The DISN Network Infrastructure System supporting VVoIP shall ensure that the one-way jitter from the CE router to CE router across the DISN Network Infrastructure for F-F nodes is 9 ms or less (≤) (5 ms or less (≤) if the CE router is collocated with an AR) for VVoIP sessions within a theater (intratheater) during any 5-minute period. Figure 5.3.3-10 illustrates the measurement points for calculating the F-F CE router-to-CE router Network Infrastructure jitter. The measurements shall occur at the router output ports to the ARs because the CE Segment incorporates the jitter through the CE router.

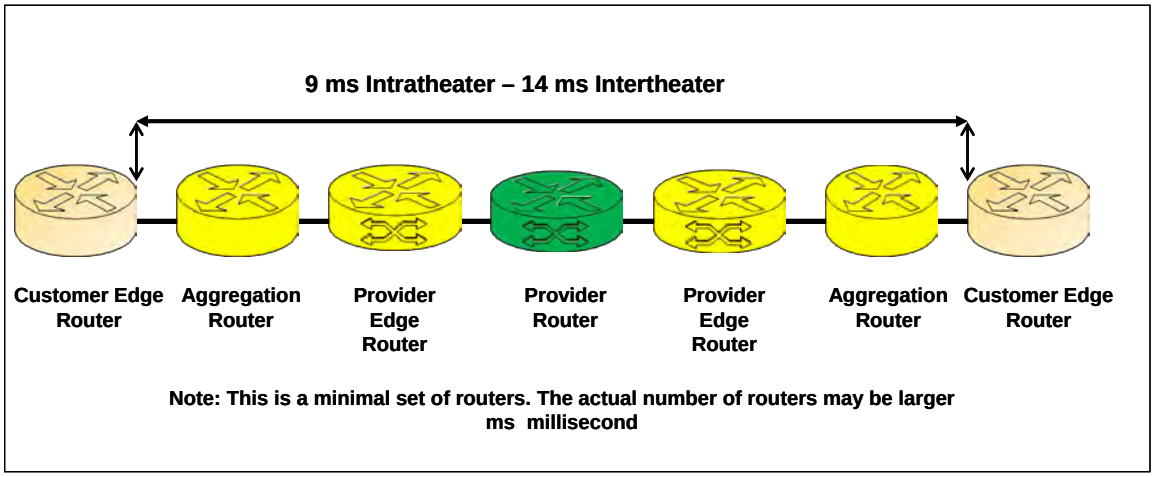


Figure 5.3.3-10. Fixed-to-Fixed CE Router-to-CE Router Network Infrastructure Jitter

5.3.3.5.4 VVoIP CE Jitter

[Required] The CE System supporting VVoIP shall ensure that the one-way jitter between the handset and CE router within the Edge Segment is 3 ms or less (≤) (5 ms or less (≤) if the CE router R is collocated with a AR) for VVoIP sessions during any 5-minute period.

5.3.3.6 VVoIP Packet Loss

Packet loss is defined in Appendix A, Section A2, Glossary and Terminology Description, and the term is used interchangeably with the term Internet Protocol Packet loss Ratio (IPLR). A single instance of packet loss measurement is defined as a record of the packet sent by the sender reference point at the destination reference point. The record is 0 if the packet was received or 1 if the packet was not received. A packet is deemed to be lost if it's one way latency exceeds an time Tmax, where Tmax is equal to 3 seconds.

5.3.3.6.1 VVoIP E2E Packet Loss

[Required] The E2E System supporting VVoIP shall ensure that the E2E IP packet loss (handset to handset) for F-F locations is 1.0 percent (%) or less (≤) for VVoIP sessions as averaged over any 5-minute period. Figure 5.3.3-11, E2E Fixed-to-Fixed Packet Loss, illustrates the measurement points for calculating the F-F E2E packet loss.

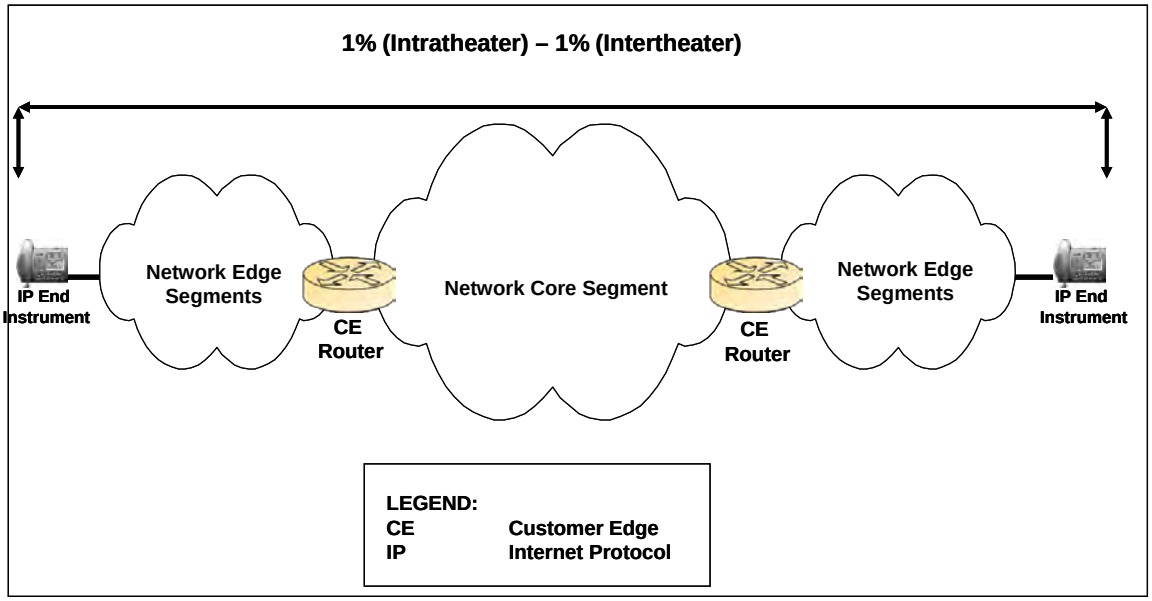


Figure 5.3.3-11. End-to-End Fixed-to-Fixed Packet Loss

[Required] To ensure the above requirement is met, the E2E System supporting VVoIP shall be designed and engineered for a one-way E2E packet loss for F-F locations of 0 percent (%) for VVoIP sessions as averaged over any 5-minute period.

5.3.3.6.2 VVoIP AR-to-AR Packet Loss

[Required] The Network Infrastructure from AR-to-AR supporting VVoIP shall ensure that the packet loss for F-F nodes is 0.3 percent (%) or less (≤) for VVoIP sessions between theaters (intertheater) as averaged over any 5-minute period. Figure 5.3.3-12, Fixed-to-Fixed AR-to-AR Packet Loss, illustrates the measurement points for calculating the F-F AR-to-AR packet loss. The measurements shall occur at the AR output ports to the CE router to incorporate the packet loss through the AR.

[Required] The Network Infrastructure from AR-to-AR supporting VVoIP shall ensure that the packet loss for F-F nodes is 0.01 percent (%) or less (≤) for VVoIP sessions within a theater (intratheater) as averaged over any 5-minute period. Figure 5.3.3-12, Fixed-to-Fixed AR-to-AR Packet Loss, illustrates the measurement points for calculating the F-F AR-to-AR packet loss. The measurements shall occur at the AR output ports to the CE router to incorporate the packet loss through the AR.

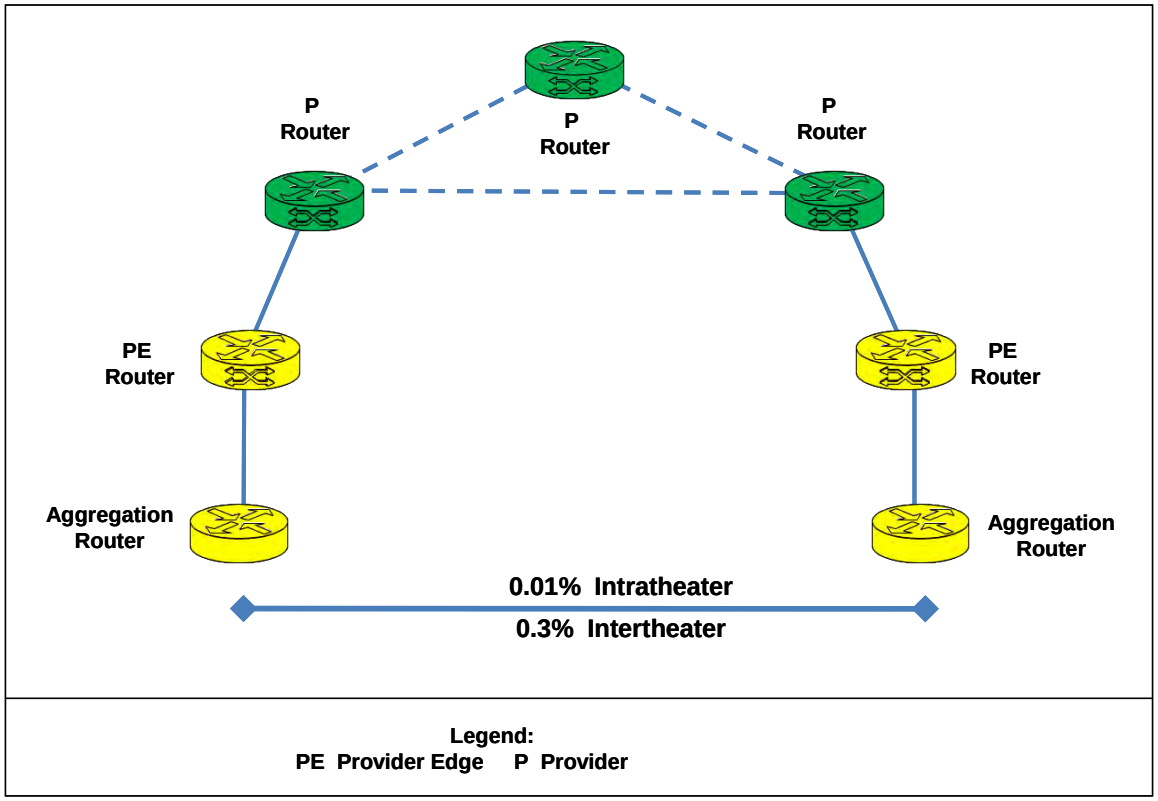


Figure 5.3.3-12. Fixed-to-Fixed AR-to-AR Packet Loss

5.3.3.6.3 VVoIP CE Router-to-CE Router Packet Loss

[Required] The DISN Network Infrastructure System supporting VVoIP shall ensure that the one-way packet loss from the CE router to CE router across the DISN Network Infrastructure for F-F nodes is 0.8 percent (%) or less (≤) (0.3 % or less (≤) if the CE routers are collocated with the ARs) for VVoIP sessions between theaters (intertheater) as averaged over any 5-minute period. Figure 5.3.3-13, Fixed-to-Fixed CE router-to-CE router Network Infrastructure Packet Loss, illustrates the measurement points for calculating the F-F CE router-to-CE router packet loss. The measurements shall occur at the router output ports to the ARs because the CE Segment incorporates the packet loss through the CE router.

NOTE: This assumes the packet loss between a collocated CE router and AR is 0.01 percent (%) or less (≤).

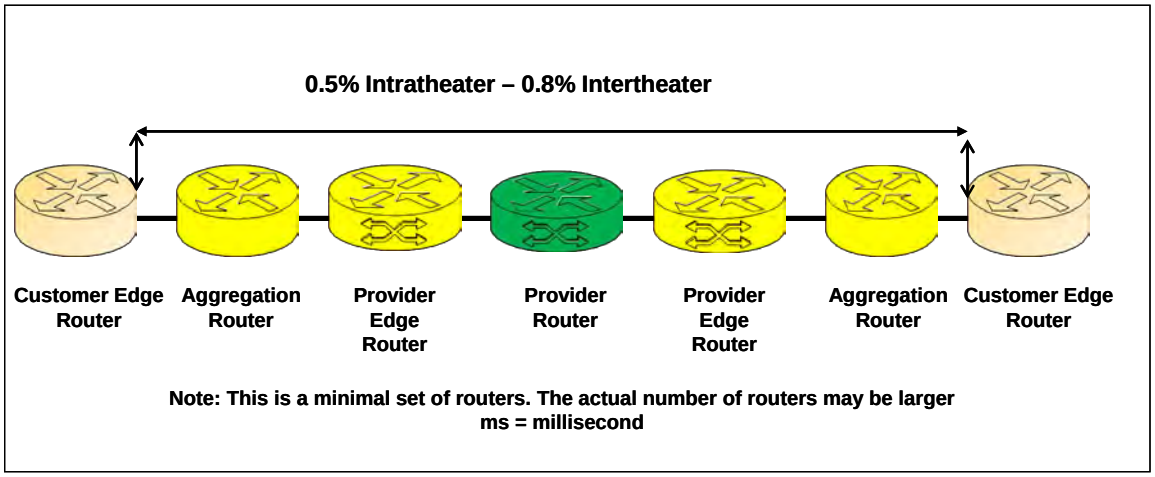


Figure 5.3.3-13. Fixed-to-Fixed Customer Edge Router-to-Customer Edge Router Network Infrastructure Packet Loss

[Required] The DISN Network Infrastructure System supporting VVoIP shall ensure that the one-way packet loss from the CE router to CE router across the DISN Network Infrastructure for F-F nodes is 0.5 percent (%) or less (≤) (0.03 percent (%) or less (≤) if the CE routers are collocated with the ARs) for VVoIP sessions within a theater (intratheater) as averaged over any five minute period. Figure 5.3.3-13, Fixed-to-Fixed CE router-to-CE router Network Infrastructure Packet Loss, illustrates the measurement points for calculating the F-F CE router-to-CE router packet loss. The measurements shall occur at the router output ports to the ARs because the CE Segment incorporates the packet loss through the CE router.

5.3.3.6.4 VVoIP CE Packet Loss

[Required] The CE System supporting VVoIP shall ensure that the one-way packet loss between the handset and CE router is 0.05 percent (%) or less (≤) for VVoIP sessions as averaged over any 5 minute period.

5.3.3.7 Internet Protocol Version 6 (IPv6)

[Required] The network infrastructure systems supporting VVoIP shall accept, route, and process IP Version 6 (IPv6) protocol traffic while providing parity to IP Version 4 (IPv4).

NOTE: The goal of this requirement is to permit applications and data owners to complete operational transition to IPv6 with at least the same functionality as currently found in IPv4.

NOTE: The IPv6 requirements are found in UCR 2008 Section, 5.3.5, IPv6 Requirements. It is assumed that:

1. The serialization and switching delay increases associated with larger IPv6 packets in comparison to IPv4 packets is insignificant.

2. The latency calculations are the same for IPv4 and IPv6 implementations.

3. Any improvements in the router processing speed due to the simplified IPv6 header will be ignored.

5.3.3.8 VVoIP Network Infrastructure Network Management

The VVoIP Network Infrastructure network management requirements for the TDM-based system are found in UCR 2008, Section 5.3.2, Assured Services Requirements; NM requirements for the IP-based system are found in UCR 2008, Section 5.3.2.17, Management of Network Appliances.

5.3.3.9 System Quality Factors

5.3.3.9.1 End-to-End Availability

The definition of availability that is found in the Telcordia Technologies Generic Requirements GR-512-CORE, *LSSGR: Reliability*, Section 12, is the basis for the E2E VVoIP network reliability. The following paragraphs outline the availability requirements for the VVoIP network.

[Required] The E2E Network Infrastructure availability when supporting C2 VVoIP between F-F locations shall be 99.95 percent (%) or greater (≥) to include scheduled maintenance.

Figure 5.3.3-14, Fixed-to-Fixed Network Infrastructure Availability illustrates the measurement points for calculating the F-F network availability.

[Required] The availability for the Network Infrastructure supporting C2 VVoIP within the F-F from AR-to-AR shall be 99.998 percent (%) or greater (≥) to include scheduled maintenance.

[Required] The availability for the Network Infrastructure supporting C2 VVoIP within the F-F from CE router-to-CE router shall be 99.96 percent (%) or greater (≥) to include scheduled maintenance.

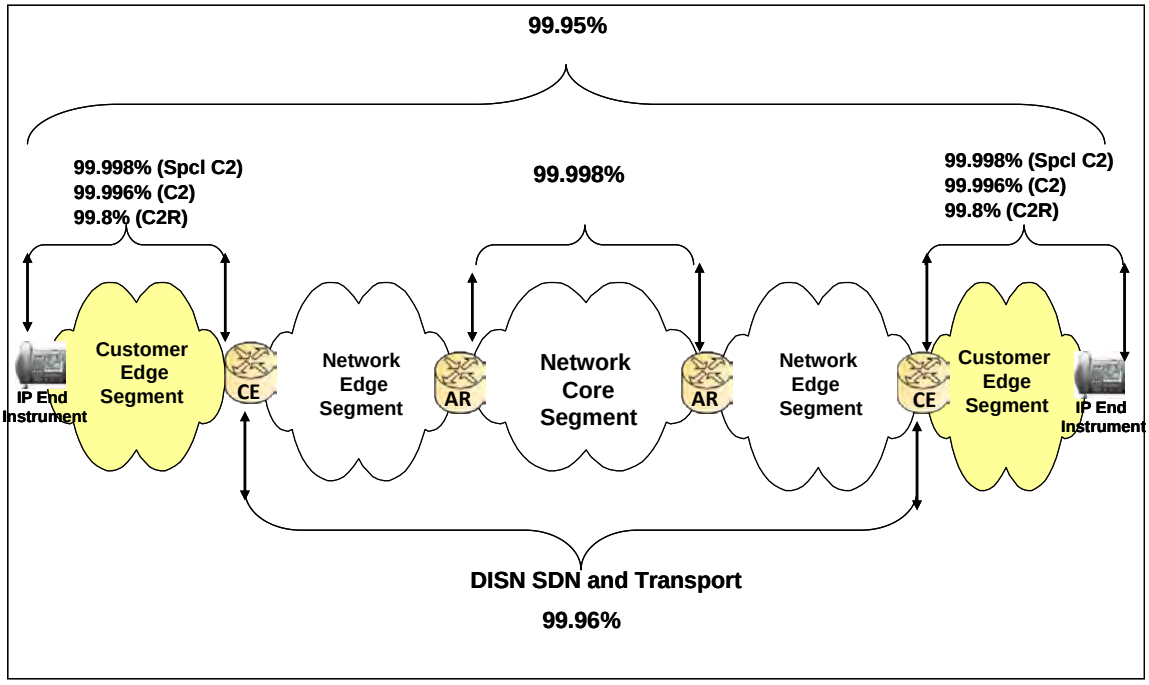


Figure 5.3.3-14. Fixed-to-Fixed Network Infrastructure Availability

[Required] The availability to include scheduled maintenance for the Network Infrastructure supporting C2 VVoIP within an Edge Segment between the handset and the CER shall be 99.998 percent (%) or greater (≥) for Special C2 users, 99.996 percent (%) or greater (>) for C2 users, and 99.8 percent (%) or greater (>) for C2(R) users. C2(R) users are defined in UCR 2008, section 4.2.1, User Categories.

[Required] The E2E Network Infrastructure supporting C2 VVoIP shall have no single point of failure to include power sources and network management.

[Required] E2E Network Infrastructure Products supporting C2 VVoIP shall support a protocol that allows for dynamic rerouting of IP packets to eliminate any single points of failure in the network.

[Required] All Network Infrastructure Products supporting C2 VVoIP shall have 8 hours of backup power.

NOTE: This requirement does not address ASLAN backup power requirements, which are addressed in Section 5.3.1, ASLAN Infrastructure Product Requirements.

[Required] The National Military Command Center (and Alternate), Combatant Commanders, or Component headquarters shall not be isolated longer than 30 minutes because of an outage in the Core Segment of the network.

[Required] In the event of an E2E Network Infrastructure component failure in a network supporting C2 VVoIP, all sessions that are active shall not be disrupted (loss of existing connection requiring redialing) and a path through the network shall be restored within 5 seconds.

[Required] All Network Infrastructure Products supporting C2 VVoIP used to meet the reliability requirements shall be capable of handling the entire session processing load in the event that its counterpart Product fails.

[Required] All Network Infrastructure Products supporting VVoIP that implement Multiprotocol Label Switching (MPLS) shall have a Fast ReRoute (FRR) capability that restores paths around a local failure (i.e., a failure involving a single router or circuit) within 50 ms.

Dual homing is physically or logically diverse in accordance with the DISN subscription rates.

[Required] The E2E Network Infrastructure availability for the E2E system supporting C2 VVoIP between F-F locations shall be 99.95 percent (%) or greater (≥) to include scheduled maintenance.

NOTE: The availability calculations will be based on best practices because there appears to be no standardized model for calculating IP network availability.

[Conditional] If the Edge Segment supports C2 users, then the system shall have two separate access connections, and shall be provisioned on physically diverse paths via two different ARs.

[Conditional] If the Edge Segment has at least two separate access connections and supports C2 users, then each connection will be traffic engineered to support 100 percent (%), which includes the 25 percent (%) surge requirement of the VVoIP traffic load.

[Required] If the Edge Segment has at least two separate access connections, then the VVoIP traffic shall only use one access connection at a time to prevent asymmetric routing.
NOTE: Data traffic may use the alternate connection.

[Conditional] If the Edge Segment supports C2 users and the CE router is collocated with an SDN containing of a robust MSPP, then a separate access connection to another robust SDN at shall be used for redundancy.

[Conditional] If the Network Infrastructure supports C2 users, then the Network Infrastructure routers shall each have an availability of 99.999 percent (%) to include scheduled maintenance.

NOTE: The availability calculations will be based on best practices because there appears to be no standardized model for calculating router availability.

[Conditional] If the Edge Segment has at least two separate access connections and the CE router detects an access connection failure, the CE router shall switch to the alternate/backup access connection.

NOTE: The detection of the access connection failure may occur either by a T1 or (SONET) level alarm (level 2), or by a loss of router HELLO status messages (level 3).

[Conditional] If the CE router has at least two separate access connections (i.e., dual homed) and detects an access connection failure, the CE router shall switch to the alternate/backup access connection using an automatic process and shall not require operator actions.

NOTE: When switchover occurs, VVoIP sessions in progress may be lost, and new sessions may not be able to be established until the IP routing updates have taken place. This may take 10 seconds or more and is dependent on the routing protocol standard update interval.

[Required] No segment of the E2E Network Infrastructure shall use split cost metric routing for VVoIP traffic.

NOTE: Split cost metric routing is a technique used to provide survivability by sending packets associated with a session across multiple paths through the Network Infrastructure. This technique often introduces unacceptable jitter.

[Conditional] If the Edge Segment has at least two access connections to provide redundancy, then the network administrators shall switch VVoIP traffic between access connections at least weekly to verify that the alternate circuit or path is working properly.

[Required] Network Infrastructure routers shall only enact switchovers based on a reduction in access network throughput or bandwidth in conjunction with network management (NM) troubleshooting procedures because the routers cannot determine where or what in the access IP connection is the cause of the reduction.

5.3.3.10 Design and Construction

5.3.3.10.1 Materials

5.3.3.10.1.1 Layer 1 – Physical Layer

[Required] All F-F Network Infrastructure Network Connections supporting VVoIP shall have a bandwidth of T1 (1.544 megabits per second (Mbps)) or greater (≥).

5.3.3.10.1.2 Layer 2 – Data Link Layer

[Required] The E2E Network Infrastructure (excluding session originators) supporting VVoIP sessions shall use the media default Maximum Transmission Unit (MTU). The media default MTU for Ethernet is 1500 bytes.

[Required] The E2E Network Infrastructure supporting VVoIP sessions shall permit packet fragmentation.

NOTE: Packet fragmentation allows packets to be fragmented, instead of discarded, if the path MTU is less than the MTU size of the packet transiting the path. This requirement is associated primarily with signaling and network management packets because the bearer packets are smaller than the MTU.

[Conditional] If the unclassified Edge System Product supporting VVoIP uses an Ethernet interface for connecting to the LAN, then its Network Interface Card (NIC) MTU size shall be set to 1400 bytes. The use of the MTU as specified will allow for overhead associated with encryptors or virtual private networks (VPNs) without causing packet fragmentation.

[Conditional] If the classified Edge System Product supporting VVoIP uses an Ethernet interface for connecting to the LAN, then its NIC MTU size shall be set to 1280 bytes. The use of the MTU as specified will allow for overhead associated with encryptors or virtual private networks (VPNs) without causing packet fragmentation.

[Required] All E2E Network Infrastructure network connections consisting of Ethernet connections that support VVoIP shall be switched full-duplex connections.

[Required] All E2E Network Infrastructure Product Ethernet interfaces shall support autonegotiation as described in the IEEE 802.3 series of standards.

[Required] All E2E Network System network links consisting of Ethernet connections that support VVoIP shall not exceed IEEE recommended distances for Ethernet cabling as shown in Table 5.3.3-4.

NOTE: The use of repeaters may extend the distances.

Table 5.3.3-4. IEEE Recommended Distances for Ethernet Cabling

	10BASE-T ETHERNET	100BASE-T FAST ETHERNET	1000BASE-T GIGABIT ETHERNET
CAT 5, 6 UTP, CAT 5e	330 ft 100 m	330 ft 100 m	330 ft 100 m
Multi-mode Fiber	6600 ft 2 km	6600 ft 2 km	1830 ft 550 m
Single-mode Fiber	15 mi 25 km	12 mi 20 km	3 mi 5 km
NOTE: All distances are for full duplex communications. In addition, it is understood that 10GBASE-T is an acceptable alternative, but the variety of cabling and distances are beyond the scope of this table.			
LEGEND: Base Baseband ft Foot km Kilometer		m Meter mi Mile UTP Unshielded Twisted Pair	

5.3.3.11 Provisioning

The bandwidth required per supported voice session on the Ethernet network infrastructure is 220 kilobits per second (Kbps) (110 Kbps each direction). This is based on G.711 (20 ms) with IP overhead (105 Kbps) associated with the Ethernet Interframe Gap and the use of Secure Real-Time Transport Protocol to secure the voice bearer. In addition, it includes the overhead associated with the Secure Real-Time Transport Control Protocol (RTCP) (5 Kbps), which is used for providing voice performance statistics for the voice bearer. Since no assumption can be made regarding whether the traffic is IPv4 or IPv6, the scenario resulting in the higher bandwidth is used (IPv6).

[Required] The E2E network infrastructure supporting VVoIP shall assume the use of G.711 (20 ms) for calculating bandwidth budgets within the fixed network even if compressed CODECs are used. For example, if G.729 is used for an F-T VVoIP session then the budget for the fixed portion of the network will still allocate 110 kbps to that session even though the session uses less bandwidth.

[Required] The Access connections supporting VVoIP shall be engineered to support one WAN (trunk) voice session (110 kbps of IP bandwidth in each direction) for every four (4) EIs

within the Edge Segment (NOTE: The 4/1 ratio does not include surge) or shall be traffic engineered in accordance with the following approach:

1. Determine the busy hour traffic load in Erlangs from current traffic pattern, matrix, or call volume using the following formula and use the Erlang B table to determine the number of connections/size of connection required to support the traffic load.

Busy Hour Offered Load	=	Total Call Time for the Busy Hour in Seconds /10 (averaged over the 10 busiest hours of the year)
Busy Hour Erlang	=	Busy Hour Offered Load in Seconds/3600

2. Calculate the Access Connection bandwidth requirement based on the following assumptions:

Assumptions:

Call Arrival Distribution	=	Poisson
Codec Type	=	G.711 (coding rate: 64000 bits/sec)
Frame size	=	20 ms interval time (0.020 Sec)
Samples/Packet	=	80 samples per packet
Frames/Packet	=	1
Frames/Second	=	50
Frame Size/Packet	=	160 bytes
Ethernet Interframe Gap	=	12 bytes
SRTP Authentication Tag	=	4 bytes
Frames/Erlang	=	50
Packets/Second/Erlang	=	50
Packet Size (for Ethernet)	=	262 bytes (assumes IPv6)
Access Bandwidth Formula	=	Busy Hour Erlang B * Packet Size * Packets/Second/Erlang B* 8 bits/byte

For example, if the Busy Hour Erlang B equals 25, then the access bandwidth should be 25*262*50*8 = 2,620,000 bps or 2.6 Mbps.

[Required] A B/P/C/S shall not reduce the number of simultaneous Access Connection (trunk) subscriptions to the DISN when they migrate from TDM to IP unless traffic engineering is completed in accordance with the preceding requirement.

NOTE: For instance, if the existing B/P/C/S subscribed for 100 simultaneous digital signal levels 0 (DS0s) to the DISN with their TDM architecture, but the engineered IP solution only requires 90 multiplied by (*) 110 Kbps of bandwidth, then the B/P/C/S design must support 100 multiplied by (*) 110 Kbps of bandwidth to meet this requirement.

[Required] The E2E network infrastructure design shall provide, at a minimum, a 25 percent increase in network capacity (throughput and number of sessions) above the current employed network capacity at all tandem switches, MFSs, MFSSs, and critical dual-homed EO switches and LSCs.

[Required] The long-haul portion of the network infrastructure shall be able to support a regional crisis in one theater, yet retain the surge capability to respond to a regional crisis occurring nearly simultaneously in another theater.

5.3.3.12 Interchangeability

[Required] All Edge System routers supporting VVoIP shall support, as a minimum, the following routing protocols and methods:

Static Routing. Static routing is a manual method for determining the path that traffic should take upon egress from a router. It is one method for interfacing between the CE router and the AR and is typically associated with single homed Edge Segments.

Intermediate System-to-Intermediate System Protocol (IS-IS). The IS-IS is an Open Systems Interconnection (OSI) protocol by which intermediate systems exchange routing information. This protocol is not intended to be used as the protocol to interface to the ARs.

Border Gateway Protocol Version 4 (BGP4). The BGP4 is a protocol for exchanging routing information between gateway hosts (each with its own router) in a network of autonomous systems and is described in RFCs 4271 [TBD] and 1772 [TBD]. It is second method for interfacing between the CE router and the AR and is typically associated with dual homed Edge Segments.

NOTE: The IPv6 requirements for BGP4 are specified in the UCR 2008, Section 5.3.5, IPv6 Requirements.

5.3.3.13 Voice Grade of Service

Grade of Service (GOS) is defined in Appendix A, Section A2, Glossary and Terminology Description. In addition, the voice and video (VVoIP only) GOS are calculated independently since the budgets associated with each are independent.

[Required] The E2E System shall provide a GOS of P.00 (zero sessions out of 100 will be "blocked" during the "busy hour") for FLASH and FLASH OVERRIDE voice and video (VVoIP only) sessions. This is also referred to as non-blocking service.

[Required] The E2E System shall provide a GOS of P.02 (two sessions out of 100 will be "blocked" during the "busy hour") and P.01 respectively during a 100 percent increase above normal precedence usage for PRIORITY and IMMEDIATE voice and video (VVoIP only) sessions at a minimum.

[Required] The E2E System supporting VVoIP shall provide a peacetime theater GOS of P.07 (seven voice sessions out of 100 will be "blocked" during the "busy hour") or better, and an inter-theater GOS of P.09 or better, as measured during normal business hours of the theaters for ROUTINE precedence voice and video (VVoIP only) sessions traversing the network from an EO or LSC EI.

[Required] The Edge Segment System supporting VVoIP shall provide a GOS between the EO and any PBX users or between an LSC and its subtended LSC do not exceed an additional blockage of P.02 for voice or video (VVoIP video only) sessions.

5.3.3.14 VVoIP Network Infrastructure Survivability

The following requirements contribute to the survivability of the VVoIP System:

[Required] No more than 15 percent of the bases, posts, camps, or stations shall be impacted by an outage in the network.

5.3.3.15 Voice Service Quality

[Required] Because intelligibility of voice communications is critical to C2, the voice service quality rating, on at least 95 percent of the voice sessions, will have a MOS in accordance with the following scenarios.

- Fixed to Fixed – 4.0
- Fixed to Tactical – 3.6
- Tactical to Tactical – 3.2

[Required] The method used for obtaining the MOS shall be in accordance with the DISR.

NOTE: The current method used is the E-Model for F-F scenarios and P.862 for Tactical Scenarios.

TABLE OF CONTENTS

SECTION **PAGE**

5.3.4 AS-SIP Requirements 779
5.3.4.1 Assured Service 779
5.3.4.2 Reference Documents 779
5.3.4.3 Applicable Standards 779
5.3.4.4 Definitions 780
5.3.4.5 Signaling Design 780
5.3.4.6 Calling Path Reference Cases 782
5.3.4.7 SIP Requirements for AS-SIP Signaling Appliances 784
5.3.4.7.1 AS-SIP Signaling Appliances 784
5.3.4.7.2 Methods 792
5.3.4.7.3 Header Fields 797
5.3.4.7.4 Response Codes 821
5.3.4.7.5 SIP Preconditions – SBU Network Only 826
5.3.4.7.5b SIP Preconditions – Classified Network Only 828
5.3.4.7.6 SIP URI and Mapping of Telephony Number into SIP URI 829
5.3.4.7.7 64kbps Transparent Calls (Clear Channel) 831
5.3.4.7.8 Transport of Route Code Information over AS-SIP 832
5.3.4.7.9 CAL General Requirements (Note: CAL Paragraphs apply to Classified only) 834
5.3.4.8 SIP Session Keep-Alive Timer 840
5.3.4.8.1 AS-SIP Signaling Appliances 840
5.3.4.9 Session Description Protocol 842
5.3.4.9.1 Session Description 842
5.3.4.9.2 Session-Level Description 843
5.3.4.9.3 Media Description 845
5.3.4.9.4 Offer/Answer Exchange 860
5.3.4.9.5 Additional Offer/Answer Rules for AS-SIP Video 860
5.3.4.9.6 Examples 861
5.3.4.10 Precedence and Preemption 863
5.3.4.10.1 Introduction 863
5.3.4.10.2 Precedence Level Communicated over SIP Signaling 863

5.3.4.10.3 ASAC Preemption Requirements 883
5.3.4.10.4 ASAC Rule Set 897
5.3.4.11 Policing of Call Count Thresholds.....910
5.3.4.11.1 Policing of Telephony Calls and Call Requests 910
5.3.4.11.2 Policing of Video Sessions and Session Requests 926
5.3.4.12 Video Telephony – General Rules.....940
5.3.4.12.2 IP-to-IP Video Telephony Call Flows 943
5.3.4.12.3 IP-to-IP Video Conference Unit Call Flows ..964
5.3.4.13 Calling Services 969
5.3.4.13.1 Introduction.....969
5.3.4.13.2 Point-to-Point Call 970
5.3.4.13.3 Call Hold.....977
5.3.4.13.4 Call Waiting.....979
5.3.4.13.5 Call Forward (Unconditional).....984
5.3.4.13.6 Call Forward (No Answer) 987
5.3.4.13.7 Call Forward (Busy) 990
5.3.4.13.8 Call Transfer 993
5.3.4.13.9 Modem on IP Networks 1012
5.3.4.14 SIP Translation Requirements for Interworking AS-SIP Signaling Appliances 1012
5.3.4.14.1 Introduction.....1012
5.3.4.14.2 Summary Description of the Three Call Types.....1022
5.3.4.14.3 SIP URI and Mapping of Telephony Number into SIP URI.....1024
5.3.4.14.4 General Requirements for Interworking AS-SIP Signaling Appliances 1025
5.3.4.14.5 ISUP Versions.....1025
5.3.4.14.6 Translation Requirements for an Interworking AS-SIP Signaling Appliance Operating as an Originating Gateway.....1026
5.3.4.14.7 Translation Requirements for Interworking AS-SIP Signaling Appliance Operating as a Terminating Gateway.....1040
5.3.4.15 Relevant Timers for the Terminating Gateway and the Originating Gateway.....1056
5.3.4.15.1 ISUP Timers.....1056
5.3.4.15.2 SIP Timers 1058

5.3.4.16 SIP Requirements for Interworking AS-SIP Signaling Appliances 1058
5.3.4.16.1 General Requirements....1058
5.3.4.16.2 Methods....1059
5.3.4.16.3 Header Fields 1061
5.3.4.16.4 Response Codes 1064
5.3.4.16.5 SIP Preconditions....1065
5.3.4.16.6 64kbps Transparent Calls (Clear Channel) ..1065
5.3.4.16.7 Transport of Route Code Information over AS-SIP 1066
5.3.4.17 Keep-Alive Timer Requirements for interworking AS-SIP Signaling Appliances 1067
5.3.4.17.1 Keep-Alive Timer Requirements for Interworking AS-SIP Signaling Appliances 1067
5.3.4.18 Precedence and Preemption Extensions for Interworking AS-SIP Signaling Appliances....1067
5.3.4.18.1 Precedence Level Communicated over SIP Signaling 1067
5.3.4.18.2 Requirements for Interworking AS-SIP Signaling Appliances 1068
5.3.4.18.3 Option Tag 'resource-priority'....1070
5.3.4.18.4 Error Conditions....1071
5.3.4.18.5 Precedence Call Rules....1074
5.3.4.19 Supplementary Services....1085
5.3.4.19.1 Introduction....1085
5.3.4.19.2 Point-to-Point Call 1086
5.3.4.19.3 Call Hold....1109
5.3.4.19.4 Call Waiting....1117
5.3.4.19.5 Call Forward (Unconditional)....1137
5.3.4.19.6 Call Forward (No Answer) 1145
5.3.4.19.7 Call Forward (BUSY) 1153
5.3.4.19.8 Call Transfer 1160

5.3.4 AS-SIP Requirements

UCR 2008, Section 5.3.4 identifies the technical specifications for an Assured Service (AS) Session Initiation Protocol (SIP) (AS-SIP). This specification is based on the commercial standards of SIP, and adds elements that allow Assured Service Access Control (ASAC) functions to be executed in a Department of Defense (DoD) network. Sections 5.3.4.1 through 5.3.4.13 of this specification addresses the enabling of signaling for Assured Service over the IP backbone. Sections 5.3.4.14 through section 5.3.4.19 of this specification address the Time Division Multiplexing (TDM)-Internet Protocol (IP) signaling interoperability requirements placed on Softswitches in order to support calls that traverse both the TDM and IP segments of the Defense Switched Network (DSN). In particular, TDM bridging call flows, TDM–to-IP call flows, and IP-to-TDM call flows are discussed.

This specification represents functional requirements to enable interoperability among various signaling products. It is not the intent of this generic requirements (GR) specification to be a complete product specification for signaling appliances. As a generic requirements specification, the capability to provide AS-SIP signaling by a product (e.g. LSC, MFSS) is called out by the respective product specifications in UCR 2008, Section 5.3.2, Assured Services Requirements. It is expected that the product specifications (a GSR) are the basis for certification testing and for the product being placed on the Approved Products List.

5.3.4.1 Assured Service

The driver behind the AS-SIP specification is the requirement for providing Assured Services to the Warfigther.

5.3.4.2 Reference Documents

The reference documents used are sited in UCR 2008, Appendix A, Definitions, Abbreviations and Acronyms, and References.

5.3.4.3 Applicable Standards

The standards used in this section are provided in UCR 2008, Appendix A, Definitions, Abbreviations and Acronyms, and References, and are referenced as part of the AS-SIP specification.

5.3.4.4 Definitions

Definitions are found in UCR 2008, Appendix A, Definitions, Abbreviations and Acronyms, and References.

5.3.4.5 Signaling Design

The network-level signaling design is depicted in Figure 5.3.4-1, Network-Level AS-SIP Signaling Design. The signaling architecture is constructed as a two-tier hierarchy. Local Session Controllers (LSCs) are located at bases/posts/camps/stations (B/P/C/Ss) and represent the level of the signaling hierarchy closest to the end instrument, and they may be thought of as the packet switched equivalent of the End Office, Private Branch Exchange Type 1 (PBX1), or Type 2 (PBX2). Softswitches are located at Service Delivery Nodes (SDNs) and represent the upper level of the hierarchy and may be thought of as analogous to class 4 Tandem Switches. Functionally, Softswitches are comprised of a Tier0 LSC and an interworking function enabling interoperability in the signaling plane between the IP portion of the DSN and the TDM portion of the DSN. An associated media gateway function performs the interworking between TDM circuit-switched bearer streams and Real Time Protocol (RTP)/User Datagram Protocol (UDP)/IP packets.

Every LSC is assigned to a primary Softswitch and to at least one secondary Softswitch.

Every Softswitch serves a set of LSCs that may be located at various B/P/C/Ss.

All voice and video call signaling messages received by an LSC from local end instruments and intended for a destination over the DISN WAN is sent by the LSC in the form of an AS-SIP message to the assigned Softswitch. Similarly, all voice and video call signaling messages sent from a remote location and intended for IP end instruments associated with a given LSC will be routed to the Softswitch assigned to the destination LSC and the Softswitch will forward the AS-SIP signaling messages to the destination LSC.

The basic AS-SIP message flow between an originating LSC assigned to one Softswitch and a destination LSC assigned to another Softswitch is:

Originating LSC --- Softswitch 1 ---------- Softswitch 2 --- Destination LSC

The basic AS-SIP message flow between an originating LSC and a destination LSC assigned to the same Softswitch is:

ORIGINATING LSC --- SOFTSWITCH --- DESTINATION LSC

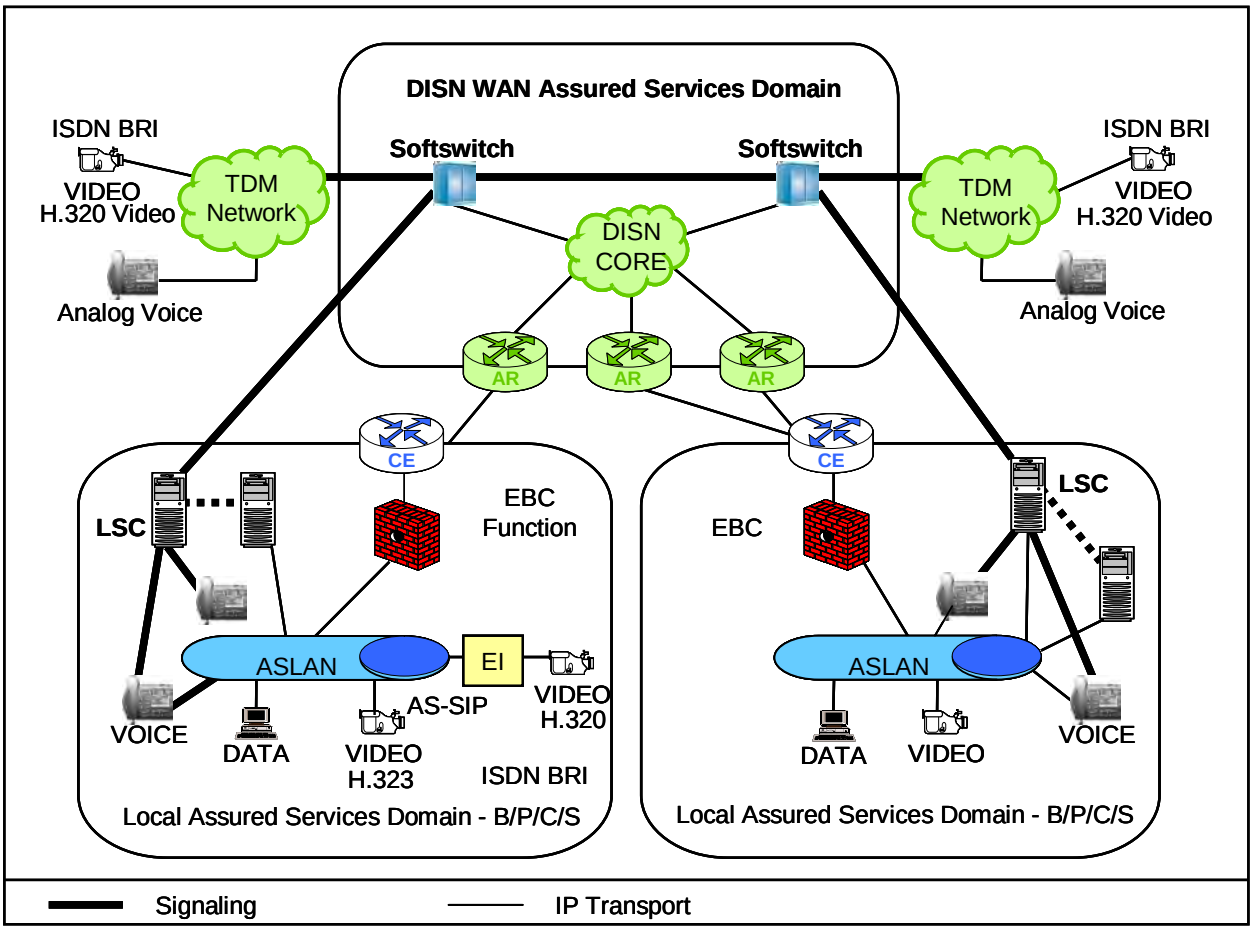


Figure 5.3.4-1. Network-Level AS-SIP Signaling Design

The access link between the Customer Edge (CE) Router and the Access Router is resource constrained and the LSC has primary responsibility for ensuring that the voice traffic across the access link does not exceed a provisioned threshold call count and that the video traffic across the access link does not exceed a provisioned threshold bandwidth.

The Softswitch is responsible for implementing a policing function to protect the access links (and to protect the DISN itself) whereby the Softswitch intervenes by blocking call requests or preempting call requests and existing calls when the Softswitch determines that the LSC has exceeded its provisioned threshold for voice or video traffic.

For the FY2008-2012 time frame, the DISN Wide Area Network (WAN) is considered to be bandwidth unlimited.

5.3.4.6 Calling Path Reference Cases

Based on the design described in UCR 2008, Section 5.3.4.5, Signaling Design, the calling patterns that must be supported in order to provide the telephony services can be identified. This section lists the referenced calling paths for the signaling associated with IP-to-IP calls over an IP core (see Figure 5.3.4-2).

The calling path reference cases for calls involving both IP and TDM signaling appliances may be found in UCR 2008, Section 5.3.2.14, SIP Translation Requirements for Interworking AS-SIP Signaling Appliances.

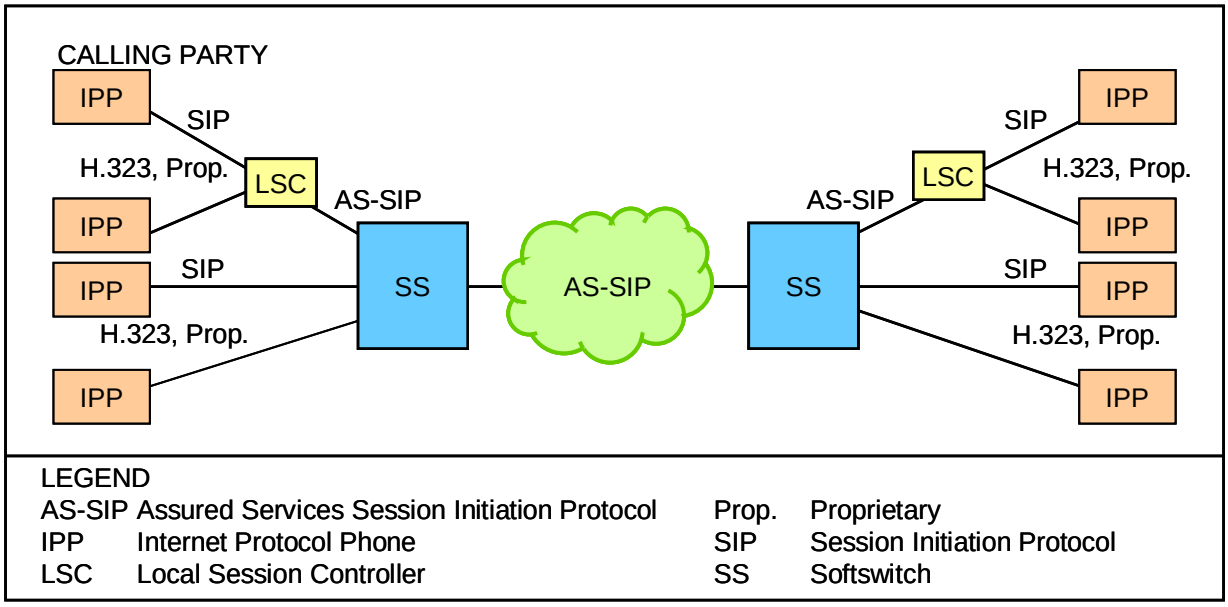


Figure 5.3.4-2. IP-to-IP Calls over an IP Backbone

NOTE: Reference cases 2A through 2P (see Table 5.3.4-1) represent the call paths when the same Softswitch serves both the calling party calling party's LSC (or the calling party's end instrument directly) and the called party's LSC (or the called party's end instrument directly).

Table 5.3.4-1. Reference Case: IP-to-IP Calls over an IP Backbone

Ref. Case	Originator Phone	Originator Signaling	Network Signaling and Call Path							Terminator Signaling	Terminator Phone
1A	IP phone	SIP	LSC	AS-SIP	Softswitch	AS-SIP	Softswitch	AS-SIP	LSC	SIP	IP phone
1B	IP phone	SIP	LSC	AS-SIP	Softswitch	AS-SIP	Softswitch	AS-SIP	LSC	H323, Prop.	IP phone
1C	IP phone	SIP	LSC	AS-SIP	Softswitch	AS-SIP	Softswitch			SIP	IP phone
1D	IP phone	SIP	LSC	AS-SIP	Softswitch	AS-SIP	Softswitch			H323, Prop.	IP phone
1E	IP phone	H323, Prop.	LSC	AS-SIP	Softswitch	AS-SIP	Softswitch	AS-SIP	LSC	SIP	IP phone
1F	IP phone	H323, Prop.	LSC	AS-SIP	Softswitch	AS-SIP	Softswitch	AS-SIP	LSC	H323, Prop.	IP phone
1G	IP phone	H323, Prop.	LSC	AS-SIP	Softswitch	AS-SIP	Softswitch			SIP	IP phone
1H	IP phone	H323, Prop.	LSC	AS-SIP	Softswitch	AS-SIP	Softswitch			H323, Prop.	IP phone
1I	IP phone	SIP			Softswitch	AS-SIP	Softswitch	AS-SIP	LSC	SIP	IP phone
1J	IP phone	SIP			Softswitch	AS-SIP	Softswitch	AS-SIP	LSC	H323, Prop.	IP phone
1K	IP phone	SIP			Softswitch	AS-SIP	Softswitch			SIP	IP phone
1L	IP phone	SIP			Softswitch	AS-SIP	Softswitch			H323, Prop.	IP phone
1M	IP phone	H323, Prop.			Softswitch	AS-SIP	Softswitch	AS-SIP	LSC	SIP	IP phone
1N	IP phone	H323, Prop.			Softswitch	AS-SIP	Softswitch	AS-SIP	LSC	H323, Prop.	IP phone
1O	IP phone	H323, Prop.			Softswitch	AS-SIP	Softswitch			SIP	IP phone
1P	IP phone	H323, Prop.			Softswitch	AS-SIP	Softswitch			H323, Prop.	IP phone
2A	IP phone	SIP	LSC	AS-SIP	Softswitch	AS-SIP			LSC	SIP	IP phone
2B	IP phone	SIP	LSC	AS-SIP	Softswitch	AS-SIP			LSC	H323, Prop.	IP phone
2C	IP phone	SIP	LSC	AS-SIP	Softswitch					SIP	IP phone
2D	IP phone	SIP	LSC	AS-SIP	Softswitch					H323, Prop.	IP phone
2E	IP phone	H323, Prop.	LSC	AS-SIP	Softswitch	AS-SIP			LSC	SIP	IP phone
2F	IP phone	H323, Prop.	LSC	AS-SIP	Softswitch	AS-SIP			LSC	H323, Prop.	IP phone
2G	IP phone	H323, Prop.	LSC	AS-SIP	Softswitch					SIP	IP phone
2H	IP phone	H323, Prop.	LSC	AS-SIP	Softswitch					H323, Prop.	IP phone
2I	IP phone	SIP			Softswitch	AS-SIP			LSC	SIP	IP phone
2J	IP phone	SIP			Softswitch	AS-SIP			LSC	H323, Prop.	IP phone
2K	IP phone	SIP			Softswitch					SIP	IP phone
2L	IP phone	SIP			Softswitch					H323, Prop.	IP phone
2M	IP phone	H323, Prop.			Softswitch	AS-SIP			LSC	SIP	IP phone
2N	IP phone	H323, Prop.			Softswitch	AS-SIP			LSC	H323, Prop.	IP phone
2O	IP phone	H323, Prop.			Softswitch					SIP	IP phone
2P	IP phone	H323, Prop.			Softswitch					H323, Prop.	IP phone

5.3.4.7 SIP Requirements for AS-SIP Signaling Appliances

The following listed sections (including sub-sections) have both SBU and Classified requirements. The Classified-specific requirements are specified in Requirements 5.3.4.7.3.1.5.1–5.3.4.7.3.1.5.3; 5.3.4.7.3.1.10–5.3.4.7.3.1.15; 5.3.4.7.3.2.3; 5.3.4.7.3.3.5.1–5.3.4.7.3.3.5.3; 5.3.4.7.3.4.8–5.3.4.7.3.4.11; 5.3.4.7.4.1.11; 5.3.4.7.5b.1–5.3.4.7.5b.8; and 5.3.4.7.9.1–5.3.4.7.9.19.2. The following listed requirements have been modified in UCR 2008, Section 6.2.1 to include those unique characteristics for the Classified application – 5.3.4.11.1.9; 5.3.4.11.1.13.2; 5.3.4.11.1.14.3-5.3.4.11.1.14.4; 5.3.4.11.1.15.2; 5.3.4.11.2.10; 5.3.4.11.2.14.2; 5.3.4.11.2.14.7; 5.3.4.11.2.15.2; and 5.3.4.11.2.7.

5.3.4.7.1 AS-SIP Signaling Appliances

In this specification, the term AS-SIP signaling appliance refers to LSCs and Softswitches. This specification will also often refer to AS-SIP signaling appliances serving SIP end instruments, or non-SIP IP end instruments, or IP end instruments in which case the requirement applies to LSCs and to the LSC component of Softswitches that directly serve SIP end instruments, or non-SIP IP end instruments, or IP end instruments, respectively.

5.3.4.7.1.1 The AS-SIP signaling appliances MUST comply with the SIP syntax and encoding rules set forth in RFC 3261. [RFC 3261, Section 25, Augmented BNF for the SIP Protocol]

5.3.4.7.1.2 The AS-SIP signaling appliances MUST comply with the requirement for SIP message structure set forth in RFC 3261, which covers SIP requests, SIP responses, SIP header fields, and SIP bodies. [RFC 3261, Section 7, SIP Messages]

5.3.4.7.1.3 When an AS-SIP signaling appliance does not understand a header field in a request (and support for the header field is not a mandatory requirement under this specification), the AS-SIP signaling appliance MUST ignore that header field and continue processing the message. The AS-SIP signaling appliances SHOULD ignore any malformed header fields that are not necessary for processing requests. [RFC 3261, Section 8.2.2, Header Inspection]

5.3.4.7.1.3a AS-SIP signaling appliances that function as back-to-back user agents (B2BUAs) MUST preserve header fields they do not understand when copying SIP messages from one side of the B2BUA to the other.

A back-to-back user agent (B2BUA) is a logical entity that receives a request and processes it as a user agent server (UAS). In order to determine how the request should be answered, it acts as a user agent client (UAC) and generates requests. Unlike a proxy server, it maintains dialog state and must participate in all requests sent on the dialogs it has established. Since it is a

concatenation of a UAC and UAS, no explicit definitions are needed for its behavior. [RFC 3261]

5.3.4.7.1.3b When an AS-SIP signaling appliance, that is implemented as a SIP proxy, receives a SIP Request message, 2xx response, or 18x response then the AS-SIP signaling appliance MUST add a Record-Route header whereby the userinfo part of the SIP URI is a unique identifier for the AS-SIP signaling appliance and an IP address is used for the host name.

Example:

Record-Route: <sip:lsc3@192.168.24.132;lr>

NOTE: This requirement is not applicable to an AS-SIP signaling appliance that is implemented as a B2BUA.

5.3.4.7.1.4 The AS-SIP signaling appliances MUST be call stateful.

5.3.4.7.1.5 Upon receipt of a new request, AS-SIP signaling appliances MUST perform request validation, route information preprocessing, determine request targets, perform request forwarding, perform response processing, process timer C, handle transport error, handle CANCEL processing, and perform proxy route processing according to RFC 3261. [RFC 3261, Sections 16.3, Request Validation; 16.4, Route Information Preprocessing; 16.5, Determine Request Targets; 16.6, Perform Request Forwarding; 16.7, Perform Response Processing; 16.8, Process Timer C; 16.9, Handle Transport Error; 16.10, Handle CANCEL Processing; and 16.12, Perform Proxy Route Processing, respectively]

NOTE: Nothing in this requirement is to be interpreted to preclude an AS-SIP signaling appliance from being implemented by means of a B2BUA in which case the functions above that apply to a B2BUA MUST be implemented and the functions associated solely with a Proxy Server but not with a B2BUA (e.g., Proxy Route and Timer C processing) are not required as long as the functional requirements and interoperability requirements of the AS-SIP signaling appliance as defined in this specification are met.

5.3.4.7.1.6 The AS-SIP signaling appliances MUST comply with the requirements applicable to non-INVITE client transactions. [RFC 3261, Sections 17.1.2, Non-INVITE Client Transaction; 17.1.3, Matching Responses to Client Transactions; 17.1.4, Handling Transport Errors; 17.2.2, Non-INVITE Server Transaction; 17.2.3, Matching Requests to Server Transactions; and 17.2.4, Handling Transport Errors]

5.3.4.7.1.7 The AS-SIP signaling appliances MUST support generation of the long form of the SIP header fields along with the receipt and processing of the long form of the SIP header fields. NOTE: The long form is the default for the SIP header fields.

5.3.4.7.1.8 The AS-SIP signaling appliances MUST support receiving and processing the compact form of the SIP header fields. [RFC 3261, Section 20, Header Fields]

5.3.4.7.1.9 The AS-SIP signaling appliances serving IP end instruments MUST support the offer/answer model for the Session Description Protocol (SDP). [RFC 3264]

5.3.4.7.1.10 In the event an AS-SIP signaling appliance receives an INVITE from a served IP end instrument and the AS-SIP signaling appliance has been unable to establish a TLS connection with its EBC and is unable to do so upon receipt of the INVITE, then the AS-SIP signaling appliance MUST reply to the INVITE with a 403 (Forbidden) response code and send an alarm to the network management system. The alarm MUST notify the network management system that the AS-SIP signaling appliance was unable to establish a TLS connection and MUST provide the identity of the EBC with which the AS-SIP signaling appliance was unable to establish the TLS connection.

5.3.4.7.1.11 In the event an EBC receives an INVITE from its AS-SIP signaling appliance and has been unable to establish a TLS connection with either the EBC or the AS-SIP signaling appliance that is the next hop for the INVITE and is unable to do so upon receipt of the INVITE, then the EBC MUST reply to the INVITE with a 403 (Forbidden) response code and send an alarm to the network management system. The alarm MUST notify the network management system that the EBC was unable to establish a TLS connection and MUST provide the identity of the AS-SIP signaling appliance or peer EBC with which it was unable to establish the TLS connection.

5.3.4.7.1.12 When a Softswitch receives an INVITE from either a served LSC or another Softswitch whose Request-URI has a DSN phone number for which the Softswitch has no entry in its Location Server, then the Softswitch MUST respond with a 404 (Not Found). Upon receipt of the 404 (Not Found) response message the originating LSC is responsible for ensuring that:

- The end instrument plays the Vacant Code Announcement (VCA) “Remote Switch. Name and Location. Your call cannot be completed as dialed. Please consult your directory and call again or ask your operator for assistance. This is a recording. Remote Switch Name and Location.”

- The end instrument is instructed to terminate the call. In the case of a SIP end instrument the originating LSC forwards the 404 (Not Found) after the VCA is played to the user.

5.3.4.7.1.13 When an LSC receives an inbound INVITE from its primary (or secondary) Softswitch whose Request-URI has a DSN phone number for which the LSC has no entry in its Location Server then the LSC MUST respond with a 404 (Not Found) response message. Upon receipt of the 404 (Not Found) the originating LSC is responsible for ensuring that:

- The end instrument plays the VCA "Remote Switch Name and Location. Your call cannot be completed as dialed. Please consult your directory and call again or ask your operator for assistance. This is a recording. Remote Switch Name and Location."

- The end instrument is instructed to terminate the call. In the case of a SIP end instrument the originating LSC forwards the 404 (Not Found) after the VCA is played to the user.

5.3.4.7.1.13a An IP packet is only allowed to carry one AS-SIP Request message or AS-SIP response message. In other words, multiple AS-SIP messages are not permitted to be carried as the payload of any given IP packet.

Early Media

NOTE: The originating AS-SIP signaling appliance interprets the presence of a sdp answer (or offer in the case of an Empty INVITE) in the first 18x response to an outbound INVITE to mean that the call is being interworked and that the end instrument will receive early media in the backward RTP bearer path. Conversely, the AS-SIP signaling appliance interprets the absence of a sdp answer (or offer in the case of an Empty INVITE) in the first 18x response to an outbound INVITE to mean that the call is NOT being interworked, early media is not going to be received by the end instrument in the backward bearer path and that ring back must be generated locally.

However, the presence of preconditions in a call flow represents the single exception to this method by which the originating AS-SIP signaling appliance determines whether the end instrument will be receiving early media over the backward bearer path or generating ring back locally.

In the case of the end-to-end status type precondition, the terminating AS-SIP signaling appliance responds to an INVITE with preconditions by sending a 183 Session Progress without sdp to indicate that the end instrument will not be receiving early media before sending the 180 ringing with the sdp. See Requirements 5.3.4.13.2.1.3 and 5.3.4.19.2.3.3. In the event the call is being inter-worked the inter-working gateway by sending a duplicate 183 Session Progress with an identical sdp answer immediately after sending the 200 OK PRACK. This will signify to the

originating AS-SIP signaling appliance that early media will be sent to the end instrument over the backward bearer path. See Requirements 5.3.4.19.2.2.3 and 5.3.4.19.2.4.3.

In the case of the segmented status type precondition, the terminating AS-SIP signaling appliance responds to an INVITE with preconditions by sending a 183 session progress without sdp to indicate that the end instrument will not be receiving early media before sending the 180 ringing with the sdp. See Requirements 5.3.4.13.2.1.4 and 5.3.4.19.2.3.2. In the event the call is being inter-worked the inter-working gateway does not send the 183 session progress but rather simply sends the 180 ringing with sdp in accordance with RFC 3312. This will signify to the originating AS-SIP signaling appliance that early media will be sent to the end instrument over the backward bearer path. See Requirements 5.3.4.19.2.2.2 and 5.3.4.19.2.4.2.

5.3.4.7.1.14 AS-SIP signaling appliances serving IP end instruments MUST ensure that all outbound INVITEs forwarded onto the DISN WAN include a Supported header with the 100rel option tag.

NOTE: All AS-SIP signaling appliances MUST support RFC 3262 Reliability of Provisional Responses in the Session Initiation Protocol (SIP).

5.3.4.7.1.15 When an AS-SIP signaling appliance receives an INVITE (having an sdp offer) and will be interworking the signaling to the TDM network, then the AS-SIP signaling appliance MUST return an sdp answer in the first non-failure reliable provisional response. For example:

IP EI ➲ LSC A ➲ Softswitch A ➲ Softswitch B ➲ EO ➲ analog EI
IP EI ⇦ LSC A ⇦ Softswitch A ⇦ Softswitch B 18x response

In this example, Softswitch B performs the signal interworking between SIP and CCS7 ISUP or ISDN, and therefore, Softswitch B MUST return an sdp answer in the first 18x response.

5.3.4.7.1.15.1 When the originating LSC (and originating SIP IP end instrument, if applicable) receives an sdp answer in the first 18x response then the originating end instrument MUST listen to the bearer stream for early media and MUST NOT generate local tones and announcements UNLESS the originating AS-SIP signaling appliance subsequently receives a SIP message in the signaling plane that requires the originating AS-SIP signaling appliance to instruct the IP end instrument to play an announcement locally.

5.3.4.7.1.16 When an AS-SIP signaling appliance receives an INVITE (having an sdp offer) intended for a served IP end instrument then the AS-SIP signaling appliance MUST NOT return an sdp answer in any provisional response and MUST only place the sdp answer in the 200 response.

5.3.4.7.1.16.1 When the originating AS-SIP signaling appliance [and originating SIP IP end instrument, if applicable] does not receives an sdp answer in the first 18x response then the originating AS-SIP signaling appliance MUST instruct the originating end instrument to generate local tones and announcements as required and the IP end instrument does not listen for early media over the bearer stream.

Early Media and Empty INVITE

5.3.4.7.1.17 When an AS-SIP signaling appliance receives an empty INVITE (i.e., an INVITE that does not include an sdp offer) and said AS-SIP signaling appliance will be interworking the signaling to the TDM network, then the AS-SIP signaling appliance MUST send an sdp offer in the first reliable non-failure provisional response (1xx greater than (>) 100).

5.3.4.7.1.17.1 When the originating AS-SIP signaling appliance (and originating SIP IP end instrument, if applicable) receives an sdp offer in the first 18x response, then the originating end instrument MUST listen to the bearer stream for early media and MUST NOT generate local tones and announcements UNLESS the originating AS-SIP signaling appliance subsequently receives a SIP message in the signaling plane that requires the originating AS-SIP signaling appliance to instruct the IP end instrument to play an announcement locally.

5.3.4.7.1.18 When an AS-SIP signaling appliance receives an Empty INVITE intended for a served IP end instrument, then the AS-SIP signaling appliance MUST NOT send an sdp offer in any provisional response (1xx greater than (>) 100) and MUST only send the sdp offer in the 200 response.

5.3.4.7.1.18.1 When the originating AS-SIP signaling appliance (and originating SIP IP end instrument, if applicable) does not receives an sdp offer in the first 18x response, then the originating AS-SIP signaling appliance MUST instruct the originating end instrument to generate local tones and announcements as required and the IP end instrument does not listen for early media over the bearer stream.

See UCR 2008, Section 5.3.4.10.4, ASAC Rule Set, for requirements relating to empty INVITE and ASAC call count.

Interworking Early Media to the TDM Network

The next section describes calling from the TDM network to establish sessions in the IP network.

5.3.4.7.1.19 When an AS-SIP signaling appliance that is interworking SIP signaling with the TDM network receives a 180 Ringing response from the IP network, the AS-SIP signaling appliance MUST ensure that the appropriate ringback tone (e.g., ringback, precedence ringback)

is generated on the TDM Network. NOTE: UCR 2008, Section 5.3.4.14, SIP Translation Requirements for Interworking AS-SIP Signaling Appliances, details the interworking for the 180 (Ringing) response in the signaling plane.

5.3.4.7.1.20. Announcements are not sent in-band on the DSN TDM network; therefore, when an AS-SIP signaling appliance that is interworking SIP signaling with the TDM network receives a 480 (Temporarily Unavailable), 486 (Busy Here), or 488 (Not Acceptable Here) from the IP Network with either no Reason header or a Reason header that does NOT have a preemption cause, the AS-SIP signaling appliance does NOT generate an announcement to be sent to the TDM network, but rather sends either a REL with Q.850 cause code 46 precedence call blocked (in the case of CCS7 ISUP) or a Disconnect (in the case of ISDN) with the appropriate cause code message to the TDM network.

If a precedence call cannot be established in the IP network because the IP resources are being utilized by the same or higher precedence traffic in the IP network, the cause code will be sent to the TDM network with a Q.850 cause code 46 precedence call blocked (in the case of ISDN).

Media Feature Tags

5.3.4.7.1.21 An AS-SIP signaling appliance that receives an outbound call request from a served IP end instrument MAY include an audio media feature tag and a video media feature tag, as appropriate, in the Contact header field of the INVITE message. [RFC 3840]

5.3.4.7.1.22 AS-SIP signaling appliances are NOT required to process and act upon the audio media tag and the video media tag in the contact header but all intermediary AS-SIP signaling appliances MUST preserve the audio media tag (if present) and the video tag (if present) when forwarding the INVITE. (i.e., intermediary AS-SIP signaling appliances MUST NOT strip off or modify the media feature tags).

P-Asserted-Identity

5.3.4.7.1.23 When an AS-SIP signaling appliance receives an INVITE from a served IP end instrument intended for a destination outside the enclave then the AS-SIP signaling appliance MUST generate the P-Asserted-Identity header as follows:

- If the identity of the caller is known, then the PAssertedID-value MUST include the name-addr field, e.g., the name of the caller in double quotes per RFC 3325.

- The PAssertedID-value MUST always contain the SIP URI of the calling end instrument whereby the userinfo part includes the full 10-digit DSN number.

Examples:

P-Asserted-Identity: "John Anderson" <sip:3121234567@dsn.mil>
P-Asserted-Identity: <sip:3121234567@dsn.mil>

5.3.4.7.1b AS-SIP Signaling Appliances Serving SIP End Instruments

5.3.4.7.1b.1 When a SIP end instrument is served by (i.e., assigned to) an AS-SIP signaling appliance, the AS-SIP signaling appliance MUST be the recipient of every outbound SIP message sent by the SIP end instrument.

5.3.4.7.1b.2 When a SIP end instrument is served by (i.e., assigned to) an AS-SIP signaling appliance, the AS-SIP signaling appliance MUST be the recipient of every inbound AS-SIP message intended for the SIP end instrument and MUST control the processing and forwarding of SIP messages to the SIP end instrument.

5.3.4.7.1b.3 The AS-SIP signaling appliances serving SIP end instruments MUST support authentication of the SIP end instruments. [RFC 3261, Sections 22.1, Framework; 22.3, Proxy-to-User Authentication; and 22.4, The Digest Authentication Scheme]

5.3.4.7.1b.4 The AS-SIP signaling appliances serving SIP end instruments MAY be capable of operating as redirect servers. [RFC 3261, Section 8.3, Redirect Servers]

5.3.4.7.1b.5 If the AS-SIP signaling appliance serving a SIP end instrument receives a SIP message with an encapsulated ISUP message (i.e., application/isup MIME object), then the AS-SIP signaling appliance MUST either:

- Respond with a 405 (Method Not Allowed), or
- Respond with a 415 (Unsupported Media Type) response with an Accept header that includes the supported Content-Types but does not include application/isup.

5.3.4.7.1c AS-SIP Signaling Appliances Serving H.323 and/or Proprietary IP End Instruments

5.3.4.7.1c.1 When an H.323 and/or proprietary IP end instrument is served by (i.e., assigned to) an AS-SIP signaling appliance, then the AS-SIP signaling appliance MUST be the recipient of every outbound call signaling message sent by the IP end instrument. NOTE: The AS-SIP signaling appliance is responsible for performing the translation function between the H.323 or proprietary signaling on the line side to the AS-SIP signaling on the trunk side.

5.3.4.7.1c.2 When a H.323 and/or proprietary IP end instrument is served by (i.e., assigned to) an AS-SIP signaling appliance, the AS-SIP signaling appliance MUST be the recipient of every inbound AS-SIP message intended for the IP end instrument and MUST control the processing of AS-SIP messages, and the translation and forwarding of H.323 or proprietary messages to the H.323 or proprietary IP end instrument.

5.3.4.7.1c.3 The AS-SIP signaling appliances serving H.323 and/or proprietary IP end instruments MUST comply with the rules for UAC behavior outside of a dialog. [RFC 3261, Section 8.1, UAC Behavior, and subsections]

5.3.4.7.1c.4 The AS-SIP signaling appliances serving H.323 and/or proprietary IP end instruments MUST comply with the rules for UAS behavior outside of a dialog. [RFC 3261, Section 8.2, UAS Behavior, and subsections]

5.3.4.7.1c.5 When an AS-SIP signaling appliance serving H.323 and/or proprietary end instruments receives a request that contains a Require header field with one or more option tags that it does not understand, then it MUST return a 420 (Bad Extension) response code. The response MUST include an Unsupported header field listing those option tags the element did not understand. [RFC 3261, Section 8.2.2.3, Require]

5.3.4.7.1c.6 The AS-SIP signaling appliances serving H.323 and/or proprietary end instruments MUST comply with the rules and procedures for dialogs. [RFC 3261, Section 12, Dialogs]

5.3.4.7.1c.7 If the AS-SIP signaling appliance serving H.323 and/or proprietary end instruments receives a SIP message with an encapsulated ISUP message (i.e., application/isup MIME object), then the AS-SIP signaling appliance MUST either:

- Respond with a 405 (Method Not Allowed), or
- Respond with a 415 (Unsupported Media Type) response with an Accept header that includes the supported Content-Types but does not include application/isup.

5.3.4.7.2 Methods

5.3.4.7.2.1 AS-SIP Signaling Appliances Serving SIP End Instruments

5.3.4.7.2.1.1 INVITE Request

5.3.4.7.2.1.1.1 The AS-SIP signaling appliances serving SIP end instruments MUST support generating and receiving SIP INVITE requests.

5.3.4.7.2.1.1.2 The AS-SIP signaling appliances serving SIP end instruments MUST comply with the requirements applicable to INVITE Client Transactions [RFC 3261, Sections 17.1.1.1, Overview of the Invite Transaction; 17.1.1.2, Formal Description; 17.1.1.3, Construction of the ACK Request; 17.1.3, Matching Responses to Client Transactions; and 17.1.4, Handling Transport Errors] and INVITE Server Transactions [RFC 3261, Sections 17.2.1, INVITE Server Transaction; 17.2.3, Matching Requests to Server Transactions; and 17.2.4, Handling Transport Errors].

5.3.4.7.2.1.1.3 The AS-SIP signaling appliances serving SIP end instruments MUST comply with the requirements of RFC 3261. [RFC 3261, Sections 13.2.1, Creating the Initial INVITE; 13.2.2, Processing the INVITE Responses; and 13.3.1, Processing of the INVITE]

5.3.4.7.2.1.1.4 The AS-SIP signaling appliances serving SIP end instruments MUST support the generating and receiving of SIP re-INVITE requests. [RFC 3261, Section 14, Modifying and Existing Session]

5.3.4.7.2.1.2 CANCEL Request

The AS-SIP signaling appliances serving SIP end instruments MUST support the generating, receiving, and processing of SIP CANCEL requests. [RFC 3261, Sections 16.7, Response Processing, and 16.10, CANCEL Processing]

5.3.4.7.2.1.3 REGISTER Request

It is RECOMMENDED that the SIP registrar function associated with AS-SIP signaling appliances serving SIP end instruments comply with RFC 3261. [RFC 3261, Section 10, Registrations] NOTE: The registrar function only refers to the registration of SIP end instruments served by AS-SIP signaling appliances; this requirement does not refer to a registration process between the LSC and Softswitch.

5.3.4.7.2.1.4 OPTIONS Request

5.3.4.7.2.1.4.1 AS-SIP signaling appliances serving SIP end instruments MUST comply with the requirements of RFC 3261, Section 11, Querying for Capabilities, which includes 11.1, Construction of OPTIONS Request, and 11.2, Processing of OPTIONS Request.

5.3.4.7.2.1.4.1.1 All Softswitches regardless of whether they serve SIP end instruments MUST comply with the requirements of RFC 3261, Section 11, Querying for Capabilities, which includes 11.1, Construction of OPTIONS Request, and 11.2, Processing of OPTIONS Request. Softswitches MUST respond to SIP OPTIONS requests when the Softswitch is identified in the

Request-URI or when the Softswitch receives an OPTIONS request in which the Max-Forwards header field value is zero.

NOTE: The OPTIONS request is employed by AS-SIP signaling appliances serving SIP end instruments as a component of the Softswitch fail-over mechanism whose complete requirements are found in UCR2008, Section 5.3.2, Assured Real Time Services.

5.3.4.7.2.1.5 BYE Request

The AS-SIP signaling appliances serving SIP end instruments MUST support the generating and receiving of SIP BYE requests and MUST comply with the requirements of RFC 3261. [RFC 3261, Section 15, Terminating a Session]

5.3.4.7.2.1.6 ACK Request

The AS-SIP signaling appliances serving SIP end instruments MUST support generating and receiving SIP ACK requests. [RFC 3261]

5.3.4.7.2.1.7 PRACK Request

5.3.4.7.2.1.7.1 The AS-SIP signaling appliances serving SIP end instruments MUST support generating and receiving the SIP PRACK method. [RFC 3262]

5.3.4.7.2.1.7.2 The AS-SIP signaling appliances serving SIP end instruments MUST support the use of the option tag “100rel” with the Require and Supported header fields, and MUST support the use of the Rack and RSeq header fields. [RFC 3262]

5.3.4.7.2.1.8 UPDATE Request

The AS-SIP signaling appliances serving SIP end instruments MUST support the generating and receiving of the SIP UPDATE method. [RFC 3311] In particular, in this specification UPDATE is recommended for refreshing the SIP session timer, is used in the alternative call transfer call flows that do not employ the REFER method, and is used in the optional end-to-end precondition call flow.

5.3.4.7.2.1.9 REFER Request

“A proxy [for example an AS-SIP signaling appliance serving SIP end instruments] should process a REFER request the same way it processes an OPTIONS request.” [RFC 3515, Section 2.6, Behavior of SIP Proxies]

5.3.4.7.2.1.10 SUBSCRIBE Request

At this time the AS-SIP GSS has not mandated the use of any event packages in conjunction with the SUBSCRIBE request. A requirement to support specified event packages may be added in the future.

5.3.4.7.2.1.11 NOTIFY Request

The AS-SIP signaling appliances serving SIP end instruments MUST support the NOTIFY method for event notification. [RFC 3265] In particular, this specification employs the NOTIFY request in the call transfer supplementary service (see Section 5.3.4.13, Calling Services).

5.3.4.7.2.2 AS-SIP Signaling Appliances Serving H.323 and/or Proprietary IP End Instruments

5.3.4.7.2.2.1 INVITE Request

5.3.4.7.2.2.1.1 The AS-SIP signaling appliances serving H.323 and/or proprietary IP end instruments MUST support generating and receiving SIP INVITE requests.

5.3.4.7.2.2.1.2 The AS-SIP signaling appliances serving H.323 and/or proprietary IP end instruments MUST comply with the requirements applicable to INVITE Client Transactions [RFC 3261, Sections 17.1.1.1, Overview of the Invite Transaction; 17.1.1.2, Formal Description; 17.1.1.3, Construction of the ACK Request; 17.1.3, Matching Responses to Client Transactions; and 17.1.4, Handling Transport Errors] and INVITE Server Transactions [RFC 3261, Sections 17.2.1, INVITE Server Transaction; 17.2.3, Matching Requests to Server Transactions; and 17.2.4, Handling Transport Errors].

5.3.4.7.2.2.1.3 The AS-SIP signaling appliances serving H.323 and/or proprietary IP end instruments MUST comply with the requirements of RFC 3261. [RFC 3261, Sections 13.2.1, Creating the Initial INVITE; 13.2.2, Processing the INVITE Responses; and 13.3.1, Processing of the INVITE]

5.3.4.7.2.2.1.4 The AS-SIP signaling appliances serving H.323 and/or proprietary IP end instruments MUST support the generating and receiving of SIP re-INVITE requests. [RFC 3261, Section 14, Modifying and Existing Session]

5.3.4.7.2.2.2 CANCEL Request

The AS-SIP signaling appliances serving H.323 and/or proprietary IP end instruments MUST support the generating and receiving of SIP CANCEL requests and MUST comply with the requirements of RFC 3261. [RFC 3261, Section 9, Canceling a Request]

5.3.4.7.2.2.3 OPTIONS Request

5.3.4.7.2.2.3.1 AS-SIP signaling appliances serving H.323 and/or proprietary IP end instruments MUST comply with the requirements of RFC 3261, Section 11, Querying for Capabilities, which includes 11.1, Construction of OPTIONS Request, and 11.2, Processing of OPTIONS Request.

5.3.4.7.2.2.3.1.1 All Softswitches regardless of whether they serve H.323 and/or proprietary IP end instruments MUST comply with the requirements of RFC 3261, Section 11, Querying for Capabilities, which includes 11.1, Construction of OPTIONS Request, and 11.2, Processing of OPTIONS Request. Softswitches MUST respond to SIP OPTIONS requests when the Softswitch is identified in the Request-URI or when the Softswitch receives an OPTIONS request in which the Max-Forwards header field value is zero.

NOTE: The OPTIONS request is employed by AS-SIP signaling appliances serving H.323 and/or proprietary IP end instruments as a component of the Softswitch fail-over mechanism whose complete requirements are found in UCR 2008, Section 5.3.2, Assured Real Time Services.

5.3.4.7.2.2.4 BYE Request

The AS-SIP signaling appliances serving H.323 and/or proprietary IP end instruments MUST support the generating and receiving of SIP BYE requests and MUST comply with the requirements of RFC 3261. [RFC 3261, Section 15, Terminating a Session]

5.3.4.7.2.2.5 ACK Request

The AS-SIP signaling appliances serving H.323 and/or proprietary IP end instruments MUST support the generating and receiving of SIP ACK requests. [RFC 3261]

5.3.4.7.2.2.6 PRACK Request

5.3.4.7.2.2.6.1 The AS-SIP signaling appliances serving H.323 and/or proprietary IP end instruments MUST support the generating and receiving of the SIP PRACK method. [RFC 3262]

5.3.4.7.2.2.6.2 The AS-SIP signaling appliances serving H.323 and/or proprietary IP end instruments MUST support the use of the option tag "100rel" with the Require and Supported header fields, and MUST support the use of the Rack and RSeq header fields. [RFC 3262]

5.3.4.7.2.2.7 UPDATE Request

The AS-SIP signaling appliances serving H.323 and/or proprietary IP end instruments MUST support the generating and receiving of the SIP UPDATE method. [RFC 3311] In particular, in this specification UPDATE is recommended for refreshing the SIP session timer, is used in the alternative call transfer call flows that do not employ the REFER method, and is used in the optional end-to-end precondition call flow.

5.3.4.7.2.2.8 REFER Request

The AS-SIP signaling appliances serving H.323 and/or proprietary IP end instruments MUST support the generating and receiving of the SIP REFER method, the Refer-To header field, and the refer event package. [RFC 3515]

The AS-SIP signaling appliances serving H.323 and/or proprietary IP end instruments MAY support generating and receiving/processing the Referred-By header. [RFC 3892]

5.3.4.7.2.2.9 SUBSCRIBE Request

At this time, this section has not mandated the use of any event packages in conjunction with the SUBSCRIBE request. A requirement to support specified event packages may be added in the future.

5.3.4.7.2.2.10 NOTIFY Request

The AS-SIP signaling appliances serving H.323 and/or proprietary IP end instruments MUST support the NOTIFY method for event notification. [RFC 3265] In particular, this specification employs the NOTIFY request in the call transfer supplementary service (see Section 5.3.4.13, Calling Services).

5.3.4.7.3 Header Fields

Table 5.3.4-2 and Table 5.3.4-3 (from RFC 3261) identify the header fields specified in RFC 3261. For the reader's convenience, a description of the symbols used in the tables augmented by header fields specified in subsequent SIP extensions are provided in Table 5.3.4-2, Summary of Header Fields, A-Z, and the following text. [RFC 3261, Section 20, Header Fields]

The **where** column values are:

R: The header field may only appear in requests.

r: The header field may only appear in responses.

2xx, 4xx, etc.: A numerical value or range that indicates response codes with which the header field can be used.

c: The header field is copied from the request to the response.

c(1): The header field is copied with the addition of a tag.

An empty entry in the **where** column indicates that the header field may be present in all requests and responses.

The **proxy** column describes the operations a proxy may perform on a header field:

a: A proxy can add or concatenate the header field if not present.

m: A proxy can modify an existing header field value.

d: A proxy can delete a header field value.

r: A proxy must be able to read the header field; thus this header field cannot be encrypted.

The next six columns relate to the presence of a header field in a method:

c: Conditional; the requirements on the header field depend on the context of the message.

m: The header field is mandatory.

m*: The header field SHOULD be sent, but clients/servers need to be prepared to receive messages without that header field.

o: The header field is optional.

t: The header field SHOULD be sent, but clients/servers need to be prepared to receive messages without that header field.

If a stream-based protocol, such as TCP, is used as a transport, then the header field MUST be sent.

*: The header field is required if the message body is not empty.

-: The header field is not applicable.

The underlined entries signify the minimum set of header fields that MUST be supported by at least one category of an AS-SIP signaling appliance.

Table 5.3.4-2. Summary of Header Fields, A–Z (Part 1)

HEADER FIELD	WHERE	PROXY	ACK	BYE	CAN	INV	OPT	REG
Accept	R		-	o	-	o	m*	o
Accept	2xx		-	-	-	o	m*	o
Accept	415		-	c	-	c	c	c
Accept-Contact	R	a r	o	o	o	o	o	-
Accept-Encoding	R		-	o	-	o	o	o
Accept-Encoding	2xx		-	-	-	o	m*	o
Accept-Encoding	415		-	c	-	c	c	c
Accept-Language	R		-	o	-	o	o	o
Accept-Language	2xx		-	-	-	o	m*	o
Accept-Language	415		-	c	-	c	c	c
Accept-Resource-Priority	200	a m d r	-	o	o	o	o	o
Accept-Resource-Priority	417	a m d r	-	o	o	o	o	o
Alert-Info	R	a r	-	-	-	o	-	-
Alert-Info	180	ar	-	-	-	m	-	-
Allow	R		-	o	-	o	o	o
Allow	2xx		-	o	-	m*	m*	o
Allow	r		-	o	-	o	o	o
Allow	405		-	m	-	m	m	m
Allow-Events	R		o	o	-	o	o	o
Allow-Events	2xx		-	o	-	o	o	o
Allow-Events	489		-	-	-	-	-	-
Authentication-Info	2xx		-	o	-	o	o	o
Authorization	R	m	m	m	m	m	m	
Call-ID	c	r	m	m	m	m	m	m
Call-Info	ar		-	-	-	o	o	o
Contact	R		o	-	-	m	o	o
Contact	1xx		-	-	-	o	-	-
Contact	2xx		-	-	-	m	o	o
Contact	3xx	d	-	o	-	o	o	o
Contact	485		-	o	-	o	o	o
Content-Disposition			o	o	-	o	o	o

HEADER FIELD	WHERE	PROXY	ACK	BYE	CAN	INV	OPT	REG
Content-Encoding			o	o	-	o	o	o
Content-Language			o	o	-	o	o	o
Content-Length		a r	t	t	t	t	t	t
Content-Type			*	*	-	*	*	*
Cseq	c	r	m	m	m	m	m	m
Date		a	o	o	o	o	o	o
Error-Info	300-699	a	-	o	o	o	o	o
Event	R		-	-	-	-	-	-
Expires			-	-	-	o	-	o
From	c	r	m	m	m	m	m	m
In-Reply-To	R		-	-	-	o	-	-
Join	R		-	-	-	o	-	-
Max-Forwards	R	a m r	m	m	m	m	m	m
Min-Expires	423		-	-	-	-	-	m
Min-SE	R	a m r	-	-	-	o	-	-
Min-SE	2xx	a r	-	-	-	o	-	-
MIME-Version			o	o	-	o	o	o
Organization	ar		-	-	-	o	o	o
P-Access-Network-Info	dr		-	o	-	o	o	o
P-Asserted-Identity	adr		-	o	-	o	o	-
P-Associated-URI	2xx		-	-	-	-	-	o
P-Called-Party-ID	R	a m r	-	-	-	o	o	-
P-Charging-Function-Addresses	adr		-	o	-	o	o	o
P-Charging-Vector	admr		-	o	-	o	o	o
P-DCS-Billing-Info	admr		-	-	-	o	-	-
P-DCS-LAES	adr		-	-	-	o	-	-
P-DCS-OSPS	R	d r	-	-	-	o	-	-
P-DCS-Redirect		a d r	-	-	-	o	-	-
P-DCS-Trace-Party-ID	R	d r	-	-	-	o	-	-
P-Media-Authorization	R	a d	o	-	-	o	-	-
P-Media-Authorization	2xx	a d	-	-	-	o	-	-
P-Media-Authorization	101-199	a d	-	-	-	o	-	-
Path	R	a r	-	-	-	-	-	o
Path	2xx		-	-	-	-	-	o
P-Preferred-Identity		a d r	-	o		o	o	-
Priority	R	a r	-	-	-	o	-	-
Privacy		a m r d	o	o	o	o	o	o
Proxy-Authenticate	407	a r	-	m	-	m	m	m
Proxy-Authenticate	401	a r	-	o	o	o	o	o
Proxy-Authorization	R	d r	o	o	-	o	o	o
Proxy-Require	R	a r	-	o	-	o	o	o
P-Visited-Network-ID	R	a d	-	-	-	o	o	o
Rack	R		-	-	-	-	-	-

HEADER FIELD	WHERE	PROXY	ACK	BYE	CAN	INV	OPT	REG
Reason	R		o	o	o	o	o	o
Record-Route	R	a r	o	o	o	o	o	-
Record-Route	2xx,18x	m r	-	o	o	o	o	-
Refer-To	R		-	-	-	-	-	-
Referred-By	R		-	o	-	o	o	o
Reject-Contact	R	a r	o	o	o	o	o	-
Replaces	R		-	-	-	o	-	-
Reply-To			-	-	-	o	-	-
Request-Disposition	R	ar	o	o	o	o	o	o
Require	ar		-	c	-	c	c	c
Resource-Priority	R	a m d r	o	o	o	o	o	o
Retry-After	404,413,480,486		-	o	o	o	o	o
	500,503		-	o	o	o	o	o
	600,603		-	o	o	o	o	o
Route	R	a d r	c	c	c	c	c	c
Rseq								
Security-Client	R	a r d	-	o	-	o	o	o
Security-Server	421,494		-	o	-	o	o	o
Security-Verify	R	a r d	-	o	-	o	o	o
Server	r		-	o	o	o	o	o
Service-Route	2xx	a r	-	-	-	-	-	o
Session-Expires	422		-	-	-	m	-	-
Session-Expires	422		-	-	-	m	-	-
SIP-Etag	2xx		-	-	-	-	-	-
SIP-If-Match	R		-	-	-	-	-	-
Subject	R		-	-	-	o	-	-
Subscription-State	R		-	-	-	-	-	-
Supported	R		-	o	o	m*	o	o
Supported	2xx		-	o	o	m*	m*	o
Timestamp			o	o	o	o	o	o
To	c(1)	r	m	m	m	m	m	m
Unsupported	420		-	m	-	m	m	m
User-Agent			o	o	o	o	o	o
Via	R	a m r	m	m	m	m	m	m
Via	rc	d r	m	m	m	m	m	m
Warning	r		-	o	o	o	o	o
WWW-Authenticate	401	a r	-	m	-	m	m	m
WWW-Authenticate	407	a r	-	o	-	o	o	o

Table 5.3.4-3. Summary of Header Fields, A–Z (Part 2)

HEADER FIELD	WHERE	PROXY	PRA	UPD	SUB	NOT	INF	MSG	REF	PUB
Accept	R		o		o	o			o	o
Accept	2xx		-		-	-			-	-
Accept	415		c		o	o			c	m*
Accept-Contact	R	ar	o	o	o	o	o	o	o	
Accept-Encoding	R		o		o	o			o	o
Accept-Encoding	2xx		-		-	-			-	-
Accept-Encoding	415		c		o	o			c	m*
Accept-Language	R		o		o	o			o	o
Accept-Language	2xx		-		-	-			-	-
Accept-Language	415		c		o	o			c	m*
Accept-Resource-Priority	200	a m d r	o	o	o	o	o	o	o	o
Accept-Resource-Priority	417	a m d r	o	o	o	o	o	o	o	o
Alert-Info	R		-		-	-			-	-
Alert-Info	180		-		-	-			-	-
Allow	R		o		o	o			o	o
Allow	2xx		o		o	o				
Allow	r		o		o	o			o	o
Allow	405		m		m	m			m	m
Allow-Events	R									o
Allow-Events	2xx									
Allow-Events	489									m
Authentication-Info	2xx		o		o	o			o	o
Authorization	R		o		o	o			o	o
Call-ID	c		m		m	m			m	m
Call-Info			-						-	o
Contact	R		-		m	m			m	-
Contact	1xx		-		o	o			-	-
Contact	2xx		-		m	o			m	-
Contact	3xx		o		m	m			o	o
Contact	485		o		o	o			o	o
Contact	3xx-6xx								o	o
Content-Disposition			o		o	o			o	o
Content-Encoding	o				o	o			o	o
Content-Language			o		o	o			o	o
Content-Length			t		t	t			o	t
Content-Type			*		*	*			*	*
Cseq	c		m		m	m			m	m
Date			o		o	o			o	o
Error-Info	300-699		o		o	o			o	o
Event	R									m

HEADER FIELD	WHERE	PROXY	PRA	UPD	SUB	NOT	INF	MSG	REF	PUB
Expires			-		o	-			o	o
Expires	2xx				-	m			-	m
From	c		m		m	m			m	m
In-Reply-To	R		-		-	-			-	-
Join	R		-	-	-	-	-	-	-	-
Max-Forwards	R		m		m	m			m	m
Min-Expires	423		-		m	-			-	m
Min-SE	R	a m r	-	o	-	-				
Min-SE	422		-	m	-	-				
MIME-Version			o		o	o			o	o
Organization			-		o	-			o	o
P-Access-Network-Info	dr		-	-	o	-	-	o	o	
P-Asserted-Identity	adr		-	-	o	o	-		o	
P-Associated-URI	2xx		-	-	-	-	-	-	-	
P-Called-Party-ID	R	a m r	-	-	o	-	-	o	o	
P-Charging-Function-Addresses	adr		o	o	o	o	o	o	o	
P-Charging-Vector	admr		o	o	o	o	o	o	o	
P-DCS-Billing-Info	admr			-	-	-	-	-	-	
P-DCS-LAES	adr			-	-	-	-	-	-	
P-DCS-OSPS	R	d r		-	o	-	-	-	-	
P-DCS-Redirect	adr	-	-	-	-	-	-			
P-DCS-Trace-Party-ID	R	d r	-	-	-	-	-	-		
P-Media-Authorization	R	a d		o	o	-	-	-		
P-Media-Authorization	2xx	a d		o	o	-	-	-		
Path										
Path										
P-Preferred-Identity		a d r	-	-	o	o			-	o
Priority	R		-		o	-		-	o	
Privacy		a d m r	o	o	o	o	o	o		
Proxy-Authenticate	407		m		m	m			m	m
Proxy-Authenticate	401		m						o	o
Proxy-Authorization	R		o		o	o			o	o
Proxy-Require	R		o		o	o			o	o
P-Visited-Network-ID	R	a d	-	-	o	-	-	o	o	
Rack	R		m		-	-				
Reason										
Record-Route	R		o		o	o			o	-
Record-Route	2xx		o		o	o			o	-

HEADER FIELD	WHERE	PROXY	PRA	UPD	SUB	NOT	INF	MSG	REF	PUB
Record-Route	18x		o						o	-
Record-Route	401,484				o	o				-
Refer-To	R		-	-	-	-	-	-	m	-
Referred-By										
Reject-Contact	R	a r	o	o	o	o	o	o	o	
Replaces	R		-	-	-	-	-	-	-	
Reply-To			-		-	-			-	
Request-Disposition	R	a r	o	o	o	o	o	o	o	
Require			c		o	o			c	o
Resource-Priority	R	a m d r	o	o	o	o	o	o	o	o
Retry-After	404,413, 480,486		o		o	o			o	o
Retry-After	500,503		o		o	o			o	o
Retry-After	600,603		o		o	o			o	o
Route	R		c		c	c			c	c
Rseq	1xx		-		o	o				
Security-Client	R	a r d	-	o	o	o	o	o		
Security-Server	421,49		-	o	o	o	o	o		
Security-Verify	R	a r d	-	o	o	o	o	o		
Server	r		o		o	o			o	o
Service-Route	2xx	a r	-							
Session-Expires	R	a m r	-	o	-	-				
Session-Expires	2xx	a r	-	o	-	-				
SIP-Etag	2xx		-	-	-	-	-	-	-	m
SIP-If-Match	R		-	-	-	-	-	-	-	o
Subject	R		-		-	-			-	o
Subscription-State										
Supported	R		o		o	o			o	o
Supported	2xx		o		o	o			o	o
Timestamp			o		o	o			o	o
To	c(1)		m		m	m			m	m
Unsupported	420		m		o	o			o	o
User-Agent			o		o	o			o	o
Via	R		m		-	o				m
Via		c								m
Via	rc	d r								m
Warning	r		o		o	o			o	o
WWW-Authenticate	401	a r	m		m	m			m	m
WWW-Authenticate	407	a r							o	o

Table 5.3.4-4 is a copy of the IANA Registry listing the header field parameters and parameter values. [RFC 3968, Section 4.1, Header Field Parameters Sub-Registry] The underlined entries

signify the header fields that MUST be supported by at least one category of an AS-SIP signaling appliance.

Table 5.3.4-4. IANA Registry Listing of Header Field Parameters

HEADER FIELD	PARAMETER NAME	PREDEFINED VALUES	REFERENCE
Accept	q	No	[RFC3261]
Accept-Encoding	q	No	[RFC3261]
Accept-Language	q	No	[RFC3261]
Authorization	algorithm	Yes	[RFC3261] [RFC3310]
Authorization	auts	No	[RFC3310]
Authorization	cnonce	No	[RFC3261]
Authorization	nc	No	[RFC3261]
Authorization	nonce	No	[RFC3261]
Authorization	opaque	No	[RFC3261]
Authorization	qop	Yes	[RFC3261]
Authorization	realm	No	[RFC3261]
Authorization	response	No	[RFC3261]
Authorization	uri	No	[RFC3261]
Authorization	username	No	[RFC3261]
Authentication-Info	cnonce	No	[RFC3261]
Authentication-Info	nc	No	[RFC3261]
Authentication-Info	nextnonce	No	[RFC3261]
Authentication-Info	qop	Yes	[RFC3261]
Authentication-Info	rspauth	No	[RFC3261]
Call-Info	purpose	Yes	[RFC3261]
Contact	expires	No	[RFC3261]
Contact	q	No	[RFC3261]
Content-Disposition	handling	Yes	[RFC3261]
Event	id	No	[RFC3265]
From	tag	No	[RFC3261]
P-Access-Network-Info	cgi-3gpp	No	[RFC3455]
P-Access-Network-Info	utran-cell-id-3gpp	No	[RFC3455]
P-Charging-Function-Addresses	ccf	No	[RFC3455]
P-Charging-Function-Addresses	ecf	No	[RFC3455]
P-Charging-Vector	icid-value	No	[RFC3455]
P-Charging-Vector	icid-generated-at	No	[RFC3455]
P-Charging-Vector	orig-ioi	No	[RFC3455]
P-Charging-Vector	term-ioi	No	[RFC3455]
P-DCS-Billing-Info	called	No	[RFC3603]
P-DCS-Billing-Info	calling	No	[RFC3603]
P-DCS-Billing-Info	charge	No	[RFC3603]
P-DCS-Billing-Info	locroute	No	[RFC3603]

HEADER FIELD	PARAMETER NAME	PREDEFINED VALUES	REFERENCE
P-DCS-Billing-Info	rksgroup	No	[RFC3603]
P-DCS-Billing-Info	routing	No	[RFC3603]
P-DCS-LAES	content	No	[RFC3603]
P-DCS-LAES	key	No	[RFC3603]
P-DCS-Redirect	count	No	[RFC3603]
P-DCS-Redirect	redirector-uri	No	[RFC3603]
Proxy-Authenticate	algorithm	Yes	[RFC3261] [RFC3310]
Proxy-Authenticate	domain	No	[RFC3261]
Proxy-Authenticate	nonce	No	[RFC3261]
Proxy-Authenticate	opaque	No	[RFC3261]
Proxy-Authenticate	qop	Yes	[RFC3261]
Proxy-Authenticate	realm	No	[RFC3261]
Proxy-Authenticate	stale	Yes	[RFC3261]
Proxy-Authorization	algorithm	Yes	[RFC3261] [RFC3310]
Proxy-Authorization	auts	No	[RFC3310]
Proxy-Authorization	cnonce	No	[RFC3261]
Proxy-Authorization	nc	No	[RFC3261]
Proxy-Authorization	nonce	No	[RFC3261]
Proxy-Authorization	opaque	No	[RFC3261]
Proxy-Authorization	qop	Yes	[RFC3261]
Proxy-Authorization	realm	No	[RFC3261]
Proxy-Authorization	response	No	[RFC3261]
Proxy-Authorization	uri	No	[RFC3261]
Proxy-Authorization	username	No	[RFC3261]
Reason	cause	Yes	[RFC3326]
Reason	text	No	[RFC3326]
Retry-After	duration	No	[RFC3261]
Security-Client	alg	Yes	[RFC3329]
Security-Client	ealg	Yes	[RFC3329]
Security-Client	d-alg	Yes	[RFC3329]
Security-Client	d-qop	Yes	[RFC3329]
Security-Client	d-ver	No	[RFC3329]
Security-Client	mod	Yes	[RFC3329]
Security-Client	port1	No	[RFC3329]
Security-Client	port2	No	[RFC3329]
Security-Client	prot	Yes	[RFC3329]
Security-Client	q	No	[RFC3329]
Security-Client	spi	No	[RFC3329]
Security-Server	alg	Yes	[RFC3329]
Security-Server	ealg	Yes	[RFC3329]
Security-Server	d-alg	Yes	[RFC3329]
Security-Server	d-qop	Yes	[RFC3329]
Security-Server	d-ver	No	[RFC3329]

HEADER FIELD	PARAMETER NAME	PREDEFINED VALUES	REFERENCE
Security-Server	mod	Yes	[RFC3329]
Security-Server	port1	No	[RFC3329]
Security-Server	port2	No	[RFC3329]
Security-Server	prot	Yes	[RFC3329]
Security-Server	q	No	[RFC3329]
Security-Server	spi	No	[RFC3329]
Security-Verify	alg	Yes	[RFC3329]
Security-Verify	ealg	Yes	[RFC3329]
Security-Verify	d-alg	Yes	[RFC3329]
Security-Verify	d-qop	Yes	[RFC3329]
Security-Verify	d-ver	No	[RFC3329]
Security-Verify	mod	Yes	[RFC3329]
Security-Verify	port1	No	[RFC3329]
Security-Verify	port2	No	[RFC3329]
Security-Verify	prot	Yes	[RFC3329]
Security-Verify	q	No	[RFC3329]
Security-Verify	spi	No	[RFC3329]
Subscription-State	expires	No	[RFC3265]
Subscription-State	reason	Yes	[RFC3265]
Subscription-State	retry-after	No	[RFC3265]
To	tag	No	[RFC3261]
Via	branch	No	[RFC3261]
Via	comp	Yes	[RFC3486]
Via	maddr	No	[RFC3261]
Via	received	No	[RFC3261]
Via	rport	No	[RFC3581]
Via	ttl	No	[RFC3261]
WWW-Authenticate	algorithm	Yes	[RFC3261] [RFC3310]
WWW-Authenticate	domain	Yes	[RFC3261]
WWW-Authenticate	nonce	No	[RFC3261]
WWW-Authenticate	opaque	No	[RFC3261]
WWW-Authenticate	qop	Yes	[RFC3261]
WWW-Authenticate	realm	No	[RFC3261]
WWW-Authenticate	stale	Yes	[RFC3261]

5.3.4.7.3.1 AS-SIP Signaling Appliances Serving SIP End Instruments and H.323 and Proprietary End Instruments

5.3.4.7.3.1.1 The AS-SIP signaling appliances serving SIP end instruments, and H.323 and proprietary IP end instruments MUST, in adherence with the enumerated RFCs, be capable of generating, receiving, and processing the following SIP header fields: [RFC 3261, Section 20,

Header Fields] [RFC 3262] [RFC 3265] [RFC 3325] [RFC 3326] [RFC 3515] [RFC 3891] [RFC 4028] [RFC 4412 as modified herein]

Accept
Alert-Info
Allow
Allow-Events
Call-ID
Contact
Content-Disposition
Content-Length
Content-Type
CSeq
Date
Event
Expires
From
Max-Forwards
Min-Expires
Min-SE
P-Asserted-Identity
Proxy-Authenticate (generate only)
Proxy-Authorization (receive and process only)
Proxy-Require (Classified only)
Rack
Reason
Record-Route
Refer-To
Replaces
Require
Resource-Priority
Retry-After
RSeq
Session-Expires
Subscription-State
Supported
To
Unsupported
Via
Warning

5.3.4.7.3.1.2 The AS-SIP signaling appliances that serve SIP end instruments and H.323 and proprietary IP end instruments MAY be capable of receiving and processing the following SIP header field.

Referred-By [RFC 3892]

5.3.4.7.3.1.3 The From header field MUST include a tag field. [RFC 3261, Section 19.3, Tags]

5.3.4.7.3.1.4 The To header field of a request that is part of a dialog MUST include a tag field. [RFC 3261, Section 19.3, Tags]

5.3.4.7.3.1.5 The AS-SIP signaling appliances serving SIP end instruments and H.323 and/or proprietary end instruments MUST support the use of option tags for the Require, Supported, and Unsupported header fields. Currently, option tags used in this specification are "replaces", "100rel", "resource-priority", "precondition", and "timer".

5.3.4.7.3.1.5.1 (NOTE: This paragraph applied to Classified only) The AS-SIP signaling appliances serving SIP end instruments MUST support the use of the option tag "confidential-access-level" for the Proxy-Require header of an INVITE or UPDATE either sent by a served SIP end instrument or intended for a served SIP end instrument.

5.3.4.7.3.1.5.2 (NOTE: This paragraph applied to Classified only) The AS-SIP signaling appliances serving non-SIP IP end instruments that generate either an INVITE or an UPDATE on behalf of a served non-SIP IP end instrument MUST include a Require header with the option tag "confidential-access-level" and a Proxy-Require header with the option tag "confidential-access-level.

5.3.4.7.3.1.5.3 (NOTE: This paragraph applied to Classified only) The AS-SIP signaling appliances serving non-SIP IP end instruments MUST support the use of the option tag "confidential-access-level" for the Require header of an INVITE or UPDATE intended for a served non-SIP IP end instrument.

5.3.4.7.3.1.6 **[FY2008-FY2010] [Objective]** When an LSC sends a SIP Request message to its local EBC intended for its Softswitch, then it is an objective requirement for the FY2008-FY2010 time frame that the LSC add two (2) Route header field values, which either may take the form of a route set comprised of two (2) Route headers where the first Route header is the sip uri for the EBC at the enclave and the second Route header is the sip uri for the EBC serving the Softswitch, or take the form of one (1) Route header with two (2) comma-separated field values. This is not a threshold requirement until FY2010.

5.3.4.7.3.1.6.1 **[FY2008-FY2010] [Conditional]** If the LSC adds a route set comprised of two (2) Route header field values, then the default format of the sip uri for the Route header will consist of an alphanumeric identifier for the userinfo part and an IP address for the host name.

Example:

Route: <sip:ebcenc1@192.168.7.125;lr>
Route: <sip:ebcsdn3@195.117.2.1;lr>

or

Route: <sip:ebcenc1@192.168.7.125;lr>, <sip:ebcsdn3@195.117.2.1;lr>

5.3.4.7.3.1.7 **[FY2010+]** When an LSC sends a SIP Request message to its local EBC intended for its Softswitch, then, as a default configuration, the LSC MUST add two (2) Route header field values, which either may take the form of a route set comprised of two (2) Route headers where the first Route header is the sip uri for the EBC at the enclave and the second Route header is the sip uri for the EBC serving the Softswitch, or take the form of one (1) Route header with two (2) comma-separated field values.

CCA-ID Parameter

The purpose behind the CCA-ID is to provide a simple mechanism for a Softswitch to identify the served LSC that is the source of the INVITE. This is important information required to enable the Softswitch to conduct its policing function. Referring to UCR 2008, Section 5.3.4.7.3.4, Softswitches Not Directly Serving IP End Instruments, the CCA-ID also provides a simple mechanism for a destination Softswitch to identify the originating Softswitch from which it receives an INVITE

5.3.4.7.3.1.8 When an AS-SIP signaling appliance (LSC or LSC component of Softswitch) either receives an INVITE from a served IP end instrument or generates an INVITE on behalf of a served H.323 or proprietary IP end instrument and the INVITE is intended for a destination over the DISN WAN, then the AS-SIP signaling appliance MUST add a CCA-ID parameter to the SIP URI of the Contact header. The value of the CCA-ID parameter consists of a variable length character string having a maximum length of 20 characters from the set specified in Requirement 5.3.4.7.3.1.8.1 and a unique value of the CCA-ID parameter is associated with each AS-SIP signaling appliance.

5.3.4.7.3.1.8.1 The syntax for the CCA-ID parameter is:

CCA-ID = token = 1*(alphanumeric / "-" / "." / "!" / "%" /”*”/ "_" / "+" / "`" / "'" / "~")

Example:

Contact: <sip:3121111111@10.10.10.10;CCA-ID= lscA.scottafb >

5.3.4.7.3.1.9 When an AS-SIP signaling appliance (LSC or LSC component of Softswitch) receives an inbound INVITE from the DISN WAN intended for a served SIP end instrument, the AS-SIP signaling appliance MUST strip off the CCA-ID parameter.

Route Header (Classified only)

(NOTE: This paragraph applied to Classified only) The Route Header requirements for AS-SIP signaling appliances serving SIP end instruments, H.323 end instruments, and proprietary IP end instruments are specified in Requirements 5.3.4.7.3.1.6 and 5.3.4.7.3.1.7. The Route Header requirements for Softswitches not directly serving IP end instruments are specified in Requirements 5.3.4.7.3.4.1 and 5.3.4.7.3.4.2. These requirement are predicated on the SBU network design whereby EBCs are required at each enclave having at least one AS-SIP signaling appliance.

The current VoSIP architecture does not employ EBCs, therefore it is anticipated that during the transition towards full implementation of AS-SIP within the Classified system there will be several instances where EBCs may or not be present at all locations encountered on an end-to-end AS-SIP call. Therefore the Classified requirements must include specifications for the various permutations of Route headers for the situations where an EBC is present at Tier0 SS or at LSC, or at both. If there is not an EBC at either location and there are no intermediary SIP signaling appliances between a LSC and its Tier0 SS then there may not be a need for a Route header.

The complete set of Route Header requirements for Classified AS-SIP signaling appliances serving IP end instruments (SIP end instrument and/or H.323 end instruments and/or proprietary IP end instruments) is set forth below in Requirements 5.3.4.7.3.1.10–5.3.4.7.3.1.15. In addition, the set of Route Header requirements for Classified Tier0 SS signaling appliances not directly serving IP end instruments is set forth in Requirements 5.3.4.3.7.3.4.8–5.3.4.3.7.3.4.11.

5.3.4.7.3.1.10 **[Required-FY2010]** If an EBC is deployed at the enclave of an LSC and an EBC is deployed at the Tier0 SS serving the given LSC, then when the LSC sends a SIP Request message to its local EBC intended for its Tier0 SS, it is an objective requirement for the FY2008-FY2010 time frame that the LSC add two (2) Route header field values, which either may take

the form of a route set comprised of two (2) Route headers where the first Route header is the sip uri for the EBC at the enclave and the second Route header is the sip uri for the EBC serving the Tier0 SS, or take the form of one (1) Route header with two (2) comma-separated field values.

5.3.4.7.3.1.10.1 **[Required-FY2010]** If the LSC adds a route set comprised of two (2) Route header field values, then the default format of the sip uri for the Route header will consist of an alphanumeric identifier for the userinfo part and an IP address for the host name.

Example:

Route: <sip:ebcenc1@192.168.7.125;lr>
Route: <sip:ebcsdn3@195.117.2.1;lr>

or

Route: <sip:ebcenc1@192.168.7.125;lr>, <sip:ebcsdn3@195.117.2.1;lr>

5.3.4.7.3.1.11 **[Required-FY2010]** If there is an EBC deployed at the enclave but not at the Tier0 SS, then when the LSC sends a SIP Request message to its local EBC intended for its Tier0 SS it is an objective requirement for the FY2008-FY2010 time frame that the LSC add two (2) Route header field values, which either may take the form of a route set comprised of two (2) Route headers where the first Route header is the sip uri for the EBC at the enclave and the second Route header is the sip uri for the Tier0 SS, or take the form of one (1) Route header with two (2) comma-separated field values.

Example:

Route: <sip:ebcencl@192.168.7.125;lr>
Route: <sip:Tier0sdn3@195.117.3.121;lr>

5.3.4.7.3.1.12 **[Required-FY2010]** If there is not an EBC deployed at the enclave but there is an EBC deployed at the Tier0 SS, then when the LSC sends a SIP request message to the EBC serving the Tier0 SS, the LSC either may add one (1) Route header with the sip uri of the EBC serving the Tier0 SS (NOTE: The EBC serving the Tier0 SS always sends its inbound sip messages to the Tier0 SS.) or add two (2) Route header field values, which either may take the form of two (2) Route headers where the first Route header is the sip uri for the EBC serving the Tier0 SS and the second Route header is the sip uri for the Tier0 SS, or take the form of one (1) Route header with two (2) comma-separated field values.

Example 1:

Route: <sip:ebcsdn3@195.117.2.1;lr>

Example 2:

Route: <sip:ebcsdn3@195.117.2.1;lr>
Route: <sip:Tier0sdn3@195.117.3.121;lr>

or

Route: <sip:ebcsdn3@195.117.2.1;lr>, <sip:Tier0sdn3@195.117.3.121;lr>

5.3.4.7.3.1.13 **[Required FY2010+]** If an EBC is deployed at the enclave of an LSC and an EBC is deployed at the Tier0 SS serving the given LSC, then when the LSC sends a SIP Request message to its local EBC, intended for its Tier0 SS, the LSC MUST add two (2) Route header field values, which either may take the form a route set comprised of two (2) Route headers, where the first Route header is the sip uri for the EBC at the enclave, and the second Route header is the sip uri for the EBC serving the Tier0 SS, or take the form of one (1) Route header and two (2) comma-separated field values.

5.3.4.7.3.1.14 **[Required FY2010+]** If there is an EBC deployed at the enclave but not at the Tier0 SS, then when the LSC sends a SIP Request message to its local EBC, intended for its Tier0 SS, the LSC MUST add two (2) Route header field values, which either may take the form a route set comprised of two (2) Route headers, where the first Route header is the sip uri for the EBC at the enclave, and the second Route header is the sip uri for the Tier0 SS, or take the form of one (1) Route header with two (2) comma-separated field values.

5.3.4.7.3.1.15 **[Required FY2010]** If there is not an EBC deployed at the enclave but there is an EBC deployed at the Tier0 SS, then when the LSC sends a SIP request message to the EBC serving the Tier0 SS, the LSC MUST either may add one (1) Route header with the sip uri of the EBC serving the Tier0 SS (NOTE: The EBC serving the Tier0 SS always sends its inbound sip messages to the Tier0 SS.) or add two (2) Route header field values, which either may take the form of two (2) Route headers where the first Route header is the sip uri for the EBC serving the Tier0 SS and the second Route header is the sip uri for the Tier0 SS, or take the form of one (1) Route header with two (2) comma-separated field values.

5.3.4.7.3.2 AS-SIP Signaling Appliances Serving SIP End Instruments (Not H.323 and Proprietary IP End Instruments)

5.3.4.7.3.2.1 **[Required]** The AS-SIP signaling appliances serving SIP end instruments, but not serving H.323 or proprietary IP end instruments, MUST, in adherence with the enumerated RFCs, be capable of generating, receiving, and processing the following SIP header fields: [RFC 3261, Section 20, Header Fields] [RFC 3262] [RFC 3325] [RFC 3326] [RFC 3891] [RFC 4028] [RFC 4412 as modified herein]

Accept
Alert-Info
Max-Forwards
Min-SE
P-Asserted-Identity
Proxy-Authenticate (generate only)
Proxy-Authorization (receive only)
Rack
Reason
Replaces
Record-Route
Resource-Priority
RSeq
Session-Expires
Supported
Via

5.3.4.7.3.2.2 The AS-SIP signaling appliances serving SIP end instruments MUST support the use of option tags for the Supported, and Unsupported header fields. Currently, option tags used in this specification are “100rel”, “resource-priority”, “precondition”, and “timer”.

5.3.4.7.3.2.3 (NOTE: This paragraph applied to Classified only) The AS-SIP signaling appliances serving SIP end instruments MUST support the use of the option tag “confidential-access-level” for the Proxy-Require header of an INVITE or UPDATE either sent by a served SIP end instrument or intended for a served SIP end instrument.

AS-SIP Signaling Appliance Acting AS-SIP Proxy Server for SIP EIs and VIA Header Requests

5.3.4.7.3.2.4 When an AS-SIP signaling appliance operating as a SIP proxy server receives an outbound SIP request from a served SIP end instrument then the AS-SIP signaling appliance MUST add its own VIA header.

5.3.4.7.3.2.5 When an AS-SIP signaling appliance operating as a SIP proxy server receives a SIP response for a served SIP end instrument then prior to forwarding the SIP response the AS-SIP signaling appliance MUST remove the topmost VIA header.

5.3.4.7.3.2.6 When an AS-SIP signaling appliance operating as a SIP proxy server receives an inbound SIP request for a served SIP end instrument then the AS-SIP signaling appliance MUST add its own VIA header.

5.3.4.7.3.2.7 When an AS-SIP signaling appliance operating as a SIP proxy server receives a SIP response from a served SIP end instrument then prior to forwarding the SIP response the AS-SIP signaling appliance MUST remove the topmost VIA header.

AS-SIP Signaling Appliance Acting as B2BUA for SIP EIs and VIA Header Requirements

5.3.4.7.3.2.8 When an AS-SIP signaling appliance operating as a B2BUA receives an outbound SIP request from a directly served SIP end instrument, then the AS-SIP signaling appliance generally does NOT copy the VIA header from the incoming call leg to the outgoing call leg however this specification does not forbid the B2BUA from copying the VIA header. The AS-SIP signaling appliance MUST add its own VIA header to the new call leg.

5.3.4.7.3.2.9 When an AS-SIP signaling appliance operating as a B2BUA receives a SIP response intended for a directly served SIP end instrument then the B2BUA removes the topmost header. The B2BUA then generates the response for the call leg in which it is acting as a UAS and MUST place the header of the directly served SIP end instrument into the SIP response.

5.3.4.7.3.2.10 When an AS-SIP signaling appliance operating as a B2BUA receives an inbound SIP request for a directly served SIP end instrument then the AS-SIP signaling appliance generally does NOT copy the VIA headers from the incoming call leg to the outgoing call leg however this specification does not forbid the B2BUA from copying the VIA headers. The AS-SIP signaling appliance MUST add its VIA header to the new call leg.

5.3.4.7.3.2.11 When an AS-SIP signaling appliance operating as a B2BUA receives a SIP response from a directly served SIP end instrument then the B2BUA removes the topmost header. The B2BUA then generates the response for the call leg in which it is acting as a UAS and MUST place the set of VIAs it had received in the original SIP request into the SIP response.

5.3.4.7.3.3 AS-SIP Signaling Appliances Serving H.323 and Proprietary IP End Instruments (Not SIP End Instruments)

5.3.4.7.3.3.1 The AS-SIP signaling appliances serving H.323 and/or proprietary IP end instruments, but not SIP end instruments, MUST, in adherence with the enumerated RFCs, be

capable of generating, receiving, and processing the following SIP header fields: [RFC 3261, Section 20, Header Fields] [RFC 3262] [RFC 3265] [RFC 3325] [RFC 3326] [RFC 3515] [RFC 3891] [RFC 4028] [RFC 4412 as modified herein]

Accept
Allow
Allow-Events
Call-ID
Contact
Content-Disposition
Content-Length
Content-Type
CSeq
Date
Event
Expires
From
Max-Forwards
Min-Expires
Min-SE
P-Asserted-Identity
Proxy-Require (Classified only)
Rack
Reason
Record-Route
Refer-To
Replaces
Require
Resource-Priority
Retry-After
RSeq
Session-Expires
Subscription-State
Supported
To
Unsupported
Via
Warning

5.3.4.7.3.3.2 The AS-SIP signaling appliances that serve H.323 and proprietary IP end instruments MAY be capable of receiving and processing the following SIP header field.

Referred-By [RFC 3892]

5.3.4.7.3.3.3 The From header field MUST include a tag field. [RFC 3261, Section 19.3, Tags]

5.3.4.7.3.3.4 The To header field of a request that is part of a dialog MUST include a tag field. [RFC 3261, Section 19.3, Tags]

5.3.4.7.3.3.5 The AS-SIP signaling appliances serving H.323 and/or proprietary IP end instruments MUST support the use of option tags for the Require, Supported, and Unsupported header fields. Currently, option tags used in this specification are "replaces", "100rel", "resource-priority", "precondition", and "timer".

5.3.4.7.3.3.5.1 (NOTE: This paragraph applied to Classified only) The AS-SIP signaling appliances serving non-SIP IP end instruments that generate either an INVITE or an UPDATE on behalf of a served non-SIP IP end instrument MUST include a Require header with the option tag "confidential-access-level" and a Proxy-Require header with the option tag "confidential-access-level.

5.3.4.7.3.3.5.2 (NOTE: This paragraph applied to Classified only) The AS-SIP signaling appliances serving non-SIP IP end instruments MUST support use of the option tag "confidential-access-level" for the Require header of an INVITE or UPDATE intended for a served non-SIP IP end instrument.

5.3.4.7.3.3.5.3 (NOTE: This paragraph applied to Classified only) Tier0 SSs not serving IP end instruments MUST support use of the option tag "confidential-access-level" for the Proxy-Require header of an INVITE or UPDATE message.

AS-SIP Signaling Appliance and VIA Header Requests

5.3.4.7.3.3.6 When an AS-SIP signaling appliance generates an outbound SIP request on behalf of a served non-SIP IP end instrument then the AS-SIP signaling appliance MUST add its own VIA header to the SIP request.

5.3.4.7.3.3.7 When an AS-SIP signaling appliance receives a SIP response for a served non-SIP IP end instrument then the AS-SIP signaling appliance operates as the UAC for SIP purposes and sends the appropriate protocol response to the non-SIP IP end instrument.

5.3.4.7.3.3.8 When an AS-SIP signaling appliance receives an inbound SIP request for a served non-SIP IP end instrument then the AS-SIP signaling appliance operates as the UAS for SIP purposes and sends the appropriate protocol request to the non-SIP IP end instrument.

5.3.4.7.3.3.9 When an AS-SIP signaling appliance generates a SIP response on behalf of a served non-SIP IP end instrument then MUST include theVIA headers received in the corresponding SIP request prior to forwarding the SIP response.

5.3.4.7.3.4 Softswitches Not Directly Serving IP End Instruments

5.3.4.7.3.4.1 **[Required]** When a Softswitch forwards a SIP request to a peer Softswitch, then the Softswitch MUST add two (2) Route header field values, which either may take the form of a route set comprised of two (2) Route headers where the first Route header is the sip uri for the EBC that serves the Softswitch and the second Route header is the sip uri for the EBC serving the peer Softswitch, or take the form of one (1) Route header with two (2) comma-separated field values.

5.3.4.7.3.4.1.1 **[Required]** The default format of the sip uri for the Route header will consist of an alphanumeric identifier for the userinfo part and an IP address for the host name.

Example:

Route: <sip:ebcsdn3@192.168.100.100;lr>
Route: <sip:ebcsdn7@196.1.2.111;lr>

or

Route: <sip:ebcsdn3@192.168.100.100;lr>, <sip:ebcsdn7@196.1.2.111;lr>

5.3.4.7.3.4.2 **[Required: MFSS]** When a Softswitch forwards a SIP request to a subtended LSC, then the Softswitch MUST add two (2) Route header field values, which either may take the form of a route set comprised of two (2) Route headers where the first Route header is the sip uri for the EBC that serves the Softswitch and the second Route header is the sip uri for the EBC serving the subtended LSC, or take the form of one (1) Route header with two (2) comma-separated field values.

5.3.4.7.3.4.2.1 **[Required]** The default format of the sip uri for the Route header will consist of an alphanumeric identifier for the userinfo part and an IP address for the host name.

Example:

Route: <sip:ebcsdn7@192.168.88.50;lr>
Route: <sip:ebcenc25@188.2.44.3;lr>

or

Route: <sip:ebcsdn7@192.168.88.50;lr>, <sip:ebcenc25@188.2.44.3;lr>

Intermediate AS-SIP Signaling Appliance Acting AS-SIP Proxy Server and VIA Header Requests

An intermediate AS-SIP signaling appliance is an AS-SIP signaling appliance that is receiving a SIP request from another AS-SIP signaling appliance and is not directly serving an IP end instrument that is a party to the given call request or established call.

5.3.4.7.3.4.3 When an intermediate AS-SIP signaling appliance operating as a SIP proxy server receives a SIP request, then the AS-SIP signaling appliance MUST add its own VIA header.

5.3.4.7.3.4.4 When an intermediate AS-SIP signaling appliance operating as a SIP proxy server receives a SIP response, then prior to forwarding the SIP response the intermediate AS-SIP signaling appliance MUST remove the topmost VIA header.

Intermediate AS-SIP Signaling Appliance Acting as B2BUA and VIA Header Requests

5.3.4.7.3.4.5 When an intermediate AS-SIP signaling appliance operating as a B2BUA receives a SIP request then the intermediate AS-SIP signaling appliance generally does NOT copy the VIA header(s) from the incoming call leg to the outgoing call leg; however, this specification does not forbid the B2BUA from copying the VIA headers. The intermediate AS-SIP signaling appliance MUST add its own VIA header to the new call leg.

5.3.4.7.3.4.6 When an intermediate AS-SIP signaling appliance operating as a B2BUA receives a SIP response then the B2BUA removes the topmost header. The B2BUA then generates the response for the call leg in which it is acting as a UAS and MUST place the set of VIAs it had received in the original SIP request into the SIP response.

CCA-ID Parameter

The CCA-ID provides a simple mechanism for a destination Softswitch to identify the originating Softswitch or served LSC from which it receives an INVITE.

5.3.4.7.3.4.7 When an intermediary Softswitch either receives an INVITE from a served LSC or from another Softswitch, then the intermediary Softswitch MUST replace the existing value of the CCA-ID parameter with the value of its own CCA-ID parameter before forwarding the INVITE onward to the next AS-SIP signaling appliance. See Requirement 5.3.4.7.3.1.8 for details on the syntax of the CCA-ID parameter as well as an example.

Tier0 Softswitches Not Directly Serving IP End Instruments – (Classified only)

Route Header – (Classified only)

5.3.4.7.3.4.8 (NOTE: This paragraph applied to Classified only) **[Conditional]** If EBCs are used in conjunction with Tier0 SSs, then when a Tier0 SS forwards a SIP request to a peer Tier0 SS, as a default configuration, the Tier0 SS MUST add two (2) Route header field values, which either may take the form of a route set comprised of two (2) Route headers where the first Route header is the sip uri for the EBC that serves the Tier0 SS and the second Route header is the sip uri for the EBC serving the peer Tier0 SS, or take the form of one (1) Route header with two (2) comma-separated field values.

5.3.4.7.3.4.8.1 The default format of the sip uri for the Route header will consist of an alphanumeric identifier for the userinfo part and an IP address for the host name.

Example:

Route: <sip:ebcsdn3@192.168.100.100;lr>
Route: <sip:ebcsdn7@196.1.2.111;lr>

or

Route: <sip:ebcsdn3@192.168.100.100;lr>, <sip:ebcsdn7@196.1.2.111;lr>

5.3.4.7.3.4.9 (NOTE: This paragraph applied to Classified only) **[Conditional]** If EBCs are used in conjunction with Tier0 SSs and at the enclaves in conjunction with LSCs, then when a Tier0 SS forwards a SIP request to served LSC, as a default configuration, the Tier0 SS MUST add two (2) Route header field values, which either may take the form of a route set comprised of two (2) Route headers where the first Route header is the sip uri for the EBC that serves the Tier0 SS and the second Route header is the sip uri for the EBC of the served LSC, or take the form of one (1) Route header with two (2) comma-separated field values.

5.3.4.7.3.4.9.1 The default format of the sip uri for the Route header will consist of an alphanumeric identifier for the userinfo part and an IP address for the host name.

Example:

Route: <sip:ebcsdn7@192.168.88.50;lr>
Route: <sip:ebcenc25@188.2.44.3;lr>

or

Route: <sip:ebcsdn7@192.168.88.50;lr>, <sip:ebcenc25@188.2.44.3;lr>

5.3.4.7.3.4.10 (NOTE: This paragraph applied to Classified only) **[Conditional]** If there is an EBC deployed at the Tier0 SS but not at the enclave of a served LSC, then when the Tier0 SS sends a SIP Request message to its local EBC intended for the served LSC, the Tier0 SS MUST add two (2) Route header field values, which either may take the form of a route set comprised of two (2) Route headers where the first Route header is the sip uri for its own EBC and the second Route header is the sip uri for the EBC serving the LSC, or take the form of one (1) Route header with two (2) comma-separated field values.

5.3.4.7.3.4.11 (NOTE: This paragraph applied to Classified only) **[Conditional]** If there is not an EBC deployed at the Tier0 SS but there is an EBC deployed at the enclave of the served LSC, then when the Tier0 SS sends a SIP Request message to EBC serving the LSC, the LSC MUST either add one (1) Route header with the sip uri of the EBC serving the LSC (NOTE: The EBC serving the LSC always sends its inbound sip messages to the LSC) or add two (2) Route header field values, which either may take the form of (2) Route headers where the first Route header is the sip uri for the EBC serving the LSC and the second Route header is the sip uri for the LSC, or take the form of one (1) Route header with two (2) comma-separated field values.

5.3.4.7.4 Response Codes

5.3.4.7.4.1 AS-SIP Signaling Appliances Serving SIP End Instruments

5.3.4.7.4.1.1 The AS-SIP signaling appliances serving SIP end instruments MUST support response processing. [RFC 3261, Section 16.7, Response Processing]

5.3.4.7.4.1.2 The AS-SIP signaling appliances serving SIP end instruments MUST support the forwarding of the provisional (1xx) response codes: 100 (Trying), 180 (Ringing), and 183 (Session Progress). [RFC 3261, Section 16.7, Response Processing]

5.3.4.7.4.1.3 The AS-SIP signaling appliances serving SIP end instruments MUST support the forwarding of the successful (2xx) response codes: 200 (OK) [RFC 3261] and (202) Accepted [RFC 3515].

5.3.4.7.4.1.4 The AS-SIP signaling appliances serving SIP end instruments MUST support the generating of a 200 (OK) response code in response to a CANCEL request. [RFC 3261, Section 16.10, CANCEL Processing]

5.3.4.7.4.1.5 The AS-SIP signaling appliances serving SIP end instruments MAY be capable of operating as redirect servers and MAY support the redirection (3xx) response codes: 300 (Multiple Choices), 301 (Moved Permanently), 302 (Moved Temporarily), and 305 (Use Proxy). [RFC 3261, Section 21.3, Redirection 3xx]

5.3.4.7.4.1.6 The AS-SIP signaling appliances serving SIP end instruments MUST support the forwarding of the request failure (4xx) response codes:

400 (Bad Request)	401 (Unauthorized)	403 (Forbidden)
404 (Not Found)	405 (Method Not Allowed)	406 (Not Acceptable)
407 (Proxy Authentication Required)	408 (Request Timeout)	410 (Gone)
413 (Request Entity Too Large)	414 (Request-URI Too Long)	415 (Unsupported Media Type)
416 (Unsupported URI Scheme)	417 (Unknown Resource-Priority)	420 (Bad Extension)
421 (Extension Required)	422 (Session Interval Too Small)	423 (Interval Too Brief)
480 (Temporarily Unavailable)	481 (Call/Transaction Does Not Exist)	482 (Loop Detected)
483 (Too Many Hops)	484 (Address Incomplete)	485 (Ambiguous)
486 (Busy Here)	487 (Request Terminated)	488 (Not Acceptable Here)
491 (Request Pending).		

5.3.4.7.4.1.7 The AS-SIP signaling appliances serving SIP end instruments MUST support the generating of a 404 (Not Found) response code if the Request-URI indicates a resource at the AS-SIP signaling appliance that does not exist. [RFC 3261, Section 16.5, Determining Request Targets]

5.3.4.7.4.1.8 The AS-SIP signaling appliances serving SIP end instruments MUST support the generating of either a 401 (Unauthorized) or a 407 (Proxy Authentication Required) response code, as appropriate. [RFC 3261, Section 22.2 User-to-User Authentication, Section 22.3, Proxy-to-User Authentication]

5.3.4.7.4.1.9 The AS-SIP signaling appliance serving SIP end instruments MUST support the generating of a 408 (Request Timeout) response code when all client transactions in a response have terminated and no final response has been received. [RFC 3261, Section 16.6, Request Forwarding]

5.3.4.7.4.1.10 The AS-SIP signaling appliances serving SIP end instruments MUST support the generating of a 416 (Unsupported URI Scheme) response code upon receipt of a Request-URI that it does not understand. [RFC 3261, Section 16.3, Request Validation]

5.3.4.7.4.1.11 (NOTE: This paragraph applied to Classified only.) AS-SIP signaling appliances MUST support the generating of a 418 (Incompatible CAL) upon receipt of an INVITE or UPDATE that cannot be resolved to a valid CAL. The 418 response SHOULD contain the CAL header with the reflected-access-level set to the last successfully resolved value in the request path. The local-access-level SHOULD be set to the access-level supported by the destination SIP EI or AS-SIP signaling appliance serving the destination non-SIP IP EI or to the access-level supported for the routing domain that failed resolution at an intermediate Tier0 SS.

5.3.4.7.4.1.12 The AS-SIP signaling appliances serving SIP end instruments that are unable to establish a target for a received request SHOULD support generating a 480 (Temporarily Unavailable) response code. [RFC 3261, Section 16.5, Determining Request Targets]

5.3.4.7.4.1.13 The AS-SIP signaling appliances serving SIP end instruments MAY generate a 482 (Loop Detected) response code if a forwarding loop is detected. [RFC 3261, Section 16.3, Request Validation]

5.3.4.7.4.1.14 The AS-SIP signaling appliances serving SIP end instruments MUST support the generating of a 483 (Too Many Hops) response code upon receiving a request [other than an OPTIONS request] in which the Max-Forwards header field has a value of zero. [RFC 3261, Section 16.3, Request Validation]

NOTE: If the method is OPTIONS, then the 483 response code is not sent, instead the requirement in RFC 3261 applies. [RFC 3261, Section 11, Querying for Capabilities]

5.3.4.7.4.1.15 The AS-SIP signaling appliances serving SIP end instruments SHOULD support the generating of a 485 (Ambiguous) response code if the Request-URI does not provide

sufficient information for the AS-SIP signaling appliance to determine the target set. [RFC 3261, Section 16.5, Determining Request Targets]

5.3.4.7.4.1.16 The AS-SIP signaling appliances serving SIP end instruments MUST support the forwarding of the server failure (5xx) response codes:

500 (Server Internal Error)	501 (Not Implemented)	502 (Bad Gateway)
503 (Service Unavailable)	504 (Server Timeout)	505 (Version Not Supported)
513 (Message Too Large) [RFC 3261]	580 (Precondition Failure) [RFC 3312]	

5.3.4.7.4.1.17 The AS-SIP signaling appliances serving SIP end instruments SHOULD generate and send upstream a 500 (Server Internal Error) response code when the only response received to a request is a 503 (Service Unavailable) response code. [RFC 3261, Section 16.7, Response Processing]

5.3.4.7.4.1.18 The AS-SIP signaling appliances serving SIP end instruments MUST support the forwarding of the global failures (6xx) response codes: 600 (Busy Everywhere), 603 (Decline), 604 (Does Not Exist Anywhere), and 606 (Not Acceptable).

5.3.4.7.4.2 AS-SIP Signaling Appliances Serving H.323 and/or Proprietary IP End Instruments

5.3.4.7.4.2.1 The AS-SIP signaling appliances serving H.323 and/or proprietary IP end instruments MUST support sending, receiving, and processing the provisional (1xx) response codes: 100 (Trying), 180 (Ringing), and 183 (Session Progress). [RFC 3261, Section 21.1, Provisional 1xx]

5.3.4.7.4.2.2 The AS-SIP signaling appliances serving H.323 and/or proprietary IP end instruments MUST support the successful (2xx) response codes: 200 (OK). [RFC 3261, Section 21.2, 200 OK, and 202 (Accepted)] [RFC 3515]

5.3.4.7.4.2.3 The AS-SIP signaling appliances serving H.323 and/or proprietary IP end instruments MAY be capable of operating as redirect servers and MAY support the following redirection (3xx) response codes: 300 (Multiple Choices), 301 (Moved Permanently), 302 (Moved Temporarily), and 305 (Use Proxy). [RFC 3261, Section 21.3, Redirection 3xxx]

5.3.4.7.4.2.4 The AS-SIP signaling appliances serving H.323 and/or proprietary IP end instruments MUST support the request failure (4xx) response codes:

400 (Bad Request)	401 (Unauthorized)	403 (Forbidden)
404 (Not Found)	405 (Method Not Allowed)	406 (Not Acceptable)
407 (Proxy Authentication Required)	408 (Request Timeout)	410 (Gone)
413 (Request Entity Too Large)	414 (Request-URI Too Long)	415 (Unsupported Media Type)
416 (Unsupported URI Scheme)	417 (Unknown Resource-Priority)	420 (Bad Extension)
421 (Extension Required)	422 (Session Interval Too Small)	423 (Interval Too Brief)
480 (Temporarily Unavailable)	481 (Call/Transaction Does Not Exist)	482 (Loop Detected)
483 (Too Many Hops)	484 (Address Incomplete)	485 (Ambiguous)
486 (Busy Here)	487 (Request Terminated)	488 (Not Acceptable Here)
491 (Request Pending)		

[RFC 3261, Section 21.4, Request Failure 4xx]

5.3.4.7.4.2.5 The AS-SIP signaling appliances serving H.323 and/or proprietary IP end instruments upon properly receiving a CANCEL for an INVITE MUST first send a 200 OK to the CANCEL and then follow up with a 487 (Request Terminated) to the INVITE.

5.3.4.7.4.2.6 The AS-SIP signaling appliances serving H.323 and/or proprietary IP end instruments MUST support the server failure (5xx) response codes:

500 (Server Internal Error) 501 (Not Implemented) 502 (Bad Gateway)

503 (Service Unavailable) 504 (Server Timeout) 505 (Version Not Supported)

513 (Message Too Large) 580 (Precondition Failure)
[RFC 3261, Section 21.5, Server Failure 5xx] [RFC 3312]

5.3.4.7.4.2.7 The AS-SIP signaling appliances serving H.323 and/or proprietary IP end instruments MUST support the global failures (6xx) response codes:

600 (Busy Everywhere) 603 (Decline) 604 (Does Not Exist Anywhere)

606 (Not Acceptable)

[RFC 3261, Section 21.6, Global Failures 6xx]

5.3.4.7.5 SIP Preconditions – SBU Network Only

5.3.4.7.5.1 The implementation of preconditions is optional for AS-SIP signaling appliances serving IP end instruments. [RFC 3312]

5.3.4.7.5.2 **[Conditional]** When an AS-SIP signaling appliance supports preconditions, the implementation must be in accordance with RFC 3312

5.3.4.7.5.3 **[Conditional]** When an AS-SIP signaling appliance supports preconditions, the activation of preconditions MUST be configurable so that the administrator of the device may enable or disable preconditions without removing the AS-SIP signaling appliance from service or losing state on existing calls or call requests

5.3.4.7.5.4 **[Conditional]** When an AS-SIP signaling appliance supports preconditions, the only required precondition-type is “qos”. [FY08-12]

5.3.4.7.5.5 **[Conditional]** When an AS-SIP signaling appliance supports preconditions, the segmented status type MUST be supported.

5.3.4.7.5. 6 **[Conditional]** When an AS-SIP signaling appliance supports preconditions, the end-to-end status type MAY be supported.

5.3.4.7.5.7 **[Conditional]** When an AS-SIP signaling appliance supports preconditions, the strength-tag MUST be set to "optional".

5.3.4.7.5.8 The AS-SIP signaling appliances serving IP end instruments that initiate an offer including one or more preconditions (and noting the strength-tag must be set to "optional") MUST include the option tag "precondition"in either a Supported header field or a Require header field. It is, however, RECOMMENDED that the Supported header field be used in this case. The lack of preconditions in the answer would indicate that the answerer did not support this extension. [RFC 3312, Integration of Resource Management and SIP, Section 11, October, 2002]

5.3.4.7.5.9 When an AS-SIP signaling appliance that does not support preconditions receives an offer including one or more preconditions and a Require header field with the option tag "precondition" then the AS-SIP signaling appliance MUST respond with a 420 (Bad Extension) response code having an Unsupported header with the option tag "precondition".

5.3.4.7.5.10 If the offering AS-SIP signaling appliance receives a 420 (Bad Extension) response code listing the option tag "precondition", then the default behavior for the AS-SIP signaling appliance is to retry the request and omit the precondition.

5.3.4.7.5.11 If the offering AS-SIP signaling appliance receives a 580 (Precondition Failure) response code, then the default behavior for the AS-SIP signaling appliance is to retry the request and omit the precondition.

5.3.4.7.5.12 **[Conditional]** When AS-SIP signaling appliances serving IP end instruments implement RFC 3312 for a call request, each local and remote AS-SIP signaling appliance MAY employ its own quality-of-service mechanism, including, but not limited to, RSVP and call counting.

5.3.4.7.5.13 The implementation of preconditions MUST be consistent with assured service precedence and preemption rules. In particular, when preconditions are applied to a precedence call request (i.e., priority or higher) and the preconditions cannot be met, except for the preemption of one or more lesser precedence calls and/or call requests, then the lesser precedence call(s) and/or call requests MUST be preempted.

NOTE: Please see UCR 2008, Section 5.3.4.10, Precedence and Preemption, for details on the precedence and preemption requirements.

An example of the AS-SIP segmented status type precondition call flow is found at Requirement 5.3.4.13.2.1.3 and an example of the AS-SIP end-to-end status type precondition call flow is found at Requirement 5.3.4.13.2.1.4.

5.3.4.7.5b SIP Preconditions – Classified Network Only

5.3.4.7.5b.1 Implementation of preconditions is mandatory for AS-SIP signaling appliances serving IP end instruments on the classified network. [RFC 3312]

5.3.4.7.5b.1.1 The activation of preconditions is the default operational mode for AS-SIP signaling appliances however AS-SIP signaling appliances MUST also be configurable so that the administrator of the device may enable or disable preconditions without removing the AS-SIP signaling appliance from service or losing state on existing calls or call requests

5.3.4.7.5b.2 At this time, the only required precondition-type is “qos”.

5.3.4.7.5b.3 The end-to-end status-type MUST be supported.

5.3.4.7.5b.4 The AS-SIP signaling appliances MUST employ the Resource Reservation Protocol (RSVP) as the network resource reservation mechanism.

5.3.4.7.5b.5 The strength-tag MUST be set to “mandatory.”

5.3.4.7.5b.6 The AS-SIP signaling appliances serving IP end instruments that initiate an offer, including one or more preconditions, MUST include a Require header field with the option tag “precondition”. [RFC 3312, Section 11, Option Tag for Preconditions]

5.3.4.7.5b.6.1 If the offering AS-SIP signaling appliance receives a 420 (Bad Extension) response code listing the option tag “precondition”, then the default behavior for the AS-SIP signaling appliance is to retry the request and omit the precondition.

5.3.4.7.5b.6.2 If the offering AS-SIP signaling appliance receives a 580 (Precondition Failure) response code, then the default behavior for the AS-SIP signaling appliance is to retry the request and omit the precondition.

5.3.4.7.5b.7 The AS-SIP signaling appliances are NOT required to support, or authorized to use, the segmented status type at the present time.

5.3.4.7.5b.8 The implementation of preconditions MUST be consistent with assured service precedence and preemption rules. In particular, when preconditions are applied to a precedence call request (i.e., priority or higher) and the preconditions cannot be met, except for the preemption of one or more lesser precedence calls and/or call requests, then the lesser precedence call(s) and/or call requests MUST be preempted.

NOTE: Please see UCR 2008, Section 5.3.4.10, Precedence and Preemption, for details on the precedence and preemption requirements.

An example of the AS-SIP end-to-end status type precondition call flow is found at Requirement 5.3.4.13.2.1.4 and an example of the AS-SIP segmented status type precondition call flow is found at Requirement 5.3.4.13.2.1.3.

5.3.4.7.6 SIP URI and Mapping of Telephony Number into SIP URI

5.3.4.7.6.1 **[Required]** When an AS-SIP signaling appliance receives a call request from a served IP end instrument intended for a destination outside the enclave in which the dialed number is from the DSN worldwide numbering plan, then the AS-SIP signaling appliance MUST ensure that the userinfo part of the SIP URI in the Request-URI field of the INVITE is the complete 10-digit DSN number.

5.3.4.7.6.1.1 **[Required]** In the event the dialed number received from the served IP end instrument is a DSN number having fewer than the full 10-digits, then the AS-SIP signaling appliance MUST prepend the three (3) area code digits (KXX) of the AS-SIP signaling appliance's local area code to create the full 10-digit DSN number.

5.3.4.7.6.1.2 **[Required]** In the event an AS-SIP signaling appliance receives an INVITE from a served SIP end instrument intended for a destination outside the enclave and having a tel URI, then the AS-SIP signaling appliance MUST convert the tel URI to a SIP URI whereby the userinfo part of the SIP URI is the full 10-digit DSN number.

5.3.4.7.6.1.3 **[Required]** The 10-digit DSN number MAY be followed by a phone-context descriptor consisting of a domain name (per RFC 3966).

5.3.4.7.6.1.4 **[Required]** A SIP URI derived from a telephone number (e.g., 10-digit DSN number) MUST have a "user=phone" field appended to the URI. In the event an AS-SIP signaling appliance receives a SIP URI from a served SIP EI that does not have the "user=phone" field then the AS-SIP signaling appliance SHALL append the "user=phone" field to the URI.

5.3.4.7.6.2 **[Required]** When an AS-SIP signaling appliance receives from another AS-SIP signaling appliance an INVITE with a Request-URI where the userinfo part is a full 10-digit DSN number either with or without a phone-context descriptor, the AS-SIP signaling appliance MUST be able to process the Request-URI field in order to forward the INVITE to the next appropriate AS-SIP signaling appliance or end instrument.

5.3.4.7.6.3 **[Required]** When an AS-SIP signaling appliance receives an emergency call request (e.g., 911, 112) (or a service code such as directory assistance (e.g., 411) or any other N11 service code) from a served IP end instrument and the emergency call request is to be sent outside the enclave over the DISN WAN, then the Request-URI field MUST be a SIP URI in which the userinfo part is 411 (or 911 or 112, etc.), which MUST include the phone-context parameter servicecode.dsn.mil, and to which MUST be appended the "user=phone" field.
It should be noted that all 911 calls are subject to network preemption and all 911 calls are subejec to endpoint preemption unless the empoint is non-preemptable.

NOTE: This requirement is meant to support the tactical scenario.

5.3.4.7.6.3.1 **[Required]** The phone number in the userinfo part of the SIP URI of the P-Asserted-Identity header is the default call back phone number for the 911 call. In the event the P-Asserted-Identity header is not present in the INVITE then the the userinfo part of the SIP URI of the From header is used as the call back phone number.

5.3.4.7.6.4 **[Required]** When an AS-SIP signaling appliance receives a call request from a served IP end instrument intended for the PSTN that is to be routed through the DSN network (as opposed to being routed directly to a PSTN gateway at the enclave), then the userinfo part of the SIP URI MUST be represented in global E.164 notation.

5.3.4.7.6.4.1 **[Required]** The format of a SIP URI that includes a global E.164 number in the userinfo part is:

sip:+<E.164number>@hostname;user=phone

where the E.164 number replaces <E.164number> including the left and right angle brackets

5.3.4.7.6.4.2 **[Required]** When the dialed number is an International number then the international number is placed after the "+" sign in the userinfo part of the SIP URI.

5.3.4.7.6.4.3 **[Required]** When the dialed number is a National significant number then the AS-SIP signaling appliance serving the calling IP end instrument is responsible for ensuring that the country code is prefixed to the dialed number and that an E.164 number is generated and placed after the "+" sign in the userinfo part of the SIP URI.

5.3.4.7.6.4.4 **[Required]** If the dialed number is a subscriber number that is to be routed through the DSN network (as opposed to being routed directly to a PSTN gateway at the enclave), then the AS-SIP signaling appliance that received the call request from the served IP end instrument MUST reject the call request. In the case of a SIP end instrument, the AS-SIP signaling appliance responds with a 484 Address Incomplete.

5.3.4.7.6.5 **[Required]** When an AS-SIP signaling appliance receives from another AS-SIP signaling appliance an INVITE with a Request-URI where the userinfo part is a global E.164 number, the AS-SIP signaling appliance MUST be able to process the Request-URI field in order to forward the INVITE to either:

- The next appropriate AS-SIP signaling appliance, or
- If the given AS-SIP signaling appliance is the interworking gateway, then conduct the SIP to ISDN or CCS7 signaling plane interworking of the SIP INVITE.
- A served EI

Following are three examples of the SIP URI of a Request-URI field of an outbound INVITE sent by the AS-SIP signaling appliance serving an IP end instrument toward the DISN WAN:

[Required] 10-digit DSN number:

sip:3154561223;phone-context=dsn.mil@pac.dsn.mil;user=phone
sip:3154561223@pac.dsn.mil;user=phone

[Required] 3-digit Service Code:

sip:911:phone-context=servicecode.dsn.mil@pac.dsn.mil;user=phone

5.3.4.7.7 64kbps Transparent Calls (Clear Channel)

5.3.4.7.7.1 [Required: Strategic Deployments – Conditional: Tactical Deployments] When an AS-SIP signaling appliance performs the Media Gateway Controller (MGC) function for a Media Gateway (MG), then the the AS-SIP signaling appliance MUST support the establishment of 64kbps unrestricted RTP bearer streams in accordance with IETF RFC 4040 "RTP Payload Format for a 64 kbit/s Transparent Call, April 2005".

5.3.4.7.7.1.1 When an AS-SIP signaling appliance (i.e., originating AS-SIP signaling appliance) receives a Q.931 SETUP message whose bearer capability information element indicates that the bearer is 64 kbps unrestricted then the AS-SIP signaling appliance MUST generate and send an outbound AS-SIP INVITE that includes the SDP parameters as specified in RFC 4040 as follows:

- The media ("m=") field is assigned the value audio. (NOTE: The media field is described in further detail in Requirement 5.3.4.9.3.1, Media ("m=") Field, of this document.)

- The attribute ("a=") field is assigned the value CLEARMODE/8000. (NOTE: The attribute field is described in further detail in Requirement 5.3.4.9.3.3, Attributes ("a=") Fields, of this document.)

- The a=ptime attribute and the a= maxptime attribute MAY be included in the SDP description. (NOTE: The attributes a=ptime and a=maxptime are described in further detail in Requirement 5.3.4.9.3.3.3 of this document.)

Example from RFC 4040:

```
m=audio 12345 RTP/AVP 97
a=rtpmap:97 CLEARMODE/8000
a=ptime:10
```

5.3.4.7.7.1.2 The originating AS-SIP signaling appliance MUST direct the Media Gateway to reserve the resources for the clear channel packetization/depacketization and to conduct the transparent relay of the 64kbps bearer stream using RTP upon completion of session establishment.

5.3.4.7.7.1.3 When an AS-SIP signaling appliance (i.e., terminating AS-SIP signaling appliance) (that is acting as a MGC for a Media Gateway) receives an AS-SIP INVITE intended for the TDM network where the SDP parameters have a media field = audio and an attribute field = CLEARMODE/8000, then the AS-SIP signaling appliance MUST create a Q.931 Setup message with a bearer capability information element indicating that the bearer is 64kbps unrestricted (depending on local policy).

5.3.4.7.7.1.4 The terminating AS-SIP signaling appliance MUST direct the Media Gateway to reserve the resources for the clear channel packetization/depacketization and to conduct the transparent relay of the 64kbps bearer stream using RTP upon completion of session establishment.

5.3.4.7.8 Transport of Route Code Information over AS-SIP

5.3.4.7.8.1 When an end instrument is served by an AS-SIP signaling appliance, then the AS-SIP signaling appliance is responsible for ensuring that the route code information dialed by the user is represented in the outbound INVITE message sent over the interface toward the DISN

WAN by appending the tgrp parameter and the trunk-context parameter to the userinfo part of the SIP URI of the Request URI as described in this subsection. [RFC 4904]

5.3.4.7.8.1.1 Table 5.3.4-5 provides the correspondence between the Route Code entered during user dialing and the associated value for the tgrp parameter and the trunk-context parameter.

Table 5.3.4-5. Route Code Digits Input by Caller and Corresponding tgrp, trunk-context

ROUTE CODE (ENTERED BY USER)	ROUTE CODE USE	tgrp	trunk-context
10	Voice Call (default)	N/A (see note)	N/A
11	Circuit Switched Data	tgrp=ccdata	trunk-context=dsn.mil
12	Satellite Avoidance	tgrp=nosat	trunk-context=dsn.mil
NOTE: 10 represents a voice call and is the default route code. Do not append a tgrp parameter and a trunk-context parameter to the Request URI of calls where the Route Code has the value 10. The absence of the tgrp parameter and trunk-context parameter is intended to signify to AS-SIP signaling appliances that the instant INVITE represents a voice call.			

5.3.4.7.8.2 When an end instrument is served by an AS-SIP signaling appliance and the user initiates a hotline call, then the AS-SIP signaling appliance MUST append a tgrp parameter and a trunk-context parameter to the userinfo part of the SIP URI of the Request URI of the INVITE message where the values are defined in Table 5.3.4-6.

Table 5.3.4-6. tgrp, trunk-context Parameters Inserted for Hotline Calls

ROUTE CODE	ROUTE CODE USE	tgrp	trunk-context
5	Hotline (off-hook) voice grade (inserted by AS-SIP signaling appliance)	tgrp=hotline	trunk-context=dsn.mil
6	Hotline (off-hook) data grade (inserted by AS-SIP signaling appliance)	tgrp=hotline-ccdata	trunk-context=dsn.mil
NOTE: The user does not dial these route codes. The AS-SIP signaling appliance shall automatically dial hotline calls when an off-hook condition occurs and convey the appropriate tgrp parameter and trunk-context parameter as specified in this table			

Example:

sip:3153435335;phone-context=dsn.mil;tgrp=hotline;trunk-context=dsn.mil@patch.dsn.mil;user=phone

5.3.4.7.8.3 When an AS-SIP signaling appliance receives an INVITE where the Request-URI includes a tgrp parameter and trunk-context parameter appended to the userinfo part of the SIP

URI then the AS-SIP signaling appliance MUST preserve the tgrp parameter and trunk-context parameter when forwarding the INVITE to another AS-SIP signaling appliance.

5.3.4.7.8.4 For the reader's convenience, Table 5.3.4-7 shows the mapping the SIP tgrp value to the ISDN Q.931 information element field / bearer capability.

Table 5.3.4-7. SIP tgrp to ISDN Q.931 Mapping

SIP TGRP=VALUE	Q.931 IE / BEARER CAPABILITY
No label	Voice Bearer Capability (BC)
tgrp=ccdata	56/64k circuit-mode data
tgrp=nosat	N/A – not defined
tgrp=hotline	Off Hook Indicator of voice, speech BC
tgrp=hotline-ccdata	Off Hook Indicator of data, 56/64k cmd BC

5.3.4.7.9 CAL General Requirements (Note: CAL Paragraphs apply to Classified only)

5.3.4.7.9.1 AS-SIP signaling appliances MUST receive, process, and forward an initial INVITE (or a re-INVITE or UPDATE) having a CAL header.

5.3.4.7.9.2 AS-SIP signaling appliances MUST generate a CAL header when creating an initial INVITE upon receipt of an outbound call request from a served non-SIP IP end instrument. AS-SIP signaling appliances MUST also generate a CAL header when creating a mid-call INVITE or UPDATE on behalf of a served non-SIP IP end instrument when the outbound request indicates a change to the desired access level.

5.3.4.7.9.3 AS-SIP signaling appliances MUST be capable of generating CALs with fixed access mode and CALs with variable access mode.

5.3.4.7.9.4 AS-SIP signaling appliances MUST be capable of receiving and processing CAL headers that request fixed access mode and CAL headers that request variable access mode and when an AS-SIP signaling appliance receives a CAL header with a mode that is different than the locally configured mode then the resulting mode must always be "fixed."

5.3.4.7.9.5 AS-SIP signaling appliances that receive an INIVITE Request (or re-INVITE or UPDATE) with a CAL header whose local-access-level cannot be resolved to an acceptable value MUST generate a 418 (Incompatible CAL) response that SHOULD include a CAL header where the reflected-access-level is set to the local-access-value from the received CAL header and the local-access-value is set to the access-level supported by the AS-SIP signaling appliance that is responding with the 418.

5.3.4.7.9.6 All intermediate AS-SIP signaling appliances in a SIP call signaling flow MUST receive, process, and forward 200 responses with CAL headers. In particular, the intermediate AS-SIP signaling appliances MUST attempt to resolve the local-access-level of the CAL header with the locally configured access value for the next routing domain and modify the local-access-field accordingly if necessary or set the local-access-field to 0 when efforts to resolve fail.

AS-SIP Signaling Appliances Serving Outbound Call Requests from Served IP End Instruments

5.3.4.7.9.7 Upon receipt of an initial call request from a served non-SIP IP end instrument, an AS-SIP signaling appliance MUST generate an INVITE with a CAL header (see Requirement 5.3.4.7.9.13 for syntax of CAL header) unless the requested access-level is not authorized for the end instrument/user and the intended mode is fixed mode (see Requirement 5.3.4.7.9.7.1).

5.3.4.7.9.7.1 When the requested access-level is NOT an authorized value for the end instrument/user then:

- If the intended mode is variable the AS-SIP signaling appliance generates an INVITE with a CAL header that resolves the local-access-level to the closest value that is authorized for the served non-SIP IP end instrument/user.

- If the intended mode is fixed the AS-SIP signaling appliance returns a 418 response.

5.3.4.7.9.8 In the absence of an indication in the call request from the non-SIP IP end instrument as to the desired access-level, local policy at the AS-SIP signaling appliance will determine what access-level to place in the local-access-level field.

5.3.4.7.9.9 In the absence of an indication in the call request from the non-SIP IP end instrument as to the desired mode, local policy at the AS-SIP signaling appliance will determine whether to assign fixed or variable mode and will then place the selected value in the access-mode field.

5.3.4.7.9.10 Upon receipt of a mid-call outbound request from a served non-SIP IP end instrument indicating a change to the desired access level, an AS-SIP signaling appliance MUST generate a re-INVITE or UPDATE with a CAL header unless the requested access-level is not authorized for the end instrument/user and the intended mode is fixed mode (see Requirement 5.3.4.7.9.10.1).

5.3.4.7.9.10.1 When the requested access-level for the mid-call request is NOT an authorized value for the end instrument/user then the AS-SIP signaling appliance returns a 418 response.

5.3.4.7.9.11 SIP end instruments SHOULD include a CAL header to convey the desired access level in initial outbound INVITEs.

5.3.4.7.9.11.1 When the local-access-level in the CAL header received by the AS-SIP signaling appliance in the outbound INVITE from a served SIP end instrument is NOT an authorized value for the end instrument/user then:

- If the mode is variable the AS-SIP signaling appliance resolves the local-access-level to the closest value that is authorized for the served non-SIP IP end instrument/user.

- If the mode is fixed the AS-SIP signaling appliance returns a 418 response.

5.3.4.7.9.11.2 If the initial INVITE received from the served SIP end instrument does not include a CAL header then the AS-SIP signaling appliance will add a CAL header and will apply local policy to determine the values used to populate the local-access-level field and the access-mode field.

5.3.4.7.9.12 SIP end instruments MUST send a CAL header in mid-call outbound INVITEs or UPDATEs if there is a need to change the access level.

5.3.4.7.12.1 When the local-access-level in the CAL header received by the AS-SIP signaling appliance in the mid-call outbound INVITE or UPDATE from a served SIP end instrument is NOT an authorized value for the end instrument/user then the AS-SIP signaling appliance returns a 418 response.

5.3.4.7.9.13 The syntax of the CAL header (and an example of the CAL header) is:

```
Confidential-Access-Level   = "Confidential-Access-Level" HCOLON local-access-level SEMI
                              reflected-access-level
local-access-level          = (access-level SEMI access-mode)
reflected-access-level      = ("ref" EQUAL access-level SEMI reflected-mode)
access-level                = (1*2DIGIT ; 0 to 99)
access-mode                 = ("mode" EQUAL mode-param)
reflected-mode              = ("rmode" EQUAL mode-param)
mode-param                  = (fixed / variable)
```

The following are examples, showing the Confidential-Access-Level header.

Confidential-Access-Level: 4;mode=variable;ref=2;rmode=fixed
Confidential-Access-Level: 50;mode=variable;ref=40;rmode=variable

5.3.4.7.9.14 All AS-SIP signaling appliances serving non-SIP IP end instruments MUST include the 'confidential-access-level' option tag in both the Require and Proxy-require headers when sending an initial outbound INVITE on behalf of the IP end instrument. (NOTE: A duplicate of this requirement is located in Section 5.3.4.7.3, Header Fields.)

5.3.4.7.9.14.1 In the case of SIP end instruments, the initial INVITE sent by the SIP end instrument SHOULD include the 'confidential-access-level' option tag in both the Require and Proxy-require headers. If the initial INVITE fails to include the "confidential-access-level" option tag in both the Require and Proxy-require headers the AS-SIP signaling appliance will add the missing header(s) and option tag.

5.3.4.7.9.15 All AS-SIP signaling appliances serving non-SIP IP end instruments MUST process the CAL header in a 200 response and SHOULD ensure that the reflected-access-level is conveyed to the caller. It is also RECOMMENDED that the name of the callee also be conveyed to the caller (if present in the 200 OK).

5.3.4.7.9.15.1 In the case of SIP end instruments the SIP end instrument MUST process the CAL header in a 200 response. The AS-SIP signaling appliance SHOULD ensure that the reflected-access-level is conveyed to the caller. It is also recommended that the name of the callee be conveyed to the caller (if present in the 200 OK).

5.3.4.7.9.16 When an AS-SIP signaling appliance receives a 418 response the AS-SIP signaling appliance is responsible for ensuring that the caller is notified that the call failed due to an inability to meet the caller's CAL requirement.

AS-SIP Signaling Appliances Receiving Inbound Invites for Served IP End Instruments

5.3.4.7.9.17 Upon receipt of an INVITE with a CAL header (or any re-INVITE or UPDATE that includes a CAL header) an AS-SIP signaling appliance serving a non-SIP IP end instrument that is the intended recipient of the message MUST process the CAL header in accordance with the procedures set forth in Requirements 5.3.4.7.9.17.1.1–5.3.4.7.9.17.1.6.

NOTE: When the INVITE with CAL header is intended for a SIP end instrument then the SIP end instrument will process the CAL header instead of the AS-SIP signaling appliance to which the SIP end instrument is assigned. A description of the procedure is provided as follows:

5.3.4.7.9.17.1 The AS-SIP signaling appliance receiving the request on behalf of the non-SIP IP end instrument (or the SIP end instrument) determines whether the received access-mode is fixed or variable.

5.3.4.7.9.17.1.1 If the access-mode is fixed and the local-access-level from the CAL header is supported by the configured CAL for the end instrument then the AS-SIP signaling appliance (or SIP end instrument) will reply with a 200 having a CAL header with the CAL value and fixed mode in the reflected-access-level. The AS-SIP signaling appliance SHOULD ensure that an indication of the access level is provided to the intended recipient of the call.

5.3.4.7.9.17.1.2 If the access-mode is fixed and the configured CAL for the end instrument does not match the value in the local-access-level of the received CAL header then the AS-SIP signaling appliance responds with a 418 (Incompatible CAL).

5.3.4.7.9.17.1.3 If: the access-mode is variable AND the access value in the CAL header can be resolved with the locally configured access value AND the locally configured access value can also be resolved with the access value for the routing domain in the return path AND the AS-SIP signaling appliance deems the 2 resolved values to be compatible THEN the resolved value for the inbound path is placed in the reflected-access-level field of the CAL header that will be sent in the 200 response and the resolved value for the outbound path will be placed in the local-access-level field of the CAL header. The AS-SIP signaling appliance SHOULD ensure that an indication of the access level is provided to the intended recipient of the call.

5.3.4.7.9.17.1.4 If the access-mode is variable AND the AS-SIP signaling appliance [or SIP end instrument] can't resolve the local-access-value in the received INVITE header with the locally configured value then the AS-SIP signaling appliance (or SIP end instrument) returns a 418 (Incompatible CAL) response.

5.3.4.7.9.17.1.5 If the access-mode is variable AND the access value in the CAL header can be resolved with the locally configured access value AND the locally configured access value can also be resolved with the access value for the routing domain in the return path AND the AS-SIP signaling appliance (or SIP end instrument) deems the 2 resolved values to be incompatible BUT local policy determines that the call should continue THEN the AS-SIP signaling appliance (or SIP end instrument) sends a 200 response that includes the CAL header wherein the local-access-level receives the value 0. The AS-SIP signaling appliance SHOULD ensure that an indication of the access level is provided to the intended recipient of the call.

5.3.4.7.9.17.1.6 If the access-mode is variable AND the access value in the CAL header can be resolved with the locally configured access value AND the locally configured access value can also be resolved with the access value for the routing domain in the return path AND the AS-SIP signaling appliance (or SIP end instrument) deems the 2 resolved values to be incompatible THEN the AS-SIP signaling appliance (or SIP end instrument) responds with a 418 (Incompatible CAL) if local policy determines the call should NOT continue.

5.3.4.7.9.18 Intermediary Tier0 SSs

When an intermediary Tier0 SS receives an INVITE (or re-INVITE or UPDATE) with a CAL header, the Tier0 SS MUST process the Request in accordance with the following procedure:~~:~~

5.3.4.7.9.18.1 The local-access-value in the CAL header is resolved against the locally configured access value for the next routing domain as follows:

5.3.4.7.9.18.1.1 For fixed mode if the local-access-level from the CAL header is a supported access value for the next routing domain then the INVITE is forwarded to the next AS-SIP signaling appliance. Otherwise (i.e., if the value of the local-access-level is not supported) then the Tier0 SS MUST reply with a 418 (Incompatible CAL).

5.3.4.7.9.18.1.2 For variable mode if the access level can be resolved to an acceptable level, the local-access-level of the CAL header is updated with the new value (if different from the received value) and the Request is forwarded to the next AS-SIP signaling appliance. The procedure for resolving a variable mode local access value in the received CAL header with a locally configured value is as follows:

> Access level values are used programmatically by each UA or proxy involved in the session to provide a resolved value based on the combination of the incoming access level value and a locally configured value. .. .. When variable mode is used, an incoming access level must be resolved against a locally configured value to provide a result. An example implementation might render this in the form of an x-y matrix vector where the x value is taken from the incoming header, the y value is taken from the locally configured value for the destination resource and the vector is the resolved value. The actual implementation may be done in different ways but should allow the flexibility of having programmable results based on the intersection of incoming access level and configured access level.

5.3.4.7.9.18.1.3 For variable mode if the Tier0 SS cannot resolve to an acceptable access-level however local policy determines the call should continue, then the Tier0 SS assigns the value 0 to the local-access-level and sends the Request to the next AS-SIP signaling appliance.

5.3.4.7.9.18.1.4 For variable mode if the Tier0 SS cannot resolve to an acceptable access-level and local policy determines the call should NOT continue then the Tier0 SS responds with a 418 (Incompatible CAL).

5.3.4.7.9.19 When an intermediary Tier0 SS receives a 200 with a CAL header, the Tier0 SS resolves the value in the local-access-level with the locally configured routing domain:

5.3.4.7.9.19.1 If the local-access-level value from the CAL header and the access-value for the locally configured routing domain in the response path can be resolved to an acceptable value, then the resolved access value (and mode, if necessary) are placed into the local-access-level.

5.3.4.7.9.19.2 If the local-access-level value the access-value for the locally configured routing domain in the response path CANNOT be resolved to an acceptable value then the local-access-value in the CAL header is set to 0.

5.3.4.8 SIP Session Keep-Alive Timer

The purpose of the SIP Session Keep-Alive Timer paragraphs is to actively signal call termination where at least one EI is no longer partaking in the session.

5.3.4.8.1 AS-SIP Signaling Appliances

5.3.4.8.1.1 The AS-SIP signaling appliances MUST support the keep-alive mechanism for SIP sessions. [RFC 4028]

5.3.4.8.1.2 Reserved

5.3.4.8.1.3 The AS-SIP signaling appliances MUST support the generating, receiving, and processing of the Session-Expires and Min-SE header fields. The RECOMMENDED value for the Session-Expires header field is 1800. The value for the Min-SE header field MUST be >= 90. [RFC 4028]

5.3.4.8.1.4 The AS-SIP signaling appliances MUST support the 422 (Session Interval Too Small) response code. [RFC 4028]

5.3.4.8.1.5 The AS-SIP signaling appliances MUST support the option tag “timer” for use with the Supported and Require header fields, however, an AS-SIP signaling appliance acting as a UAC or a SIP EI acting as a UAC MUST NOT place the “option tag “timer’ in either a Require header or a proxy-require header. [RFC 4028]

5.3.4.8.1.6 The AS-SIP signaling appliances SHOULD use the UPDATE method (as opposed to the INVITE method) to perform subsequent session refreshes in order to minimize the processing impact.

5.3.4.8.1.7 The UPDATE method used to perform subsequent session refreshes SHOULD NOT include an SDP offer in order to minimize the processing impact.

5.3.4.8.1.8 When an AS-SIP signaling appliance receives an outbound request from a served H.323 or proprietary IP end instrument, then the AS-SIP signaling appliance MUST operate in accordance with the UAC behavior (when responsible for performing the refresh). [RFC 4028, Sections: 7.1, Generating an Initial Session Refresh Request; 7.2, Processing a 2xx Response; 7.3, Processing a 422 Response; 7.4, Generating Subsequent Session Refresh Requests; and 10, Performing Refreshes]

5.3.4.8.1.9 When an AS-SIP signaling appliance receives an outbound request from a served SIP end instrument then:

5.3.4.8.1.9.1 If the SIP end instrument supports the keep-alive mechanism [RFC 4028], the AS-SIP signaling appliance MUST operate in accordance with the proxy behavior. [RFC 4028, Section 8, Proxy Behavior] The AS-SIP signaling appliance MUST meet the requirements set forth in RFC 4028. [RFC 4028, Sections 8.1, Processing of Requests; 8.2, Processing of Responses; and 8.3, Session Expiration]

5.3.4.8.1.9.2 If the SIP end instrument does NOT support the keep-alive mechanism [RFC 4028], the AS-SIP signaling appliance MUST operate in accordance with the UAC behavior (when responsible for performing the refresh). [RFC 4028, Sections 7.1, Generating an Initial Session Refresh Request; 7.2, Processing a 2xx Response; 7.3, Processing a 422 Response; 7.4, Generating Subsequent Session Refresh Requests; and 10, Performing Refreshes]

5.3.4.8.1.10 When an AS-SIP signaling appliance receives a call request from another AS-SIP signaling appliance~~,~~ and the destination is a served H.323 or proprietary IP end instrument, then the AS-SIP signaling appliance MUST operate in accordance with the UAS behavior (when responsible for performing the refresh). [RFC 4028 Sections 9, UAS Behavior, and 10, Performing Refreshes]

5.3.4.8.1.11 **[FY 2008-2012]** When an AS-SIP signaling appliance receives a call request from another AS-SIP signaling appliance~~,~~ and the destination is a served SIP end instrument, then:

5.3.4.8.1.11.1 If the SIP end instrument supports the keep-alive mechanism [RFC 4028], the AS-SIP signaling appliance MUST operate in accordance with the proxy behavior set forth in RFC 4028. [RFC 4028, Section 8, Proxy Behavior] The AS-SIP-signaling appliance MUST meet the requirements set forth in RFC 4028. [RFC 4028, Sections 8.1, Processing of Requests; 8.2, Processing of Responses; and 8.3, Session Expiration]

5.3.4.8.1.11.2 If the SIP end instrument does NOT support the keep-alive mechanism [RFC 4028], the AS-SIP signaling appliance MUST operate in accordance with the UAS behavior (when responsible for performing the refresh). [RFC 4028, Sections 9, UAS Behavior, and 10, Performing Refreshes]

NOTE: The AS-SIP signaling appliance serving a SIP end instrument is charged with knowing whether the SIP end instrument supports the RFC 4028 session timer. It is assumed that the AS-SIP signaling appliance acquires this information as part of the SIP end instrument registration process or by configuration. In the alternative, the AS-SIP signaling appliance may obtain this information by other means such as by sending an INVITE with the Require header and the option tag "timer" to the SIP end instrument, which will reply with either a Supported header with the option tag "timer" or a 420 (Bad Extension) and an Unsupported header with the option tag "timer".

5.3.4.8.1.12 **[FY 2012]** All AS-SIP end instruments MUST support the keep-alive mechanism. [RFC 4028]

5.3.4.9 Session Description Protocol

5.3.4.9.1 Session Description

5.3.4.9.1.1 "A session description consists of a session-level description (details that apply to the whole session and all media streams) and optionally several media-level descriptions (details that apply to a single media stream)." [RFC 2327, Section 6, SDP Specification]

5.3.4.9.1.2 When SDP information is present in a SIP message, the SIP message MUST have a content-type header having the MIME Content-Type "application/sdp".

Content-Type: application/sdp

5.3.4.9.1.3 The SDP parser in the AS-SIP signaling appliance MUST be able to accept and handle without error any SDP line types even if the application ignores the contents. [RFC 2327, Section 6, SDP Specification]

5.3.4.9.1.4 The SDP parser in the AS-SIP signaling appliance MUST completely ignore any SDP session description that contains a "type" letter that it does not understand. A UAS encountering this situation SHOULD return a 488 (Not Acceptable Here) final response code, preferably including a Warning SIP header field with a 307 (Warning) response code.

5.3.4.9.1.5 The session-level description of the SDP session description MUST include the following four mandatory line types and MUST appear in the following order: [RFC 2327]

v=
o=
s=
t=

NOTE: When any of the optional line types are included in the session level section of the session description they MUST also be placed in accordance with the relative ordering defined in RFC 4566.

5.3.4.9.1.6 Use of the "p="or "e=" line type in the session-level description is optional. [RFC 4566]

5.3.4.9.1.7 The session-level section of the session description is followed by zero or more media-level sections. Each media-level description starts with an "m=" line, and is terminated by either the next "m=" line or by the end of the session description. An individual media description may have any number of attributes ("a=" fields), which are media specific. [RFC 2327]

5.3.4.9.1.8 The connection ("c=") line MAY be placed at the session-level description, the media-level description, or both description levels. [RFC 2327]

5.3.4.9.1.9 When the connection ("c=") line is placed in the session-level description, it applies to all media of the session unless overridden by connection information in the media-level description. [RFC 2327]

5.3.4.9.1.10 If the connection ("c=") line is not present in the session-level description, then it MUST be present in each media-level description in the SDP session description. [RFC 2327]

5.3.4.9.1.11 The attribute mechanism ("a=") is optional and MAY be placed at the session-level description, the media-level description, or both description levels. [RFC 2327]

5.3.4.9.1.12 When the attribute mechanism ("a=") is placed in the session-level description, it applies to all media of the session unless overridden by attribute information of the same name in the media-level description. [RFC 2327]

5.3.4.9.2 Session-Level Description

The session-level description consists of a protocol version line, an origin line, a session name line, and a time line.

5.3.4.9.2.1 Protocol Version ("v=") Line

v=0

5.3.4.9.2.1.1 The "v=" line MUST be set to zero.

5.3.4.9.2.2 Origin ("o=") Line

o=<username> <session id> <sess-version> <network type> <address type> <address>

5.3.4.9.2.2.1 The <username> MUST NOT contain spaces and can be set to "-".

5.3.4.9.2.2.2 The numeric value of the <session id> MUST be representable with a 64-bit signed integer. [RFC 3264, Section 5, Generating the Initial Offer]

5.3.4.9.2.2.3 The <session id> SHOULD be set to a Network Time Protocol (NTP) timestamp in integer format, reflecting the time of the original creation of the session description. [RFC 2327, Section 6, SDP Specification]

5.3.4.9.2.2.4 The numeric value of the <sess-version> in the origin ("o=") line MUST be representable with a 64-bit signed integer. [RFC 3264, Section 5, Generating the Initial Offer]

5.3.4.9.2.2.5 "The initial value of the version MUST be less than (2**62)-1, to avoid rollovers." [RFC 3264, Section 5, Generating the Initial Offer]

5.3.4.9.2.2.6 The <sess-version> SHOULD be set to an NTP timestamp in integer format. [RFC 2327, Section 6, SDP Specification]

5.3.4.9.2.2.7 Every time a modification is made to the session data the <sess-version> MUST be incremented by one. [RFC 2327, Section 6, SDP Specification]

5.3.4.9.2.2.8 The <network type>, <address type>, and <address> SHOULD identify the SIP host that originates the session description, even if the description relates to a different host (for example, a media gateway). Following this convention avoids having to change the originator value if the media flows are redirected. A consequence of this recommendation is that there is no necessary relationship between the host identification on the origin ("o=") line and addresses given on a connection ("c=") line.

5.3.4.9.2.2.9 The first offer sent in a SIP session is an original session description, originated at the offering end. If the answer is otherwise the same as the offer (including the addressing information), RFC 3264, Section 6 says that the origin ("o=") line can also remain identical. This is an unlikely circumstance. In the more usual case, the answer has different addresses at least reflecting that end of the media flow. An initial answer that is different from an initial offer MUST be viewed as an original session description, originated by the answering end. This means that the answer MUST contain a new origin ("o=") line, constructed from the point of view of the answering SIP host. [RFC 3264, Section 6, Generating the Answer]

5.3.4.9.2.2.10 After the initial offer-to-answer exchange, if either end passes a session description to the other (whether in an offer or an answer) that is unchanged from what it last sent, the origin ("o=") line MUST be the same as previously sent. If there is any change, RFC 3264 requires that the <version> MUST be incremented by one while the rest of the origin ("o=") line remains unchanged. [RFC 3264, Section 8, Modifying the Session]

5.3.4.9.2.3 Session Name ("s=") Line

s= -

The session name ("s=") line SHOULD be set to "-". [RFC 3264, Section 5, Generating the Initial Offer]

5.3.4.9.2.4 Time ("t=") Line

t=0 0

The time ("t=") line SHOULD be set to "0 0". [RFC 3264, Section 5, Generating the Initial Offer]

5.3.4.9.3 Media Description

The media description consists of one or more media ("m=") fields and subfields.

5.3.4.9.3.1 Media ("m=") Field

m=<media> <port> <protocol> <format>

5.3.4.9.3.1.1 A session description MAY contain a number of media descriptions.

5.3.4.9.3.1.2 Each media description starts with an "m=" field and is terminated by the next "m=" field, or by the end of the session description. A media field has subfields.

5.3.4.9.3.1.2.1 The first subfield <media> is the media type (for example, audio and video). [RFC 2327, Section 6, SDP Specification]

5.3.4.9.3.1.2.2 The second subfield <port> is the transport port to which the media stream is sent. [RFC 2327, Section 6, SDP Specification]

5.3.4.9.3.1.2.3 The third subfield <protocol> is the transport protocol. For example, Real-Time Transport Protocol (RTP)-Audio/Video Profile (AVP) denotes RTP used under the RTP Profile for Audio and Video Conferences. [RFC 2327, Section 6, SDP Specification]

5.3.4.9.3.1.2.4 The fourth and subsequent subfields <format> are a media format description. [RFC 2327, Section 6, SDP Specification] For example,

m=audio 49170 RTP/AVP 0

5.3.4.9.3.2 Connection Data ("c=") Field

c=<nettype> <addrtype> <connection-address>

5.3.4.9.3.2.1 The first subfield <nettype> is the network type. Initially, this specification allows only "IN." [RFC 2327, Section 6, SDP Specification]

5.3.4.9.3.2.2 The second subfield <addrtype> is the address type. This specification supports the use of IPv4 [RFC 2327] or IPv6 [RFC 3266].

5.3.4.9.3.2.3 The third subfield <connection-address> is the connection address. [RFC 2327, Section 6, SDP Specification]

5.3.4.9.3.2.4 When the <addrtype> is IPv4 and the <connection-address> is a unicast address, then the format of the connection address will use the standard IPv4 decimal dotted notation.

5.3.4.9.3.2.5 The slash notation defined for multicast group addresses MUST NOT be used with unicast addresses. [RFC 2327, Section 6, SDP Specification] For example,

IN IP4 118.2.36.42

5.3.4.9.3.2.6 **[FY2012]** When the <addrtype> is IPv4 and the <connection-address> is a multicast group address, then the multicast connection address MUST have a time to live (TTL) value appended to the address using a slash as a separator. [RFC 2327, Section 6, SDP Specification] For example,

IN IP4 224.2.3.5/127

5.3.4.9.3.2.7 **[FY2012]** For multicast group addresses, the following notation is permitted and AS-SIP signaling appliances MUST support processing and MAY support generating the following notation: [RFC 2327, Section 6, SDP Specification]

<base multicast address> <ttl> <number of addresses>

where the *number of addresses* refers to the contiguous assignment of multicast addresses above the *base multicast address*

Example:

c=IN IP4 224.2.13.5/127/3

This is the same as including multiple "c=" lines, for example,

c=IN IP4 224.2.13.5/127
c=IN IP4 224.2.13.6/127
c=IN IP4 224.2.13.7/127

5.3.4.9.3.2.8 Reserved.

5.3.4.9.3.2. Reserved.

5.3.4.9.3.2.10 Reserved.

5.3.4.9.3.2.11 Reserved.

5.3.4.9.3.2.12 Reserved.

5.3.4.9.3.2.13 Multiple addresses or connection ("c=") lines MAY be specified in a media description. [RFC 2327, Section 6, SDP Specification]

5.3.4.9.3.2.14 Only one connection ("c=") line is permitted at the session description level. [RFC 2327, Section 6, SDP Specification]

5.3.4.9.3.3 Attributes ("a=") Fields

a=

5.3.4.9.3.3.1 "Attributes are the primary means for extending SDP. Attributes may be defined to be used as "session-level" attributes, "media-level" attributes, or both. A media description may

have any number of attributes ("a=" fields) which are media specific. These are referred to as "media-level" attributes and add information about the media stream. Attribute fields can also be added before the first media field; these "session-level" attributes convey additional information that applies to the conference as a whole rather than to individual media; …" [RFC 2327, Section 6, SDP Specification]

5.3.4.9.3.3.2 The SDP parser in the AS-SIP signaling appliance MUST be able to accept and handle any attribute ("a=") field without error, even if it does not recognize the attribute. An unrecognized attribute MUST be ignored rather than treated as an error case. If the unrecognized attribute was sent in an SDP offer, it MUST NOT appear in the answer.

5.3.4.9.3.3.2.1 In this specification, the following attributes are used:

```
a=recvonly
a=sendrecv
a=sendonly
a=rtcp:<port>
a=rtpmap:<payload type> <encoding name>/<clock rate> [/<encoding parameters>]
a=curr:<precondition-type> <status-type> <direction-tag>
a=des:<precondition-type> <strength-tag> <status-type> <direction-tag>
a=conf:<precondition-type> <status-type> <direction-tag>
```

5.3.4.9.3.3.2.2 The rtpmap attribute maps from an RTP payload type number (as used in an "m=" line) to an encoding name denoting the payload format to be used.

Example 1: [RFC 4566]

```
m=audio 49232 RTP/AVP 98
a=rtpmap:98 L16/16000/2
```

Example 2: [RFC 4566]

```
m=audio 49230 RTP/AVP 96 97 98
a=rtpmap:96 L8/8000
a=rtpmap:97 L16/8000
a=rtpmap:98 L16/11025/2
```

5.3.4.9.3.3.2.3 The codec formats (as depicted in example 2 above) are listed in the order of preference from the most preferred codec to the least preferred codec.

5.3.4.9.3.3.2.4 The “a=curr”, “a=des”, and “a=conf” media level SDPattributes are used in conjunction with preconditions as defined in RFC 3312.

Example:

```
m=audio 20000 RTP/AVP 0
a=curr:qos local none
a=curr:qos remote none
a=des:qos mandatory local sendrecv
a=des:qos mandatory remote sendrecv
a=curr:qos e2e none
a=des:qos optional e2e sendrecv
```

5.3.4.9.3.3.3 In this specification, the following attributes SHOULD be supported:

```
a=ptime:<packet time>
a=maxptime:<maximum packet time>
a=fmtp:<format> <format specific parameters>
```

5.3.4.9.3.3.3.1 The a=ptime:<packet time> attribute gives the length of time in milliseconds represented by the media in a packet. [RFC 2327]

5.3.4.9.3.3.3.2 The a=maxptime:<maximum packet time> attribute provides the maximum amount of media that can be encapsulated in each packet, expressed in milliseconds. [RFC 4566]

5.3.4.9.3.3.3.3 The a=fmtp:<format> <format specific parameters> attribute allows parameters, specific to a particular format, to be conveyed in a way that the SDP does not have to understand them.

5.3.4.9.3.4 Bandwidth (“b=”) Field

```
b=<bwtype>:<bandwidth>
```

5.3.4.9.3.4.1 The bandwidth (“b=”) field denotes the proposed bandwidth to be used by the session or media.

5.3.4.9.3.4.2 On the session level, the bandwidth (“b=”) field represents a total bandwidth figure for all media at all sites.

5.3.4.9.3.4.3 On the media level, the bandwidth ("b=") field is required for every video media ("m=") line.

5.3.4.9.3.4.4 On the media level, the bandwidth ("b=") field is NOT required for audio media ("m=") lines.

5.3.4.9.3.4.5 When used in the session level, the <bwtype> subfield shall be Application-Specific Maximum (AS).

5.3.4.9.3.4.6 When used in the media level, <bwtype> subfield shall be Transport Independent Application-Specific (TIAS) [RFC 3890].

5.3.4.9.3.4.7 The <bandwidth> subfield is interpreted as kilobits per second.

5.3.4.9.3.5 Bandwidth Modifier Application Rules

5.3.4.9.3.5.1 When there are multiple audio codecs in a single "m=" line, the bandwidth modifier ("b=TIAS") MAY be present and, if present, MUST reflect the largest bit rate that those codecs can support.

5.3.4.9.3.5.2 When there are multiple audio codecs in a single "m=" line and it is necessary to indicate the bitrate for particular audio codecs then an "a=fmtp:' format attribute will be associated with each audio codec to indicate the applicable bitrate.

Example:

```
m=audio 15134 RTP/AVP 102 0 97 18
b=TIAS:64000
a=rtpmap:102 G7221/16000
a=fmtp:102 bitrate=32000
a=rtpmap:0 PCMU/8000
a=rtpmap:97 SIREN14/16000
a=fmtp:97 bitrate=24000
a=rtpmap:18 G729A/8000
```

NOTE: The audio codecs in this example are used for illustrative purposes only and the presence or absence of an audio codec has no implications with regard to whether a given audio codec is required to be supported on the DSN.

5.3.4.9.3.5.3 When there are multiple video codecs in a single "m=" line, the bandwidth modifier ("b=TIAS") must be present. The bandwidth modifier must be set to the value equal to

the user-selected bandwidth value or the lowest value of the video codecs's upper limits, depending on which one is smaller. For example, if the user selects to launch a 2 M bits/second video call and the video codec is capable of receiving H.261/H.263 at 2 M bits/second, and H.264 at 384 K bits/second, then the bandwidth modifier ("b=TIAS") value must be set at b=TIAS:384000.

5.3.4.9.3.5.4 The following example is a video SDP using both kinds of bandwidth modifiers:

```
v=0
o=TestVideo 1627471320 0 IN IP4 192.168.100.146
s=-
c=IN IP4 192.168.100.146
b=AS:384
t=0 0
m=audio 49178 RTP/AVP 99 98 97 102 101 103 9 15 0 8 18
b=TIAS:64000
a=rtpmap:99 SIREN14/16000
a=fmtp:99 bitrate=48000
a=rtpmap:98 SIREN14/16000
a=fmtp:98 bitrate=32000
a=rtpmap:97 SIREN14/16000
a=fmtp:97 bitrate=24000
a=rtpmap:102 G7221/16000
a=fmtp:102 bitrate=32000
a=rtpmap:101 G7221/16000
a=fmtp:101 bitrate=24000
a=rtpmap:103 G7221/16000
a=fmtp:103 bitrate=16000
a=rtpmap:9 G722/8000
a=rtpmap:15 G728/8000
a=rtpmap:0 PCMU/8000
a=rtpmap:8 PCMA/8000
a=rtpmap:18 G729A/8000
m=video 49180 RTP/AVP 109 34 96 31
b=TIAS:320000
a=rtpmap:109 H264/90000
a=fmtp:109 profile-level-id=42800c;max-mbps=10000
a=rtpmap:34 H263/90000
a=rtpmap:96 H263-1998/90000
a=fmtp:96 SQCIF=1;QCIF=1;CIF=1;CIF4=2;F;J;T
```

a=rtpmap:31 H261/90000
a=fmtp:31 CIF=1;QCIF=1

5.3.4.9.3.6 H.261 Codec Parameters

5.3.4.9.3.6.1 The H.261 video SDP must meet the following formats:

5.3.4.9.3.6.1.1 The media name in the "m=" line of the SDP MUST be video.

5.3.4.9.3.6.1.2 The encoding name in the "a=rtpmap" line of the SDP MUST be H261.

5.3.4.9.3.6.1.3 The clock rate in the "a=rtpmap" line of the SDP MUST be 90000.

5.3.4.9.3.6.1.4 The SDP MUST use the fmtp media format description line to specify optional parameters, such as CIF, QCIF, and D.

5.3.4.9.3.6.1.4.1 The fmtp parameters for H.261 are as follows:

a=fmtp:xx H261_option

where *xx* is the RTP payload type number. It can be a static or dynamic payload number. The recommendation is to use the dynamic payload number.

5.3.4.9.3.6.1.4.2 The syntax of H261_option is:

H261_option = *Size / *Annex SP
Size = "QCIF" "=" "mpi ;/ "CIF" "=" mpi ;
mpi = 1*2DIGIT
Annex = "D";

5.3.4.9.3.6.1.5 The Size parameter specifies the supported picture size and the frame rate. Recommendation H.261 defines two resolutions: QCIF and CIF. The default value is QCIF.

5.3.4.9.3.6.1.6 The minimum picture interval (MPI) is an integer value (1.4) and it means the maximum picture frame rate is (29.97/MPI) frames/second. The definition of the MPI is according to the video codec specification. The default value is 1.

5.3.4.9.3.6.1.7 The CIF parameter has the format of parameter=value. It describes the maximum supported frame rate for the CIF resolution. Permissible values are integer values 1 to 4, which correspond to a maximum rate of 29.97/the specified value.

5.3.4.9.3.6.1.8 The QCIF parameter has the format of parameter=value. It describes the maximum supported frame rate for the QCIF resolution. Permissible values are integer values 1 to 4, which correspond to a maximum rate of 29.97/the specified value.

5.3.4.9.3.6.1.9 Picture sizes and MPI: A terminal SHOULD announce only those picture sizes (with their MPIs) that it is willing to receive. For example, MPI=2 means that the maximum (decodeable) picture rate per second is about 15. If the receiver does not specify the picture size /MPI optional parameter, then it SHOULD be ready to receive the QCIF resolution with MPI=1.

5.3.4.9.3.6.1.10 Support for still image graphics must be specified according to Recommendation H.261 Annex D. The default value is none. This option MUST NOT appear unless the sender of the SDP message is able to decode this option. This option SHALL be considered as a receiver's capability even when sent in a sendonly offer.

5.3.4.9.3.6.1.11 An example of media representation in SDP (where CIF is 15 frames per second, QCIF is 30 frames per second, and Annex is D) is as follows:

```
m=video 49170/2 RTP/AVP 31
a=rtpmap:31 H261/90000
a=fmtp:31 CIF=2;QCIF=1;D
```

5.3.4.9.3.7 H.263 Codec Parameters

5.3.4.9.3.7.1 The video/H263-1998 and video/H263-2000 media types are mapped to fields in the SDP as follows:

5.3.4.9.3.7.1.1 The media name in the "m=" line of the SDP MUST be video.

5.3.4.9.3.7.1.2 The encoding name in the "a=rtpmap" line of the SDP MUST be H263-1998 or H263-2000.

5.3.4.9.3.7.1.3 The clock rate in the "a=rtpmap" line of the SDP MUST be 90000.

5.3.4.9.3.7.1.4 The SDP MUST use the fmtp media format description line to specify optional parameters.

5.3.4.9.3.7.1.4.1 The fmtp parameters for H.263 are represented in the SDP attribute, as follows:

a=fmtp:*xx* H263_option

where the *xx* is the RTP payload type number. It can be a static or dynamic payload number. The recommendation is to use the dynamic payload number.

5.3.4.9.3.7.1.4.2 The syntax of H263_option is:

H263_option = *Size ; / *Annex ;/ *Params;
Size = “SQCIF” “=” mpi;/ “QCIF” “=” mpi; / “CIF” “=” mpi ;/ “CIF4” “=” mpi ;I
“CIF16” “=” mpi; / “CUSTOM” “=” “XMAX”, “YMAX”, “MPI”;
“XMAX” “=” xmax
“YMAX” “=” ymax
“MPI” “=” mpi
mpi = 1*2DIGIT
xmax=1*4DIGIT
ymax=1*4DIGIT
Annex = “D” “= “F”; / “I”; / “J”; / “K” “=” annex_k ;/ “N” “=” annex_n; / “P” “=” annex_p ; / “T”;
annex_k= “1” / “2” / “3” / “4”
annex_n= “1” / “2” / “3” / “4”
annex_p= “1” / “2” / “3” / “4”

5.3.4.9.3.8 Maximum Picture Frame Rate

5.3.4.9.3.8.1 The MPI is an integer value (1..32) and it means the maximum picture frame rate is (29.97/MPI) frames/second. The definition of the MPI is according to the video codec specification.

The default value is 1.

5.3.4.9.3.9 Picture Size Options

5.3.4.9.3.9.1 The SQCIF parameter specifies the MPI for the SQCIF resolution. Permissible values are integer values from 1 to 32, which correspond to a maximum frame rate of 29.97/the specified value frames per second.

5.3.4.9.3.9.2 The QCIF parameter specifies the MPI for the QCIF resolution. Permissible values are integer values from 1 to 32, which correspond to a maximum frame rate of 29.97/the specified value frames per second.

5.3.4.9.3.9.3 The CIF parameter specifies the MPI for the CIF resolution. Permissible values are integer values from 1 to 32, which correspond to a maximum frame rate of 29.97/the specified value frames per second.

5.3.4.9.3.9.4 The CIF4 parameter specifies the MPI for the 4CIF resolution. Permissible values are integer values from 1 to 32, which correspond to a maximum frame rate of 29.97/the specified value frames per second.

5.3.4.9.3.9.5 The CIF16 parameter specifies the MPI for the 16CIF resolution. Permissible values are integer values from 1 to 32, which correspond to a maximum frame rate of 29.97/the specified value frames per second.

5.3.4.9.3.9.6 The CUSTOM parameter specifies the MPI for a custom defined resolution. The CUSTOM parameter receives three comma-separated values: XMAX, YMAX, and MPI. The XMAX and YMAX values describe the number of pixels in the X and Y axis and must be divisible by 4. Permissible values for MPI are integer values from 1 to 32, which correspond to a maximum frame rate of 29.97/the specified value.

5.3.4.9.3.9.7 If the receiver does not specify the picture size/MPI optional parameter, then it MUST be ready to receive the QCIF resolution with MPI=1.

5.3.4.9.3.9.8 A system that declares support of a specific MPI for one resolution SHALL also implicitly support a lower resolution with the same MPI. An example of the usage of these parameters is as follows:

CIF=4;QCIF=3;SQCIF=2;CUSTOM=360,240,2

5.3.4.9.3.9.9 This means that the encoder SHOULD send CIF picture size, which it can decode at MPI=4. If that is not possible, then QCIF with MPI value=3. If neither are possible, then SQCIF with MPI value=2. The receiver is able to (but least preferred) decode custom picture sizes (max 360x240) with MPI=2.

NOTE: Most decoders support at least QCIF and CIF fixed resolutions and they are expected to be available almost in every H.263-based video application.

5.3.4.9.3.9.10 An example of H.263 SDP in an offer is as follows.

a=fmtp:xx CIF=4;QCIF=2;F;K=1

5.3.4.9.3.9.11 This means that the sender of this message can decode the H.263 bit stream with the following options and parameters: The preferred resolution is CIF (its MPI is 4), but if that is not possible, then the QCIF size is all right. The AP and slicesInOrder-NonRect options MAY be used.

5.3.4.9.3.10 H.263-2000

5.3.4.9.3.10.1 The H.263-2000 can be specified in two different SDP syntaxes.

5.3.4.9.3.10.1.1 The H.263-2000 can apply the optional parameters of the H.263-1998 provided that PROFILE and LEVEL SHALL NOT be used.

5.3.4.9.3.10.1.2 The H.263-2000 can apply the PROFILE and LEVEL as defined in the Annex X of H.263-2000, provided there is no use of H.263-1998 annex option values. Annex X of H.263-2000 defines profiles, which group annexes for specific applications.

5.3.4.9.3.10.2 If the second SDP syntax is chosen, the ftmp must follow:

a=fmtp:xx H263-2000_option

(The *xx* is the RTP payload type number. It can be a static or dynamic payload number. The recommendation is to use the dynamic payload number.)

H263-2000_option = "PROFILE" "=" profile_value ; / "LEVEL" "=" level_value ; / "INTERLACE" "=" interface_value

5.3.4.9.3.10.3 Specific optional parameters that may be used with the H.263-2000 type are:

5.3.4.9.3.10.3.1 The profile_value parameter is an H.263 profile number, in the range 0 through 10, specifying the supported H.263 annexes and subparts based on H.263 annex X[H263X].

5.3.4.9.3.10.3.2 The level_value parameter is the level of bit stream operation, in the range 0 through 100, specifying the level of computational complexity of the decoding process. A system that specifies support of a PROFILE MUST specify the supported LEVEL.

5.3.4.9.3.10.3.3 The interface_value parameter is interlaced or 60 fields that indicate the support for interlace display mode.

5.3.4.9.3.10.4 When the PROFILE and LEVEL parameters are not specified, Baseline Profile (Profile 0) Level 10 are the default values. An example of H.263-2000 in PROFILE and LEVEL is as follows:

```
m = video 8398 RTP/AVP 107 104 116 117 118 119
a=rtpmap:107 h263-2000/90000
a=rtpmap:104 h263-2000/90000
a=rtpmap:116 h263-2000/90000
```

a=rtpmap:117 h263-2000/90000
a=rtpmap:118 h263-2000/90000
a=rtpmap:119 h263-2000/90000
a=fmtp:107 profile=3;level=10
a=fmtp:104 profile=3;level=40
a=fmtp:116 profile=0;level=40
a=fmtp:117 profile=0;level=30
a=fmtp:118 profile=0;level=20
a=fmtp:119 profile=0;level=10

5.3.4.9.3.11 ITU-T H.264 Codec Parameters

5.3.4.9.3.11.1 The MIME media type video/H264 string is mapped to fields in the SDP as follows:

5.3.4.9.3.11.1.1 The media name in the “m=” line of the SDP MUST be video.

5.3.4.9.3.11.1.2 The encoding name in the “a=rtpmap” line of the SDP MUST be H264 (the MIME subtype).

5.3.4.9.3.11.1.3 The clock rate in the “a=rtpmap” line of the SDP MUST be 90000.

5.3.4.9.3.11.2 The AS-SIP signaling appliance must following the requirements of RFC 3984 where it specifies the rules for applying H.264 parameters to the SDP offer/answer model. [RFC 3984, Section 8.2.2, Usage with the SDP Offer/Answer Mode]

5.3.4.9.3.11.3 The fmtp parameters for H.264 are represented in the SDP attribute, as follows:

a=fmtp:xx H264_option

where xx is the RTP dynamic payload number

5.3.4.9.3.11.4 The syntax of the OPTIONAL parameters of H264_option is

H264_option = *Params

Params=
/ “profile-level-id” “=” value ; / ”max-mbps” “=” value; / “max-fs” “=” value;
/ “max-cpb” “=” value ; / “max-dpb” “=” value ; / “max-br” “=” value ;
/ “redundant-pic-cap” “=” value ; / “sprop-parameter-sets” “=” value ; / “parameter-add” “=” value ;
/ “packetization-mode” “=” value ; / “sprop-nterleaving-depth” “=” value ; / “deint-buf-cap” “=” value ;
/ “sprop-deint-buf-req” “=” value ; / “sprop-init-buf-time” “=” value ; / “sprop-max-don-diff” “=” value ;
/ “max-rcmd-nalu-size” “=” value

5.3.4.9.3.11.5 The OPTIONAL parameters include “profile-level-id”, “max-mbps”, “max-fs”, “max-cpb”, “max-dpb”, “max-br”, “redundant-pic-cap”, “sprop-parameter-sets”, “parameter-add”, “packetization-mode”, “sprop-nterleaving-depth”, “deint-buf-cap”, “sprop-deint-buf-req”, “sprop-init-buf-time”, “sprop-max-don-diff”, and “max-rcmd-nalu-size”.

5.3.4.9.3.11.6 The definitions of optional parameters can be found in RFC 3984.

5.3.4.9.3.11.7 An example of media representation in the SDP (where Baseline Profile, Level 3.0, some constraints of the Main profile may not be obeyed) is as follows:

```
m=video 49170 RTP/AVP 98
a=rtpmap:98 H264/90000
a=fmtp:98 profile-level-id=42A01E;
        sprop-parameter-sets=Z0IACpZTBYmI,aMljiA==
```

5.3.4.9.3.12 People and Content

5.3.4.9.3.12.1 The SDP syntax for People and Content is:

```
content-attribute   = “a=content:” mediacnt-tag
mediacnt-tag        = mediacnt *(“,” mediacnt)
mediacnt            = “slides” / “speaker” / “sl” / “main”
                          / “alt” / “user-floor” / mediacnt-ext
mediacnt-ext        = token
```

5.3.4.9.3.12.2 The predefined "content" attribute values are:

5.3.4.9.3.12.2.1 The slides value is a media stream that includes presentation slides. The media type can be, for example, a video stream or a set of instant messages with pictures. Typical use for this value is on-line seminars and courses. This is similar to the "presentation" role in H.239.

5.3.4.9.3.12.2.2 The speaker value is an image from the speaker. The media can be, for example, a video stream or a still image. Typical use for this value is on-line seminars and courses.

5.3.4.9.3.12.2.3 The sl value means that the media stream contains sign language. The media type is a video stream. Typical use for this value is the one where the audio stream is translated into sign language.

5.3.4.9.3.12.2.4 The main value means that the main stream is taken from the main source. Typical use for this value is a concert where the camera is shooting the performer.

5.3.4.9.3.12.2.5 The alt value means that the main stream is taken from the alternative source. This is the alternative media stream. Typical use for this value is an event where there is a separate ambient sound and the main sound. The alternative audio stream could be, for example, a sound of a jungle. Another example is the video of the conference room while the main is the video of the speaker. This is similar to the "live" role in H.239.

5.3.4.9.3.12.2.6 The user-floor value indicates that a user level floor control is required. In other words, this is meant for a system without any mechanism for floor control and where a human needs to determine whether an act of floor control (for example, saying "over") is needed or not. Typically, this can be used with walkie-talkie-type devices and with transcoded text over IP (ToIP) streams originating from Telecommunications Devices for the Deaf (TDDs).

5.3.4.9.3.12.2.7 The following is an example of the SDP session description that uses the "content" attribute:

```
v=0
o=Alice 292742730 29277831 IN IP4 131.163.72.4
s=-
c=IN IP4 131.164.74.2
t=0 0
m=audio 25000 RTP/AVP 0
m=video 35000 RTP/AVP 31
a=content:alt
```

```
m=video 35100 RTP/AVP 31
a=content:slides
```

5.3.4.9.4 Offer/Answer Exchange

5.3.4.9.4.1 RFC 3264 sets forth an offer/answer model for SDP.

5.3.4.9.4.1.1 The AS-SIP signaling appliance MUST perform SDP offer/answer exchanges in compliance with RFC 3264 with additional rules for SIP video listed in Section 5.3.4.9.5, Additional Offer/Answer Rules for AS-SIP Video.

5.3.4.9.4.1.2 The AS-SIP signaling appliance MUST comply with:

- RFC 3264, Section 5, Generating the Initial Offer
- RFC 3264, Section 6, Generating the Answer
- RFC 3264, Section 7, Offerer Processing of the Answer
- RFC 3264, Section 8, Modifying the Session
- RFC 3264, Section 9, Indicating Capabilities

5.3.4.9.5 Additional Offer/Answer Rules for AS-SIP Video

5.3.4.9.5.1 Generating the Initial Offer

The AS-SIP signaling appliance shall include bandwidth modifiers for the video “m=” lines in the SDP.

5.3.4.9.5.2 Generating the Answer

5.3.4.9.5.2.1 The answer must include bandwidth modifiers in all video media streams.

5.3.4.9.5.2.2 The value of the bandwidth modifier in each video “m=” line must not be greater than the value in the corresponding video “m=” line listed in the initial offers.

5.3.4.9.5.2.3 The answerer MUST send a media stream using a media format in the offer that is also listed in the answer, and SHOULD send using the most preferred media format in the offer that is also listed in the answer.

5.3.4.9.5.2.4 The answerer MUST send media using a bandwidth that is not greater than the value of the bandwidth attribute in the answer.

5.3.4.9.5.3 Offerer Processing of the Answer

5.3.4.9.5.3.1 The offerer MUST send a media stream using a media format listed in the answer, and it SHOULD use the first media format listed in the answer. [RFC 3264]

5.3.4.9.5.3.2 The offerer MUST send the video media stream using a bandwidth that is no higher than the value of the bandwidth modifier returned in the answer.

5.3.4.9.6 Examples

5.3.4.9.6.1 Basic SDP Exchange

The caller, Alice, wants to call the callee, Bob. Alice's codec generates the offer as:

```
[Offer]
v=0
o=Alice 1627471320 1627471320 IN IP4 192.168.100.146
s=-
c=IN IP4 192.168.100.146
b=AS:384
t=0 0
                    m=audio 49178 RTP/AVP  0 8 18
b=TIAS:64000
a=rtpmap:0 PCMU/8000
a=rtpmap:8 PCMA/8000
a=rtpmap:18 G729A/8000
                    m=video 49180 RTP/AVP 109 34 96 31
b=TIAS:320000
a=rtpmap:109 H264/90000
a=fmtp:109 profile-level-id=42800c;max-mbps=10000
a=rtpmap:34 H263/90000
a=rtpmap:96 H263-1998/90000
a=fmtp:96 SQCIF=1;QCIF=1;CIF=1;CIF4=2;F;J;T
a=rtpmap:31 H261/90000
                    a=fmtp:31 CIF=1;QCIF=1
```

Bob's codec has a lower bandwidth profile so it generates the answer as:

```
[Answer]
v=0
o=Bob 2890844730 2890844730 IN IP4 host.example.com
```

```
s=-
c=IN IP4 host.example.com
b=AS:300
                    t=0 0
m=audio 49920 RTP/AVP 18
b=TIAS:8000
a=rtpmap:18 G729A/8000
m=video 53000 RTP/AVP 109
b=TIAS:248000
a=rtpmap:109 H264/90000
a=fmtp:109 profile-level-id=42800c;max-mbps=10000
```

5.3.4.9.6.2 re-INVITE

During the call, Bob's codec was informed by other means that the network is congested so it creates a new offer with a further reduced bandwidth as:

```
[Offer]
v=0
o=Bob 2890844730 2890844731 IN IP4 host.example.com
s=-
c=IN IP4 host.example.com
b=AS:150
t=0 0
m=audio 49920 RTP/AVP 18
b=TIAS:8000
                    a=rtpmap:18 G729A/8000
m=video 53000 RTP/AVP 109
b=TIAS:120000
                    a=rtpmap:109 H264/90000
a=fmtp:109 profile-level-id=42800c;max-mbps=10000
```

Alice's codec accepts the changes:

```
[Answer]
v=0
o=Alice 1627471320 1627471321 IN IP4 192.168.100.146
s=-
c=IN IP4 192.168.100.146
b=AS:150
t=0 0
```

```
m=audio 49920 RTP/AVP 18
                    b=TIAS:8000
a=rtpmap:18 G729A/8000
m=video 53000 RTP/AVP 109
b=TIAS:120000
a=rtpmap:109 H264/90000
a=fmtp:109 profile-level-id=42800c;max-mbps=10000
```

5.3.4.10 Precedence and Preemption

5.3.4.10.1 Introduction

This section provides the detailed requirements for the execution of preemption and the handling of precedence information.

5.3.4.10.2 Precedence Level Communicated over SIP Signaling

It should be noted that this section of UCR 2008 incorporates a number of modifications to RFC 4412, Communications Resource Priority for the Session Initiation Protocol (SIP). In particular, a modification has been made to the fields of the Resource-Priority header whereby the namespace has been subdivided into two (2) subfields: network domain and precedence-domain; separated by a dash delimiter (-) (ASCII 45d). This modification impacts the processing rules for the Resource-Priority header. In addition, single character text string representations of decimal digits have been defined for the r-priority values associated with the “dsn” network domain.

5.3.4.10.2.1 Resource-Priority Header Field

The precedence level of the call request MUST be set forth in a SIP Resource-Priority header field whose syntax is in accordance with RFC 4412 as modified in UCR 2008, Section 5.3.4.10.2, Precedence Level Communicated Over SIP Signaling. [RFC 4412, Section 3.1, The ‘Resource-Priority’ Header Field]

```
Resource-Priority        = "Resource-Priority" HCOLON
                                 r-value *(COMMA r-value)
    r-value              = namespace "." r-priority
    namespace            = token-nodot “-“ precedence-domain
    r-priority           = token-nodot
    precedence-domain    = "0" / "1" / "2" / "3" / "4" / "5" / "6" / "7" / "8" / "9"
                                 / "A" / "B" / "C" / "D" / "E" / "F"
    token-nodot          = 1*( alphanum / "!" / "%" / "*" / "_" / "+" / "`" / "'" / "~" )
```

An example Resource-Priority header field is shown below:

Resource-Priority: dsn-000000.2

NOTE: The r-priority values assigned to the various precedence levels of the "dsn" network domain consist of a single character text string for an authorized decimal digit.

5.3.4.10.2.1.1 Namespace

5.3.4.10.2.1.1.1 The namespace consists of two (2) subfields: network domain and precedence-domain, which are separated by the dash delimiter (-)(which is ASCII 45d).

5.3.4.10.2.1.1.2 The network domain subfield identifies the applicable priority scheme and dictates the set of legitimate values that may be assigned to the accompanying r-priority field.

5.3.4.10.2.1.1.3 **[FY2008-FY2012]** AS-SIP signaling appliances are only required to recognize the "dsn" network domain.

5.3.4.10.2.1.1.3.1 (Classified only) [FY2008-FY2012] AS-SIP signaling appliances in the classified network are only required to recognize the "drsn" network domain.

5.3.4.10.2.1.1.3a **[FY2012+]** AS-SIP signaling appliances are required to be capable of recognizing a maximum of 50 valid network domains and each network domain identifier can be a maximum of 10 characters in length.

5.3.4.10.2.1.1.4 The set of valid network domains for a given AS-SIP signaling appliance SHALL be configurable by the network administrator of an AS-SIP signaling appliance at installation and at any time thereafter. Network domains are configurable on a per appliance basis whereby one set of valid network domains applies to all of the IP end instruments served by a given AS-SIP signaling appliance.

5.3.4.10.2.1.1.5 The precedence-domain subfield is a string of six alphanumeric characters from the set: '0', '1', '2', '3', '4', '5', '6', '7', '8', '9', 'A', 'B', 'C', 'D', 'E', and 'F'.

5.3.4.10.2.1.1.6 Call requests are permitted to preempt other call requests and other calls that have the same value for the precedence-domain subfield.

NOTE: After FY2012 when there can be a variety of valid values for the network domain subfield, then a call request having one value for the network domain subfield can preempt a lesser precedence existing call or call request having a different value for the network domain

subfield as long as the value for the precedence-domain subfield of the new call request is the same as for the existing call.

5.3.4.10.2.1.1.7 Call requests are NOT permitted to preempt other call requests and other calls that have a different value for the precedence-domain subfield.

5.3.4.10.2.1.1.8 When a circumstance arises whereby an AS-SIP signaling appliance receives a precedence call request and is called on to make a preemption decision, the AS-SIP signaling appliance can only preempt calls of lesser precedence that have the same value for the precedence-domain as the pending precedence call request.

5.3.4.10.2.1.1.9 The default value for the precedence-domain field is "000000."

5.3.4.10.2.1.2 r-priority

5.3.4.10.2.1.2.1 In order to protect against external inferences regarding the precedence level of SIP signaling messages that, in part, exploit analysis of the length of encrypted messages, a one-to-one correspondence has been defined between each precedence level in the "dsn" network "domain" and a single character text string representation of a decimal value (see Table 5.3.4-8).

Table 5.3.4-8. r-priority Values

r-priority	CORRESPONDING DECIMAL VALUE
routine	'0'
priority	'2'
immediate	'4'
flash	'6'
flash-override	'8'

5.3.4.10.2.1.2.2 Whenever a Resource-Priority header field has a network domain subfield with the value "dsn," then the r-priority value must be the single character text string representation of the decimal digit corresponding to the intended precedence level as depicted in Table 5.3.4-8.

5.3.4.10.2.1.2.3 **[Required]** AS-SIP signaling appliances MUST support the r-priority values '0', '2', '4', '6', '8' for the network domain "dsn."

5.3.4.10.2.1.2.4 **[FY2012+]** The single character text string representations of '1', '3', '5','7', '9' will be valid r-priority values for the network domain "dsn."

Classified only: Requirements 5.3.4.10.2.1.2.5–5.3.4.10.2.1.2.8

5.3.4.10.2.1.2.5 In order to protect against external inferences regarding the precedence level of SIP signaling messages that, in part, exploit analysis of the length of encrypted messages, a one-to-one correspondence has been defined between each precedence level in the "drsn" network "domain" and a single character text string representation of a decimal value (see Table 5.3.4-8a).

Table 5.3.4-8a. r-priority Values

r-priority	CORRESPONDING DECIMAL VALUE
routine	'0'
priority	'2'
immediate	'4'
flash	'6'
flash-override	'8'
flash-override-override	'9'

5.3.4.10.2.1.2.6 Whenever a Resource-Priority header field has a network domain subfield with the value "dsn," then the r-priority value must be the single character text string representation of the decimal digit corresponding to the intended precedence level as depicted in Table 5.3.4-8a.

5.3.4.10.2.1.2.7 **[Required]** AS-SIP signaling appliances MUST support the r-priority values '0', '2', '4', '6', '8', '9' for the network domain "drsn."

5.3.4.10.2.1.2.8 **[FY2012+]** The single character text string representations of '1', '3', '5','7'will be valid r-priority values for the network domain "drsn."

5.3.4.10.2.2 Requirements for AS-SIP Signaling Appliances Serving IP End Instruments

AS-SIP signaling appliances serving IP end instruments refer to LSCs and to the LSC component of Softswitches that directly serve IP end instruments.

NOTE: For the Classified network the default network domain subfield for FY2008-FY2012 is "drsn." The requirements set forth in Section 5.3.4.10.2.2 are made applicable to the Classified network by substituting "drsn" for "dsn" in each requirement.

SIP Message without Resource-Priority Header Received from Served SIP End Instrument

5.3.4.10.2.2.1 **[FY2008-2012]** Whenever a DSN AS-SIP signaling appliance receives an INVITE, UPDATE, or REFER request from a served SIP end instrument that does not contain a Resource-Priority header field, the AS-SIP signaling appliance MUST add a Resource-Priority

header having one (1) resource value (i.e., namespace.r-priority). The AS-SIP signaling appliance assigns the appropriate values for the namespace (i.e., network domain subfield: "dsn" and precedence-domain subfield: "000000") and for the r-priority field in accordance with the dialed string and local policy). In the case of precedence call requests, the AS-SIP signaling appliance MUST authenticate the requester and determine that the requester is authorized to employ the precedence level before forwarding the SIP message. If these conditions are not met, then UCR 2008, Section 5.3.4.10.2.4, Error Conditions, subsections Authentication Failure and Authorization Failure detail the error handling.

5.3.4.10.2.2.2 **[After FY2012]** Whenever the AS-SIP signaling appliance on the DSN receives an INVITE, UPDATE, or REFER request from a served SIP end instrument that does not contain a Resource-Priority header field, the AS-SIP signaling appliance MUST add a Resource-Priority header and MAY add multiple Resource-Priority headers as dictated by local policy. A given Resource-Priority header MUST contain a resource value (i.e., namespace.r-priority) and MAY contain multiple resource values as dictated by local policy.

SIP Message with Resource-Priority Header Received from Served SIP End Instrument

5.3.4.10.2.2.3 **[FY2008-2012]** Whenever a DSN AS-SIP signaling appliance receives a call signaling message from a served SIP end instrument having a Resource-Priority header, the AS-SIP signaling appliance MUST ensure that the Resource-Priority header field contains a namespace having a valid network domain subfield, a valid precedence-domain subfield, and an authorized r-priority value for the given network domain subfield.

A network domain ID received from a directly served SIP end instrument is considered valid when it is known to the AS-SIP signaling appliance and when its use by the AS-SIP end instrument is consistent with local policy. For DSN AS-SIP signaling appliances in the FY2008-2012 time frame, the valid value for the network domain subfield for an AS-SIP message originating at a directly served SIP end instrument is "dsn."

The precedence-domain subfield MAY be absent from the Resource-Priority header field in which case it is assumed to be the default text string "000000."

A precedence-domain subfield received from a directly served SIP end instrument is considered valid when it has a conformant syntax and when the value is consistent with local policy. For FY2008-2012, the valid value for a precedence-domain subfield in the namespace of a Resource-Priority header in an AS-SIP message originating from a served SIP end instrument in the DSN is the text string "000000."

5.3.4.10.2.2.3.1 **[FY 2008-2012]** In the event the DSN AS-SIP signaling appliance does not recognize the network domain, then the AS-SIP signaling appliance will substitute the valid network domain subfield (i.e., "dsn") and set the value in the r-priority field to "0" (routine).

5.3.4.10.2.2.3.2 **[FY2008-2012]** In the event the precedence-domain subfield in the Resource-Priority header received from the served SIP end instrument has a value other than the text string "000000," the AS-SIP signaling appliance MUST change the value to the text string "000000."

5.3.4.10.2.2.3.3 **[FY2008-2012]** In the event the DSN AS-SIP signaling appliance recognizes the network domain and the network domain is considered valid in accordance with local policy, then the r-prioriy field MUST have a value that is from the authorized set of r-priority values for the given network domain. In FY2008-2012, the only valid network domain for an AS-SIP message originating at a served DSN SIP end instrument is "dsn" and the set of authorized r-priority values are 0', '2', '4', '6', '8'. When the value in the r-priority field is not valid, then the AS-SIP signaling appliance sets the r-priority field to "0." In the case of precedence call requests, the AS-SIP signaling appliance MUST authenticate the requester and determine that the requester is authorized to employ the precedence level before forwarding the SIP message. If these conditions are not met, then UCR 2008, Section 5.3.4.10.2.4, Error Conditions, subsections Authentication Failure and Authorization Failure, detail the error handling.

5.3.4.10.2.2.3.4 **[FY2008-2012]** In the event the DSN AS-SIP signaling appliance receives a SIP message from a served SIP end instrument with a Resource-Priority header having multiple resource values or a SIP message having multiple Resource-Priority headers then:

- If none of the resource values has a network domain of "dsn," the DSN AS-SIP signaling appliance MUST remove all the existing Resource-Priority headers and replace them with one (1) Resource-Priority header having a network domain of "dsn" and an r-priority value of "0." The precedence-domain subfield MUST be assigned the text string "000000."

- If one of the resource values has a network domain of "dsn," the DSN AS-SIP signaling appliance MUST remove all but that one Resource-Priority header and place the resource value with "dsn" into the Resource-Priority header. If the precedence-domain subfield is any value other than the text string "000000," then it must be replaced with the text string "000000." The r-priority field MUST have an authorized value (i.e., for "dsn" the authorized values are '0', '2', '4', '6', '8'), and if it does not, then the r-priority field will be assigned the value "0." In the case of precedence call requests, the AS-SIP signaling appliance MUST authenticate the requester and determine that the requester is authorized to employ the precedence level before forwarding the SIP message. If these conditions are not met, then UCR 2008, Section

5.3.4.10.2.4, Error Conditions, subsections Authentication Failure and Authorization Failure, detail the error handling.

- If "dsn" appears in more than one (1) resource value, then the DSN AS-SIP signaling appliance MUST remove all the Resource-Priority headers and replace them with one (1) Resource-Priority header populated with a resource value having "dsn" in the network domain and "0" in the r-priority field. For FY2008-2012, the precedence domain field MUST be the text string "000000."

5.3.4.10.2.2.4 **[After FY2012]** Whenever a DSN AS-SIP signaling appliance receives a call signaling message from a served SIP end instrument having one or more Resource-Priority headers (whereby each Resource-Priority header has one or more resource values), the AS-SIP signaling appliance MUST:

5.3.4.10.2.2.4.1 **[After FY2012]** Remove the resource values where the network domain subfield is not valid (i.e., resource values whose network domain is either not known to the AS-SIP signaling appliance or is known but its use by the AS-SIP end instrument is not consistent with local policy).

5.3.4.10.2.2.4.2 **[After FY2012]** Whenever all resource values in a Resource-Priority header are deemed invalid, then the Resource-Priority header is removed.

5.3.4.10.2.2.4.3 **[After FY2012]** If there are no valid resource values thereby resulting in the removal of all Resource-Priority headers, then the AS-SIP signaling appliance MUST add a Resource-Priority header and MAY add multiple Resource-Priority headers as dictated by local policy. A given Resource-Priority header MUST contain a resource value (i.e., namespace.r-priority) and MAY contain multiple resource values as dictated by local policy.

5.3.4.10.2.2.4.4 **[After FY2012]** When the removal of resource values due to invalid network domain IDs results in the retention of one or more resource values, the corresponding r-priority value in each case MUST be authorized for the given network domain. In the event an r-priority value is not authorized, then it is replaced with the lowest precedence value for that network domain. In the case of precedence call requests, the AS-SIP signaling appliance MUST authenticate the requester and determine that the requester is authorized to employ the precedence level before forwarding the SIP message. If these conditions are not met, then UCR 2008, Section 5.3.4.10.2.4, Error Conditions, subsections Authentication Failure and Authorization Failure, detail the error handling. The precedence-domain subfield received from a served SIP end instrument is considered valid when it has conformant syntax and when the value is consistent with local policy. If the AS-SIP signaling appliance determines that a given

precedence-domain field is invalid, then the AS-SIP signaling appliance MUST replace it with a value that is consistent with local policy.

Call Request Received from Served H.323 or Proprietary IP End Instrument

5.3.4.10.2.2.5 **[FY2008-2012]** Whenever a DSN AS-SIP signaling appliance receives a call signaling message from a served H.323 or proprietary IP end instrument that is translated into a SIP INVITE, UPDATE, or REFER request, the AS-SIP signaling appliance MUST add a Resource-Priority header having one (1) resource value (i.e., namespace.r-priority). The AS-SIP signaling appliance assigns the appropriate values for the namespace (i.e., network domain subfield: "dsn" and precedence-domain subfield: "000000") and for the r-priority field in accordance with the dialed string and local policy. In the case of precedence call requests, the AS-SIP signaling appliance MUST authenticate the requester and determine that the requester is authorized to employ the precedence level before forwarding the SIP message. If the request is not authenticated the AS-SIP signaling appliance MUST give the requester the opportunity to conduct the necessary authentication and if the requester is not authorized to use the requested precedence level, then the unauthorized precedence announcement (UPA) shall be announced and/or displayed to the user (see Table 5.3.4-9, Announcements) through the end instrument. For switch name and location, the announcement shall indicate the local AS-SIP signaling appliance serving the IP end instrument. Then the call request MUST be terminated.

5.3.4.10.2.2.6 **[After FY2012]** Whenever the AS-SIP signaling appliance on the DSN receives a call signaling message from a served H.323 or proprietary IP end instrument that is translated into a SIP INVITE, UPDATE, or REFER request, the AS-SIP signaling appliance MUST add a Resource-Priority header and MAY add multiple Resource-Priority headers as dictated by local policy. A given Resource-Priority header MUST contain a resource value (i.e., namespace.r-priority) and MAY contain multiple resource values as dictated by local policy.

AS-SIP Message with Resource-Priority Header for Served IP End Instrument

5.3.4.10.2.2.7 **[FY2008-2012]** AS-SIP signaling appliances serving IP end instruments MUST support receiving and processing the Resource-Priority header field to determine whether to deny a call request or to preempt an existing call or call request and, if so, to create and send the appropriate signaling messages to implement the denial or preemption. See UCR 2008, Section 5.3.4.10.3, ASAC Preemption Requirements, for the details of the preemption requirements on AS-SIP signaling appliances.

Table 5.3.4-9. Announcements

ANNOUNCEMENT CONDITION	ANNOUNCEMENT
An equal or higher precedence call is in progress	Blocked Precedence Announcement (BPA). "(Local LSC name and Location) or "(Remote AS-SIP signaling appliance name and location) Equal or higher precedence calls have prevented completion of your call. Please hang up and try again. This is a recording. (Local LSC name and Location) or (Remote AS-SIP signaling appliance name and location)"
Unauthorized Precedence level is attempted	Unauthorized Precedence Level Announcement (UPA). "(Local LSC name and Location). The precedence used is not authorized for your line. Please use an authorized precedence or ask your attendant for assistance. This is a recording. (Local LSC name and Location)."
Busy station not equipped for preemption	Busy Not Equipped Announcement (BNEA). "(Remote AS-SIP signaling appliance name and location). The number you have dialed is busy and not equipped for call waiting or preemption. Please hang up and try again. This is a recording. (Remote AS-SIP signaling appliance name and location)."
Attendant Queue Announcement (ATQA)	"This is the <site name> Local Session Controller. All attendants are busy now. Please remain on the line until an attendant becomes available or try your call later. This is a recording. <site name> Local Session Controller."

5.3.4.10.2.2.8 **[After FY2012]** When an AS-SIP signaling appliance receives an AS-SIP message intended for a served IP end instrument and there are either multiple Resource Priority headers or multiple resource values within a Resource Priority header and the AS-SIP signaling appliance recognizes more than one resource value having a valid network domain (where the value in the network domain subfield is considered valid if it is one of the known network domains with which the AS-SIP signaling appliance has been configured) then:

5.3.4.10.2.2.8.1 The AS-SIP signaling appliance selects the valid namespace having the highest associated priority level. [RFC 4412, Section 8.1]

5.3.4.10.2.2.8.2 In the event the valid namespaces with the highest priority levels are equivalent, then the AS-SIP signaling appliance selects one of these network domains based on local policy.

5.3.4.10.2.3 Option Tag 'resource-priority'

5.3.4.10.2.3.1 The AS-SIP signaling appliances serving H.323 or proprietary IP end instruments MUST support the option tag 'resource-priority' for use with the Require header field.

5.3.4.10.2.3.1.1 The AS-SIP signaling appliance MUST receive and accept a Require header field with the option tag 'resource-priority' in the INVITE, UPDATE, and REFER messages on behalf of the H.323 and proprietary EIs. AS-SIP signaling appliances MUST NOT reject the message with a 420 (Bad Extension) but rather MUST accept the request and convert it as required for the non-SIP IP EI.

5.3.4.10.2.3.2 The AS-SIP signaling appliances serving SIP end instruments that do not implement the resource-priority header MUST handle the option tag 'resource-priority' in the Require header field on behalf of their served SIP end instruments. The mechanism employed by the AS-SIP signaling appliance is left to vendor-specific implementation.

5.3.4.10.2.4 Error Conditions

AS-SIP Signaling Appliance Serving IP End Instrument: Improper Network-Domain, Priority Value, or Precedence-Domain

NOTE: For the Classified network the default network domain subfield for FY2008-FY2012 is "drsn". The requirements set forth in Section 5.3.4.10.2.4 are made applicable to the Classified network by substituting "drsn" for "dsn" in each requirement.

FY2008-2012

5.3.4.10.2.4.1 **[FY2008-2012]** When the DSN AS-SIP signaling appliance receives a SIP request with a Resource Priority header intended for a served IP end instrument and the SIP request either does not have a Require header or has a Require header but not the option tag 'resource-priority' then:

5.3.4.10.2.4.1.1 If the AS-SIP signaling appliance does not recognize the value of the network domain subfield of the namespace, then the network domain subfield is treated as if it were set to "dsn" and the r-priority value is treated as if it were set to "0." If the precedence-domain subfield is either syntactically flawed or does not consist of the text string "000000," then it is still treated as if it had the value "000000."

Implementation Note: One valid implementation for treating the precedence domain subfield as if it had the value "000000" is for the AS-SIP signaling appliance to change the precedence domain subfield to "000000". It is by no means required that the AS-SIP signaling appliance convert the precedence domain subfield to "000000' but it is an allowed method for complying with the requirement. This implementation note applies to every requirement in the UCR that specifies the AS-SIP signaling appliance is to treat the precedence domain subfield as if it had the value "000000".

5.3.4.10.2.4.1.2 If the AS-SIP signaling appliance recognizes the value of the network domain subfield of the namespace but the r-priority field does not have an authorized value for the given network domain, then the r-priority value is treated as if it were set to the lowest priority level. If the precedence-domain subfield is either syntactically flawed or does not consist of the text string "000000," then it is still treated as if it had the value "000000."

5.3.4.10.2.4.1.3 If the AS-SIP signaling appliance receives a namespace with a recognized network domain and an authorized r-priority value whose precedence-domain subfield has a text string that is either syntactically invalid or does not consist of the text string "000000," then the precedence-domain subfield is treated as if it were set to the text string "000000."

5.3.4.10.2.4.2 **[FY2008-2012]** When the AS-SIP signaling appliance receives a SIP request with a Resource Priority header intended for a served IP end instrument and the SIP request has a Require header field with an option tag 'resource-priority' then:

5.3.4.10.2.4.2.1 If the AS-SIP signaling appliance does not recognize the value of the network domain subfield of the namespace, then the AS-SIP signaling appliance MUST reject the request with a 417 (Unknown Resource-Priority) response code.

5.3.4.10.2.4.2.2 If the AS-SIP signaling appliance recognizes the value of the network domain subfield but the value of the r-priority field is not valid for the given network domain, then the r-priority value is treated as if it were set to the lowest priority level. If the precedence-domain subfield has a text string that is syntactically invalid or does not consist of the text string "000000," then the precedence-domain subfield is treated as if it were set to "000000."

5.3.4.10.2.4.2.3 If the AS-SIP signaling appliance recognizes the value of the network domain and the r-priority field has an authorized value for the network domain but the precedence-domain subfield has a text string that is syntactically invalid or does not consist of the text string "000000," then the precedence-domain subfield is treated as if it were set to "000000."

5.3.4.10.2.4.3 **[After FY2012]** When the DSN AS-SIP signaling appliance receives a SIP request with 1 or more Resource Priority headers intended for a served IP end instrument and the SIP request either does not have a Require header or has a Require header but not the option tag 'resource-priority' then:

5.3.4.10.2.4.3.1 If there is either one (1) Resource Priority header with at least two (2) namespaces or if there are two (2) or more Resource Priority headers (i.e., two (2) or more different namespaces) and the DSN AS-SIP signaling appliance does not recognize the value of the network domain subfield in any of the namespaces, then the AS-SIP signaling appliance MUST treat the network domain as if it were "dsn" and treat the r-priority value as if it were set

to "0." If the precedence-domain subfield has a text string that is syntactically invalid, then the precedence-domain subfield is treated as if it were set to "000000."

5.3.4.10.2.4.3.2 If there are multiple resource values having valid network domains, then in any case where the r-priority value associated with the valid network domain is not an authorized value it is treated as if it were set to the lowest priority level. When the priority levels of the resource values are compared to determine which resource value will be used for precedence and preemption purposes, then the resource values with valid network domains but having unauthorized r-priority values will be treated as having the lowest precedence level when the comparison is made, and the resource value with the highest priority will be selected. In each case, the precedence-domain is interpreted as is unless it is syntactically flawed in which case it is treated as the text string "000000."

5.3.4.10.2.4.4 **[After FY2012]** When the AS-SIP signaling appliance receives a SIP request with at least one (1) Resource Priority header intended for a served IP end instrument and the SIP request has a Require header field with an option tag 'resource-priority' then:

5.3.4.10.2.4.4a.1 If there is either one (1) Resource Priority header with at least two (2) namespaces or if there are two (2) or more Resource Priority headers (i.e., two (2) or more different namespaces) and the AS-SIP signaling appliance does not recognize the value of the network domain subfield in any of the namespaces, then the AS-SIP signaling appliance MUST reject the request with a 417 (Unknown Resource-Priority) response code.

5.3.4.10.2.4.4a.2 If there are multiple resource values having valid network domains, then in any case where the r-priority value associated with the valid network domain is not an authorized value it is treated as if it were set to the lowest priority level. When the priority levels of the resource values are compared to determine which resource value will be used for precedence and preemption purposes, then the resource values with valid network domains but having unauthorized r-priority values will be treated as having the lowest precedence level when the comparison is made, and the resource value with the highest priority will be selected. In each case, the precedence-domain is interpreted as is unless it is syntactically flawed in which case it is treated as the text string "000000."

Intermediary Softswitch: Improper Network-Domain, Priority Value, or Precedence-Domain

Originating Softswitch [FY2008-2012]

5.3.4.10.2.4.4b **[Objective]** When a Softswitch receives a SIP request with a Resource Priority header from a served LSC and the SIP request either does not have a Require header or has a Require header but not the option tag 'resource-priority' then:

5.3.4.10.2.4.4b.1 **[Objective]** If the Softswitch does not recognize the value of the network domain subfield of the namespace, then for ASAC classification purposes, which become significant when the Softswitch is called on to conduct policing (see Section 5.3.4.11, Policing of Call Count Thresholds), the SIP message is classified as follows:

- Network domain subfield equals "dsn"
- R-priority value equals "0" (routine)
- Precedence-domain subfield equals "000000"

5.3.4.10.2.4.4b.2 **[Objective]** If the Softswitch recognizes the value of the network domain subfield of the namespace but the r-priority field does not have an authorized value for the given network domain, then for ASAC classification purposes the SIP message is classified as follows:

- Network domain subfield is not changed (FY2008-FY2012 it is "dsn.")

- R-priority value is treated as if it were set to the lowest priority level (FY2008-FY2012 it is "0.")

- Precedence-domain subfield equals "000000"

5.3.4.10.2.4.4b.3 **[Objective]** If the Softswitch receives a namespace with a recognized network domain and an authorized r-priority value whose precedence-domain subfield has a text string that is either syntactically invalid or does not consist of the text string "000000," then the precedence-domain subfield is classified as if it were set to the text string "000000."

5.3.4.10.2.4.4c **[Objective]** When a Softswitch receives a SIP request with a Resource Priority header from a served LSC and the SIP request has a Require header field with an option tag 'resource-priority' then:

5.3.4.10.2.4.4c.1 **[Objective]** If the Softswitch does not recognize the value of the network domain subfield of the namespace, then the Softswitch MUST reject the request with a 417 (Unknown Resource-Priority) response code.

5.3.4.10.2.4.4c.2 **[Objective]** If the Softswitch recognizes the value of the network domain subfield but the value of the r-priority field is not valid for the given network domain, then for ASAC classification purposes the SIP message is classified as follows:

- Network domain subfield is not changed (FY2008-FY2012 it is "dsn.")

- R-priority value is treated as if it were set to the lowest priority level (FY2008-FY2012 it is "0.")

- Precedence-domain subfield equals “000000”

5.3.4.10.2. 4.4c.3 **[Objective]** If the Softswitch recognizes the value of the network domain and the r-priority field has an authorized value for the network domain but the precedence-domain subfield has a text string that is syntactically invalid or does not consist of the text string “000000,” then the precedence-domain subfield is classified as if it were set to “000000.”

Terminating Softswitch [FY2008-2012]

5.3.4.10.2.4.4d **[Objective]** When a Softswitch receives a SIP request with a Resource Priority header intended for a served LSC and the SIP request either does not have a Require header or has a Require header but not the option tag ‘resource-priority,’ then the Softswitch takes no action with regard to the resource priority header until it receives a response from the served LSC and proceeds as follows:

5.3.4.10.2.4.4d.1 **[Objective]** If the served LSC responds with a 1xx greater than (>) 100 or a 200 and if the Softswitch does not recognize the value of the network domain subfield of the namespace, then for ASAC classification purposes the SIP message is classified as follows:

- Network domain subfield equals “dsn”
- R-priority value equals “0” (routine)
- Precedence-domain subfield equals “000000”

5.3.4.10.2.4.4d.2 **[Objective]** If the served LSC responds with a 1xx greater than (>) 100 or a 200 and if the Softswitch recognizes the value of the network domain subfield of the namespace but the r-priority field does not have an authorized value for the given network domain, then for ASAC classification purposes the SIP message is classified as follows:

- Network domain subfield is not changed (FY2008-FY2012 it is “dsn.”)

- R-priority value is treated as if it were set to the lowest priority level (FY2008-FY2012 it is “0.”)

- Precedence-domain subfield equals “000000.”

5.3.4.10.2.4.4d.3 **[Objective]** If the served LSC responds with a 1xx greater than (>) 100 or a 200 and if the Softswitch receives a namespace with a recognized network domain and an authorized r-priority value whose precedence-domain subfield has a text string that is either syntactically invalid or does not consist of the text string “000000,” then the precedence-domain subfield is classified as if it were set to the text string “000000.”

5.3.4.10.2.4.4e **[Objective]** When a Softswitch receives a SIP request with a Resource Priority header from a served LSC and the SIP request has a Require header field with an option tag 'resource-priority,' then the Softswitch takes no action with regard to the resource priority header until it receives a response from the served LSC and proceeds as follows:

5.3.4.10.2.4.4e.1 **[Objective]** If the served LSC responds with a 1xx greater than (>) 100 or a 200 and if the Softswitch does not recognize the value of the network domain subfield of the namespace, then the Softswitch MUST:

- Send a 417 (Unknown Resource-Priority) response code to the remote initiating party
- Send a CANCEL request (in the case of a 1xx) or a BYE request (in the case of a 2xx) to the local LSC

5.3.4.10.2.4.4e.2 **[Objective]** If the served LSC responds with a 1xx greater than (>) 100 or a 200 and if the Softswitch recognizes the value of the network domain subfield but the value of the r-priority field is not valid for the given network domain, then for ASAC classification purposes the SIP message is classified as follows:

- Network domain subfield is not changed (FY2008-FY2012 it is "dsn.").
- R-priority value is treated as if it were set to the lowest priority level (FY2008-FY2012 it is "0.").
- Precedence-domain subfield equals "000000."

5.3.4.10.2.4.4e.3 **[Objective]** If the served LSC responds with a 1xx greater than (>)100 or a 200 and if the Softswitch recognizes the value of the network domain and the r-priority field has an authorized value for the network domain but the precedence-domain subfield has a text string that is syntactically invalid or does not consist of the text string "000000," then the precedence-domain subfield is classified as if it were set to "000000."

Authentication Failure

5.3.4.10.2.4.5 The AS-SIP signaling appliances serving IP end instruments are responsible for the authentication of the IP end instruments they represent, and in the case of outbound precedence call requests, the AS-SIP signaling appliance must be software configurable for purposes of enabling or disabling authentication of the requestor. In the event that the requesting IP end instrument employs SIP signaling and the AS-SIP signaling appliance is configured with requestor authentication enabled, and the requestor of an outbound precedence call request is not

authenticated, then the responsible AS-SIP signaling appliance MUST return the request to allow the requestor to insert the appropriate credentials. A 407 (Proxy Authentication Required) or a 401 (Unauthorized) response code, as appropriate, shall be sent to the SIP end instrument. [RFC 4412, Section 4.6.3, Authentication Failure]

NOTE: The mechanisms employed to authenticate the initiator of above ROUTINE precedence sessions is described in UCR 2008, Section 5.4, Information Assurance Requirements, and includes methods such as a prompt to enter a user PIN and then a prompt to enter a authorizatrion PIN.

Authorization Failure

5.3.4.10.2.4.6 The AS-SIP signaling appliances serving IP end instruments are responsible for the authorization of the IP end instruments they represent and this includes the authority to request a particular precedence level. In the event that the requesting IP end instrument requests a precedence level for which it has insufficient authorization, then the responsible AS-SIP signaling appliance MUST announce and/or display the unauthorized precedence announcement (UPA) to the user (see Table 5.3.4-9, Announcements) through the end instrument (for switch name and location, the announcement shall indicate the AS-SIP signaling appliance serving the IP end instrument), and reject the call request and reply with a 403 (Forbidden) response code. [RFC 4412, Section 4.6.4, Authorization Failure]

5.3.4.10.2.4.6b **[FY2008-2012]** The set of announcements in Table 5.3.4-9, Announcements (i.e., BPA, UPA, BNEA, ATQA), is an FY2008-2012 requirement. Additional announcements MAY be specified at a later time.

5.3.4.10.2.4.6c **[FY2008-2012]** When the announcement is BPA or BNEA and the location of the event is a remote AS-SIP signaling appliance, then for the FY2008-FY2012 time frame the announcement in Table 5.3.4-9, Announcements, identifying the switch name and location as "remote AS-SIP signaling appliance." This requirement MAY be modified for the post-FY2012 time frame.

Insufficient Resources

5.3.4.10.2.4.7.1 If an AS-SIP signaling appliance receives an inbound routine call request over the IP network for a served end instrument and the AS-SIP signaling appliance has insufficient bandwidth-related resources (e.g., due to call count threshold) to handle the call request, the AS-SIP signaling appliance MUST reply with a 488 (Not Acceptable Here) response code and SHOULD include a Warning header with warning code 370 (Insufficient Bandwidth).

5.3.4.10.2.4.7.2 If an AS-SIP signaling appliance receives an inbound precedence call request (i.e., with precedence level "priority" or above) over the IP network for a served end instrument and the AS-SIP signaling appliance has insufficient bandwidth-related resources (e.g., due to call count threshold) to handle the call request, and if there are insufficient existing calls (and/or call requests) of lower precedence whose removal would provide the necessary resources to support the pending call request, then:

5.3.4.10.2.4.7.2.1 The AS-SIP signaling appliance MUST reply with a 488 (Not Acceptable Here) response code and SHOULD include a Warning header with warning code 370 (Insufficient Bandwidth), and

5.3.4.10.2.4.7.2.2 The AS-SIP signaling appliance serving the calling IP end instrument MUST arrange for a BPA (see Table 5.3.4-9, Announcements) to be played and/or displayed to the user through the calling IP end instrument.

5.3.4.10.2.4.7.3 In the event that an AS-SIP signaling appliance receives a call request and has insufficient server resources to handle the signaling load, then the AS-SIP signaling appliance MUST reply with a 503 (Service Unavailable) response code. If the call request is a precedence call request (Priority or higher), then the AS-SIP signaling appliance serving the calling IP end instrument MUST arrange for a BPA (see Table 5.3.4-9, Announcements) to be played and/or displayed to the user through the calling IP end instrument.

Re-INVITE with Different Resource Priority Header

5.3.4.10.2.4.8 In the case of a two-party call the Resource Priority header of a re-INVITE or UPDATE MUST be identical to that of the original INVITE. The network domain field MUST be identical, the r-priority value MUST be identical, and the precedence-domain field MUST be identical. Note: In the case of the unattended call transfer supplementary service and the attended call transfer supplementary service re-INVITEs or UPDATEs that are used to replace the transferor in the transferor – transfer target call leg with the transferee MAY require that the Resource Priority header in the re-INVITE or UPDATE be different from that of the original INVITE from the Transferee – Transferor call leg. In addition, a 3-way call that reverts to a 2-way call in which each leg has a different precedence level will require that the Resource Priority header in the re-INVITE or UPDATE for the party on the lesser precedence call leg be different from that found in the original INVITE.

5.3.4.10.2.4.8.1 In the event the Resource Priority header of the re-INVITE is not identical to that of the original INVITE (and neither of the exception cases in the note of Requirement 5.3.4.10.2.4.8 apply) then any AS-SIP signaling appliance that receives the re-INVITE with the differing Resource Priority header MUST send a 403 (Forbidden) response.

5.3.4.10.2.5 Precedence Call Rules

5.3.4.10.2.5.1 When a precedence call (i.e. Priority or higher) is offered successfully to a called party, the calling party MUST receive an audible ringback precedence call tone. See Table 5.3.4-10, DSN Information Signals, for details on audible ringback precedence call tone.

Table 5.3.4-10. DSN Information Signals*

SIGNAL	FREQUENCIES (Hz)	SINGLE TONE LEVEL	COMPOSITE LEVEL	INTERRUPT RATE	TONE ON	TONE OFF
Audible Ringback Precedence Call	440 + 480 (Mixed)	-19 dBm0	-16 dBm0	30 IPM	1640 ms	360 ms
Alerting (Ring) Routine	-	-	-	10 IPM	2000 ms	4000 ms
Alerting (Ring) Precedence	-	-	-	30 IPM	1640 ms	360 ms
Preemption Tone	440 + 620 (Mixed)	-19 dBm0	-16 dBmo		Steady on	
Call Waiting (Precedence Call)	440	-13 dBm0		Continuous at 6 IPM	100 ± 20 ms Three Bursts	9700 ms
Conference Disconnect Tone	852 and 1336 (alternated at 100 ms Intervals)	-24 dBm0		Steady on	2000 ms (per occurrence)	
Override Tone	440			Continuous at 6 IPM	2000 ms (followed by) 500 ms on and 7500 ms off	
Camp On	440	-13 dBm0			Single burst 0.75 to 1 second	
*This table is a copy ofUCR 2008, Table 5.2.4-5, DSN Information Signals, with ringing signal added.						

5.3.4.10.2.5.2 In the case of an IP end instrument for which the user has NOT activated call forwarding, when a precedence call is not answered within a predetermined period of between 15-45 seconds and precedence call waiting has not been accepted, then the AS-SIP signaling appliance serving the IP end instrument MUST provide a global default diversion to a designated directory number (e.g., Attendant Console).

5.3.4.10.2.5.3 In the case of an IP end instrument for which the user has NOT activated call forwarding, when a precedence call request is sent to an IP end instrument that is busy with a higher precedence call, the precedence call waiting MUST be invoked whereby the precedence call waiting tone is applied to the called party. See Table 5.3.4-10, DSN Information Signals.

5.3.4.10.2.5.3.1 If, after receiving the precedence call waiting signal, the busy called IP end instrument does not answer the incoming call within the maximum programmed time interval, the AS-SIP signaling appliance serving the IP end instrument MUST provide a global default diversion to a designated directory number (e.g., Attendant Console).

5.3.4.10.2.5.4 In the case of an IP end instrument for which the user has NOT activated call forwarding, when a precedence call request is sent to an IP end instrument that is busy with a call of equal precedence to the new call request, then the precedence call waiting tone MUST be applied to the called party. See Table 5.3.4-10, DSN Information Signals.

5.3.4.10.2.5.4.1 If, after receiving the precedence call waiting signal, the busy called IP end instrument does not answer the incoming call within the maximum programmed time interval, the AS-SIP signaling appliance serving the IP end instrument MUST provide a global default diversion to a designated directory number (e.g., Attendant Console).

5.3.4.10.2.5.4.a In the case of an IP end instrument for which the user has NOT activated call forwarding, if a precedence call is sent to an IP end instrument that is busy with a lower precedence call, then the existing lower precedence call MUST be preempted and the incoming call shall be established.

5.3.4.10.2.5.4.b In the case of an IP end instrument for which the user has activated call forwarding busy, if a precedence call is sent to an IP end instrument that is busy with a lower precedence call (or calls if three-way calling is established), then the existing call (or 3-way call) at the busy station MUST be preempted and the incoming call established, i.e., the Call Forwarding service shall not be invoked.

5.3.4.10.2.5.5 In the case of an IP end instrument for which the user has activated call forwarding busy, if a precedence call is sent to an IP end instrument that is busy with a higher or equal precedence call or calls, then the Call Forwarding service MUST be invoked.

5.3.4.10.2.5.5.1 The precedence level of calls is preserved during the forwarding process, and the forwarded-to user may be preempted.

5.3.4.10.2.5.5.2 If Call Forwarding Busy has been activated by the called party and the called party has specified a forwarded-to party, the forwarding procedure MUST be performed. If a precedence call is forwarded (including possible multiple forwarding) and is not responded to by any forwarded-to party (e.g., called party busy with a call of equal or higher precedence level; or called party busy and nonpreemptable) within a specified period of time (typically 30 seconds), the AS-SIP signaling appliance serving the called party shall divert the precedence call to the attendant.

5.3.4.10.2.5.6 In the case of an IP end instrument for which the user has activated call forwarding on no answer the precedence level of calls MUST be preserved during the forwarding process and the forwarded to user may be preempted.

5.3.4.10.2.5.7 In the case of an IP end instrument for which the user has activated call forwarding on no answer and has specified a forwarded-to party, the forwarding procedure MUST be performed. If a precedence call is forwarded (including possibly multiple forwarding) and is not responded to by any forwarded-to party (e.g., called party busy with a call of equal or higher precedence level; or called party busy and nonpreemptable) within a specified period of time (typically 30 seconds), the AS-SIP signaling appliance serving the called party shall divert the precedence call to the attendant.

5.3.4.10.2.6 Call Origination Busy

5.3.4.10.2.6.1 Whenever there is only one appearance remaining on an end instrument and a user initiates the sequence of events to make an outbound call (e.g., goes off-hook, or inputs the first dialing digit, or invokes the telephony communication program and selects the number to dial on a telephony computer screen), then:

5.3.4.10.2.6.1.1 In the event the inbound call request is routine the inbound call request will be rejected. A 486 (Busy Here) response will be sent back to the originating AS-SIP signaling appliance.

5.3.4.10.2.6.1.2 In the event of an inbound precedence call request whose precedence level is higher than that of an existing call on at least one occupied appearance then the end instrument shall conduct the standard endpoint preemption process on the lowest such occupied appearance.

5.3.4.10.2.6.1.3 In the event of an inbound precedence call request whose precedence level is lower than or equal to all existing occupied appearances on the end instrument or in the event the end instrument only has one appearance then the end instrument SHALL implement one of the following two alternatives:

5.3.4.10.2.6.1.3.1 Alternative1. Refrain from acting on the inbound request until the user has either completed the dialing sequence for the outbound call or at least completed input of the precedence level information for the outbound call request so that the priority level of the outbound call request can be compared to the priority level of the inbound call request.

5.3.4.10.2.6.1.3.1.1 If the inbound precedence call request has a higher priority than the outbound call request then the inbound call request will preempt the outbound call request.

5.3.4.10.2.6.1.3.1.2 If the inbound precedence call request has a priority less than or equal to the outbound request then the outbound call request will proceed and upon successful establishment of the outbound call the subsequent called party actions shall be as specified in UCR 2008 Section 5.3.4.10.2.5, Precedence Call Rules.

5.3.4.10.2.6.1.3.1.3 If the outbound precedence call cannot be successfully established then upon termination of the attempted outbound call establishment (e.g., caller goes on-hook), a precedence ringing tone will be played to alert the called party of the inbound precedence call request.

5.3.4.10.2.6.1.3.2 Alternative 2. The inbound precedence call request is sent to the global default diversion number.

5.3.4.10.3 ASAC Preemption Requirements

If a session has to be preempted to support a higher precedence session, the use of the Reason Header shall be in accordance with RFC 4411 and RFC 3326 as modified in this generic requirement.

Preemption can only take place for sessions of the same precedence domain. In other words, a precedence call request can only preempt an existing call or call request that has the same value for its precedence-domain subfield.

5.3.4.10.3.1 Reason Header for Preemption

5.3.4.10.3.1.1 The AS-SIP signaling appliances MUST support the Reason header field [RFC 3326] for use, at a minimum, with the BYE request, the CANCEL request, the 480 (Temporarily Unavailable) response, 486 (Busy Here), and the 488 (Not Acceptable Here) response.

5.3.4.10.3.1.2 The syntax for the Reason header field is found in RFC 3326, Section 2, The Reason Request Header Field, and is repeated herein for the reader's convenience:

```
Reason           =  "Reason" HCOLON reason-value *(COMMA reason-value)
reason-value     =  protocol *(SEMI reason-params)
protocol         =  "SIP" / "Q.850" / token
reason-params    =  protocol-cause / reason-text / reason-extension
protocol-cause   =  "cause" EQUAL cause
cause            =  1*DIGIT
reason-text      =  "text" EQUAL quoted-string
reason-extension =  generic-param
```

5.3.4.10.3.1.3 For purposes of preemption, AS-SIP signaling appliances MUST support the reason-value "Preemption" and the four Reason-params defined in RFC 4411, Section 5, Preemption Reason Header Cause Codes and Semantics.

Reason: preemption ;cause=1 ;text="UA Preemption"
Reason: preemption ;cause=2 ;text="Reserved Resources Preempted"
Reason: preemption ;cause=3 ;text="Generic Preemption"
Reason: preemption ;cause=4 ;text="Non-IP Preemption"

5.3.4.10.3.1.4 In addition, as the current set of Reason-params in RFC 4411 fails to fully meet our needs, the AS-SIP signaling appliances MUST support a fifth Reason-param intended to characterize a network preemption event that occurs in the IP portion of the network but is not due to a RSVP preemption occurrence:

Reason: preemption; cause=5; text="Network Preemption"

The appropriate usage of the preemption Reason-params is described in the following paragraphs.

5.3.4.10.3.2 Preemption at the IP End Instrument

5.3.4.10.3.2.1 General Preemption Rules for Behavior at IP End Instruments

5.3.4.10.3.2.1.1 When the precedence-domain subfield of the Resource-Priority header field of the incoming precedence call request is different from the precedence-domain of the existing call at the IP end instrument, then the incoming precedence call request MUST not preempt the existing call. Instead, the AS-SIP signaling appliance serving the called IP end instrument MUST provide a global default diversion to a designated directory number (e.g., Attendant Console).

5.3.4.10.3.2.1.1a When a precedence call request is sent to an AS-SIP signaling appliance and intended for a served non-preemptable IP end instrument that is busy with another call, then the AS-SIP signaling appliance serving the called IP end instrument MUST provide a global default diversion to a designated directory number (e.g., Attendant Console). In the event the call request cannot be directed to a designated directory number and is rejected, then the response will be a 480 (Temporarily Unavailable) with either no Reason header or a Reason header that does NOT have a preemption cause.

NOTE: When the AS-SIP signaling appliance serving the calling IP end instrument receives the 480 (Temporarily Unavailable) response, it MUST send a Busy Not Equipped Announcement (BNEA), and then a termination message to the served calling IP end instrument.

NOTE: For completeness, it should be noted that when an AS-SIP signaling appliance serving a calling IP end instrument receives an inbound 486 (Busy Here) response code or a 488 (Not Acceptable Here) response code (see UCR 2008, Section 5.3.4.10.3.3, Network Preemption) with either no Reason header or a Reason header that does NOT have a preemption cause for an outbound precedence call request, then the AS-SIP signaling appliance MUST send a BPA to the served calling IP end instrument, and then send a termination message to end the call request.

5.3.4.10.3.2.1.2 When a precedence call request is sent to a preemptable IP end instrument that is busy with a call of lower precedence (having no idle appearances and having the same value for the precedence-domain subfield), then the lower precedence call MUST be preempted (regardless of whether the lower precedence call and the new higher precedence call request are of the same media type; in other words, in endpoint preemption a lower precedence audio call will be preempted by a higher precedence audio call request or a higher precedence video call request and a lower precedence video session will be preempted by a higher precedence video session request or a higher precedence audio call request). The active busy IP end instrument MUST receive a continuous preemption tone until an on-hook signal is received and the other party shall receive a preemption tone for a minimum of 3 seconds. After going on-hook, the station to which the precedence call is directed MUST be provided with precedence ringing and the calling party MUST receive an audible ringback precedence tone. When the called IP end instrument goes back off-hook, it MUST be connected to the preempting call. (Details of this scenario are described in UCR 2008, Section 5.3.4.10.3.2.2, Required Behavior at Called IP End Instrument When Active Call is Preempted by Higher Precedence Call Request). See Table 5.3.4-10, DSN Information Signals, for details on the preemption tone, ringing signal, and the audible ringback precedence call tone.

5.3.4.10.3.2.1.3 Reserved

5.3.4.10.3.2.1.4 Whenever an AS-SIP signaling appliance performs an endpoint preemption of an existing call for a served IP end instrument, the AS-SIP signaling appliance MUST NOT consider the existing call to be terminated until the AS-SIP signaling appliance has received an acknowledgement from its local IP end instrument that the call has been terminated (e.g., in the case of a SIP end instrument this means receiving a 200 OK to a BYE) and until the AS-SIP signaling appliance has received a 200 OK to the BYE sent to the remote AS-SIP signaling appliance serving the remote IP end instrument whose call is being preempted.

5.3.4.10.3.2.1.5 Whenever an AS-SIP signaling appliance performs an endpoint preemption of an inbound call request for a served IP end instrument, the AS-SIP signaling appliance MUST NOT consider the existing call request to be terminated until the AS-SIP signaling appliance has received an acknowledgement from its local IP end instrument that the call has been terminated (e.g., in the case of a SIP end instrument receiving a 200 OK to a BYE or a 200 OK to a

CANCEL followed by a 487 Request Terminated to the INVITE) and until the AS-SIP signaling appliance has received an ACK to the 486 response code (which has a Reason header where the Reason-params has the value preemption ;cause=1 ;text="UA Preemption") sent to the remote AS-SIP signaling appliance serving the remote IP end instrument whose call is being preempted.

NOTE: If the local SIP end instrument is RFC 2543 compliant but not RFC 3261 compliant it will not send a 487 Request Terminated and the local AS-SIP signaling appliance will consider the call leg with the local SIP end instrument terminated upon receipt of the OK to the CANCEL.

5.3.4.10.3.2.1.6 Whenever an AS-SIP signaling appliance performs an endpoint preemption of an outbound call request for a served IP end instrument, the AS-SIP signaling appliance MUST NOT consider the existing call request to be terminated until the AS-SIP signaling appliance has received an acknowledgement from its local IP end instrument that the call has been terminated (e.g., in the case of a SIP end instrument receiving a 200 OK to a BYE) and has received a 200 OK to the BYE or a 200 OK to a CANCEL from the remote AS-SIP signaling appliance serving the remote IP end instrument whose call is being preempted.

NOTE: Since RFC 2543 compliant SIP appliances do not send a 487 (Request Terminated) if the local AS-SIP signaling appliance were to wait for a 487 Request Terminated from the far end that is not being sent, the delay until the call could technically be considered to have been cancelled is 64*T1 seconds (where T1 is defined in RFC 3261, Section 17.1.1.1). Hence we will consider the call terminated upon the receipt of the 200 OK.

5.3.4.10.3.2.2 Required Behavior at Called IP End Instrument When Active Call is Preempted by Higher Precedence Call Request

5.3.4.10.3.2.2.1 Whenever an AS-SIP signaling appliance receives a call request intended for a served IP end instrument that has one line active with a call that is of lower precedence than the incoming call request (and has no idle appearances) then the active call MUST be preempted in accordance with the following behavior

5.3.4.10.3.2.2.1.1 The active IP end instrument MUST receive a continuous preemption tone until an on-hook signal is received (see Table 5.3.4-10, DSN Information Signals).

5.3.4.10.3.2.2.1.2 The other party to the active call MUST receive a preemption tone for at least 3 seconds (see Table 5.3.4-10, DSN Information Signals).

5.3.4.10.3.2.2.1.3 When the user places the active IP end instrument receiving the continuous preemption tone on-hook, the user MUST receive a precedence ringing tone (see Table 5.3.4-10, DSN Information Signals).

5.3.4.10.3.2.2.1.4 When the user places the active IP end instrument on-hook, the calling party of the new call request MUST receive an audible ringback precedence tone (see Table 5.3.4-10, DSN Information Signals).

5.3.4.10.3.2.2.1.5 When the user goes back off-hook, the new higher precedence call is established.

NOTE: If call waiting is assigned on the active line, it MUST be ignored and the preemption MUST proceed.

Multiple Appearances

5.3.4.10.3.2.2.1a **[FY2008-FY2010]** IP end instruments MUST be limited to two (2) appearances per directory number and limited to, at most, two (2) directory numbers.

5.3.4.10.3.2.2.2 Whenever an AS-SIP signaling appliance receives a call request intended for a served IP end instrument that has multiple appearances and one directory number, then

5.3.4.10.3.2.2.2.1 If the incoming call request has a higher precedence than an existing call and there is at least one call appearance not in use, then a precedence ringing tone MUST be provided on an unused call appearance. The called party has the option of placing the current call on hold and picking up the incoming precedence call or ignoring the call. The calling party MUST be provided with an audible ringback precedence call tone (see Table 5.3.4-10, DSN Information Signals).

5.3.4.10.3.2.2.2.2 If the incoming call request has a higher precedence (and the same value for the precedence domain subfield)[1] than one or more existing calls (even existing calls that are on hold) but all call appearances are in use, then the existing lowest precedence call is preempted. The lowest precedence call MUST be preempted regardless of whether the lowest precedence call and the new higher precedence call request are of the same media type; in other words, a lowest precedence audio call is preempted by a higher precedence audio call request or a higher precedence video call request and the lowest precedence video session is preempted by a higher precedence video session request or a higher precedence audio call request.

5.3.4.10.3.2.2.2.3 When the existing lowest precedence call is a held call, then a preemption tone is sent to both the held caller and to the corresponding appearance on the IP end instrument of the destination directory number that has placed the call on hold. After a preset time, the held call is cleared and a precedence ring is provided to the corresponding appearance on the

[1] In the FY2008-FY2012 time frame there is only 1 valid value for the precedence domain subfield (i.e. "000000') therefore in the FY2008-FY2012 time period the value of the precedence domain subfield will never prevent the higher precedence inbound call request from preempting an existing lower precedence call at the end instrument.

destination directory number of the IP end instrument. Then the user hears the precedence ringing, indicating that the call on hold has been dropped. The user also sees the precedence level of this new call on the station set display. The user has the option of answering the call, letting it forward to an alternate party, and/or letting it divert to an attendant. The calling party MUST be provided with an audible ringback precedence call tone (see Table 5.3.4-10, DSN Information Signals).

5.3.4.10.3.2.2.2.4 When an existing active call has the lowest precedence, a preemption tone is sent to the active call and the destination directory number. When the user goes on-hook, a precedence ring is received indicating the incoming precedence call. The calling party MUST be provided with an audible ringback precedence call tone (see Table 5.3.4-10, DSN Information Signals).

5.3.4.10.3.2.2.3 Whenever an AS-SIP signaling appliance receives a call request intended for a served IP end instrument that has multiple appearances and two directory numbers, then the preemption behavior for each directory number and its multiple appearances is the same as described previously in Requirement 5.3.4.10.3.2.2.2 for an IP end instrument that has multiple appearances and one directory number.

5.3.4.10.3.2.3 Implementing Preemption on Behalf of Called IP End Instruments

Endpoint Preemption of an Active Call

5.3.4.10.3.2.3.1 Whenever an AS-SIP signaling appliance initiates an endpoint preemption of an active call on behalf of a called IP end instrument, then the AS-SIP signaling appliance MUST:

5.3.4.10.3.2.3.1.1 Activate user signaling (i.e., preemption tone) at the local IP end instrument where the existing call is being preempted.

5.3.4.10.3.2.3.1.2 Send a BYE request with a Reason header where the Reason-params has the value preemption ;cause=1 ;text="UA Preemption" over the IP network toward the other AS-SIP signaling appliance serving the remote IP end instrument whose call is being preempted. The AS-SIP signaling appliance serving the remote IP end instrument MUST activate the preemption tone at the IP end instrument for at least 3 seconds and then signal the IP end instrument that the session is being terminated.

5.3.4.10.3.2.3.1.3 The AS-SIP signaling appliance serving the local IP end instrument that is experiencing the IP endpoint preemption will receive a 200 (OK) response code.

5.3.4.10.3.2.3.1.4 When the local IP end instrument goes on-hook the AS-SIP signaling appliance activates user signaling (i.e., precedence ringing tone) at the local IP end instrument

and sends a 180 Ringing to the remote AS-SIP signaling appliance serving the calling IP end instrument whose precedence call request has initiated the endpoint preemption. The remote AS-SIP signaling appliance will activate user signaling (i.e., precedence ringback tone) to the calling IP end instrument and the call setup for the precedence call request continues as usual.

Endpoint Preemption of an Inbound Call Request

5.3.4.10.3.2.3.2 Whenever an AS-SIP signaling appliance performs an endpoint preemption of an inbound call request on behalf of a called IP end instrument (e.g. The AS-SIP signaling appliance has forwarded the INVITE to the end instrument and may have received a 180 ringing but has not received a 200 OK), then the AS-SIP signaling appliance MUST:

5.3.4.10.3.2.3.2.1 Send a termination message to the local IP end instrument to end the current inbound call request that is being preempted in favor of the new higher precedence call request. The termination message will terminate the ringing tone.

NOTE: There is no particular purpose to playing the preemption tone as the phone is on-hook.

5.3.4.10.3.2.3.2.2 Send a 486 (Busy Here) response code and a Reason header where the Reason-params has the value preemption ;cause=1 ;text="UA Preemption" over the IP network toward the remote AS-SIP signaling appliance serving the IP end instrument that initiated the call request being preempted. The remote AS-SIP signaling appliance will interrupt the user signaling (i.e., ringback) to the IP end instrument whose call request is being preempted. The AS-SIP signaling appliance activates a preemption tone for 3 seconds and then signals the IP end instrument that the session is being terminated.

5.3.4.10.3.2.3.2.3 The local AS-SIP signaling appliance will receive an ACK response to the 486 (Busy Here) response code.

5.3.4.10.3.2.3.2.4 The local AS-SIP signaling appliance will continue the call setup for the higher precedence call by activating user signaling at the local IP end instrument (i.e., precedence ringing tone), sending a 180 (Ringing) response to the remote AS-SIP signaling appliance serving the higher precedence call request, and so forth.

Endpoint Preemption of an Outbound Call Request

5.3.4.10.3.2.3.3 Whenever an AS-SIP signaling appliance performs an endpoint preemption of an outbound call request on behalf of an IP end instrument that has not received a 2xx response, then the AS-SIP signaling appliance MUST:

5.3.4.10.3.2.3.3.1 Interrupt current user signaling associated with the outbound call request (e.g., ringback) and activate user signaling (i.e., preemption tone) at the local IP end instrument where the existing call is being preempted.

5.3.4.10.3.2.3.3.2 If an early dialog has been established, send a BYE or CANCEL request with a Reason header where the Reason-params has the value preemption ;cause=1 ;text="UA Preemption" to the AS-SIP signaling appliance serving the called IP end instrument at the other end of the preempted call request. The remote AS-SIP signaling appliance will terminate the call that deactivates the ringing tone.

NOTE: There is no particular purpose to playing the preemption tone for 3 seconds prior to terminating the call unless the AS-SIP signaling appliance has received a 200 OK (or equivalent) from its local IP end instrument indicating the phone is off-hook.

5.3.4.10.3.2.3.3.3 If an early dialog has NOT been established, send a CANCEL request with a Reason header where the Reason-params has the value preemption ;cause=1 ;text="UA Preemption" to the AS-SIP signaling appliance serving the called IP end instrument in the preempted call request. (Note: If the AS-SIP signaling appliance has not received any provisional response it MUST wait to receive a provisional response before sending the CANCEL. In the event the first response is a final response then the AS-SIP signaling appliance sends a BYE instead of a CANCEL) The remote AS-SIP signaling appliance will terminate the call that deactivates the ringing tone.

NOTE: There is no particular purpose to playing the preemption tone for 3 seconds prior to terminating the call unless the AS-SIP signaling appliance has received a 200 OK (or equivalent) from its local IP end instrument indicating the phone is off-hook.

5.3.4.10.3.2.3.3.4 The AS-SIP signaling appliance will receive a 200 (OK) response code to the BYE or CANCEL request. In the case of a CANCEL request the AS-SIP signaling appliance will generally receive a 487 Request Terminated to the INVITE request. However, since RFC 2543 compliant SIP appliances do not send a 487 (Request Terminated) if the local AS-SIP signaling appliance were to wait for a 487 (Request Terminated) from the far end that is not being sent, the delay until the call could technically be considered to have been cancelled is 64*T1 seconds (where T1 is defined in RFC 3261, Section 17.1.1.1). Hence we will consider the call terminated upon the receipt of the 200 OK.

5.3.4.10.3.2.3.3.5 Upon the receiver going on-hook, the local AS-SIP signaling appliance will continue the call setup for the higher precedence call by activating user signaling at the local IP end instrument (i.e., precedence ringing tone), sending a 180 (Ringing) response to the remote AS-SIP signaling appliance, and continuing call establishment as usual.

Remote AS-SIP Signaling Appliance Response to Notification of IP Endpoint Preemption

5.3.4.10.3.2.3.4 Whenever an AS-SIP signaling appliance receives an inbound BYE request with a Reason Header whose Reason-params has the value preemption ;cause=1 ;text="UA Preemption" intended to preempt an existing call, then:

5.3.4.10.3.2.3.4.1 If the served IP end instrument is a SIP end instrument, the AS-SIP signaling appliance activates the user signaling requirements (e.g., sends a preemption tone for a minimum of 3 seconds), and then sends the BYE request to the SIP end instrument to terminate the session. The SIP end instrument responds back with a 200 (OK) that the AS-SIP signaling appliance forwards over the IP network.

5.3.4.10.3.2.3.4.2 If the served IP end instrument is an H.323 or proprietary IP end instrument, the AS-SIP signaling appliance activates the user signaling requirements (e.g., sends a preemption tone for a minimum of 3 seconds), sends a termination signaling message to the IP end instrument to terminate the session, and responds back over the network with a 200 (OK).

5.3.4.10.3.2.3.5 Whenever an AS-SIP signaling appliance receives an inbound 486 (Busy Here) response code with a Reason header where the Reason-params has the value preemption ;cause=1 ;text="UA Preemption" for an outbound call request (i.e. the AS-SIP signaling appliance is serving an IP end instrument that initiated a call request (which has not completed) and the far end is conducting endpoint preemption) then:

5.3.4.10.3.2.3.5.1 If the served IP end instrument is a SIP end instrument, the AS-SIP signaling appliance deactivates the user signaling (i.e., ringback), activates a preemption tone for 3 seconds, then sends the 486 (Busy Here) response to the SIP end instrument to terminate the session. The SIP end instrument returns an ACK that the AS-SIP signaling appliance forwards over the network.

5.3.4.10.3.2.3.5.2 If the served IP end instrument is an H.323 or proprietary IP end instrument, the AS-SIP signaling appliance deactivates the user signaling (i.e., ringback), activates a preemption tone for 3 seconds, then conducts call termination with the IP end instrument. The AS-SIP signaling appliance sends an ACK back over the network.

5.3.4.10.3.2.3.6 Whenever an AS-SIP signaling appliance receives an inbound BYE request (or an inbound CANCEL request) with a Reason Header whose Reason-params has the value preemption ;cause=1 ;text="UA Preemption" for an inbound call request in the process of session establishment (receiver is still on-hook), then:

5.3.4.10.3.2.3.6.1 If the served IP end instrument is a SIP end instrument, the AS-SIP signaling appliance sends the BYE request (or CANCEL request) to the SIP end instrument to terminate

the call (and deactivate the ringing tone). The SIP end instrument returns a 200 OK which the AS-SIP signaling appliance forwards over the network. In the case of a CANCEL request the SIP end instrument will generally return a 487 (Request Terminated) to the INVITE which the AS-SIP signaling appliance will forward over the network.

5.3.4.10.3.2.3.6.2 If the served IP end instrument is an H.323 or proprietary IP end instrument, the AS-SIP signaling appliance sends a termination signaling message to the IP end instrument to terminate the session and deactivate the ringing tone. The AS-SIP signaling appliance responds back over the network with a 200 OK. In the case of a CANCEL request the AS-SIP signaling appliance sends a 487 (Request Terminated) to the remote AS-SIP signaling appliance (for the INVITE).

5.3.4.10.3.3 Network Preemption

5.3.4.10.3.3.1 Circumstances under which an AS-SIP Signaling Appliance Performs Network Preemption

5.3.4.10.3.3.1.1 When an AS-SIP signaling appliance receives an outbound precedence call request from a served IP end instrument and there are insufficient resources to support the outbound precedence call request (e.g., call count threshold has been reached for the link), the AS-SIP signaling appliance MUST compare the precedence level of the new precedence call request with the precedence levels of the existing calls and/or call requests to determine whether there are sufficient resources of lesser precedence that can be preempted to accommodate the new precedence call request. This comparison can only occur for calls and call requests having the same value for the precedence-domain subfield in the namespace of the Resource-Priority header field.

5.3.4.10.3.3.1.1.1 If there are no preemptable resources to accommodate the new precedence call request, the AS-SIP signaling appliance MUST reject the precedence call request. The AS-SIP signaling appliance is responsible for overseeing the playing of the BPA at the local IP end instrument followed by the termination of the call request. The BPA will indicate that the local AS-SIP signaling appliance blocked the precedence call.

NOTE: In the case of a local SIP end instrument, a suitable final non-2xx response to be sent by the AS-SIP signaling appliance (after the BPA) is a 488 (Not Acceptable Here) response code that SHOULD include a Warning header field with warning code 370 (Insufficient Bandwidth).

5.3.4.10.3.3.1.1.2 If there are sufficient resources that are preemptable, the AS-SIP signaling appliance MUST preempt existing call requests and calls using the following scheme:

- Identify the lowest priority call requests and calls having the same value for the precedence-domain subfield. If there is directionalization, then the set of preemptable call requests and calls consists only of those calls and call requests initiated in the same direction as the new precedence call request (i.e., a new outbound precedence call request is compared against other outbound call requests and calls; a new inbound precedence call request is compared against other inbound call requests and calls).

- Preempt call requests before preempting existing calls.

- If there are insufficient call requests and calls at the lowest priority to meet the preemption needs, then go to the next lowest priority level and preempt call requests before preempting existing calls (all of which MUST have the same value for the precedence-domain subfield).

- Repeat this process until the necessary resources have been freed up for the precedence call request. (NOTE: The AS-SIP signaling appliance has determined at the start that there were sufficient lesser precedence call requests and calls to satisfy the resource requirements of the precedence call request.)

The mechanism for selecting between call requests of a given priority level or between existing calls of a given priority level is left to the vendor with the caveat that the ordering scheme must be deterministic and must always be applied consistently. For example, if there are multiple call requests at the ROUTINE priority level, the AS-SIP signaling appliance may preempt call requests based on the most recent call request being preempted first or the oldest call request being preempted first. Whatever methodology is selected it is required that it be deterministic and that it be applied the same way every time. The AS-SIP signaling appliance MUST perform the network preemption per UCR 2008, Section 5.3.4.10.3.3.2, Implementing the Network Preemption, and then send the AS-SIP INVITE for the new precedence call request into the WAN. [Network Preemption]

5.3.4.10.3.3.1.2 When an AS-SIP signaling appliance receives an inbound precedence call request from a remote AS-SIP signaling appliance that is intended for a served IP end instrument and there are insufficient resources to support the inbound precedence call request (e.g., call count threshold has been reached for the link), the AS-SIP signaling appliance MUST compare the precedence level of the new precedence call request with the precedence levels of the existing calls and/or call requests to determine whether there are sufficient resources of lesser precedence that can be preempted to accommodate the new precedence call request. This comparison can only occur for calls and call requests having the same value for the precedence-domain subfield in the namespace of the Resource-Priority header field.

5.3.4.10.3.3.1.2.1 If there are no preemptable resources to accommodate the new precedence call request, the AS-SIP signaling appliance MUST reject the precedence call request by sending a 488 (Not Acceptable Here) response code that SHOULD include a Warning header field with warning code 370 (Insufficient Bandwidth) to the remote AS-SIP signaling appliance serving the calling IP end instrument. NOTE: The remote AS-SIP signaling appliance serving the calling IP end instrument will ensure that a BPA is played to its local IP end instrument and then terminate the call request. The BPA will notify the user that the call was blocked by a remote AS-SIP signaling appliance. The individual switch name and location of the preempting switch will not be conveyed to the user.

5.3.4.10.3.3.1.2.2 If there are sufficient resources that are preemptable, the AS-SIP signaling appliance MUST preempt existing call requests and calls as described in Requirement 5.3.4.10.3.3.1.1.2 (preempt lowest priority call requests before lowest priority existing calls, etc.). The AS-SIP signaling appliance MUST perform the network preemption per UCR 2008, Section 5.3.4.10.3.3.2, Implementing the Network Preemption. The AS-SIP signaling appliance will then forward the new precedence call request to its local IP end instrument. [Network Preemption]

5.3.4.10.3.3.2 Implementing the Network Preemption

5.3.4.10.3.3.2.1 Whenever an AS-SIP signaling appliance preempts an existing call of a served IP end instrument, the AS-SIP signaling appliance MUST NOT consider the existing call to be terminated until the AS-SIP signaling appliance has received an acknowledgement from its local IP end instrument that the call has been terminated (e.g., in the case of a SIP end instrument this means receiving a 200 OK to a BYE) and until the AS-SIP signaling appliance has received a 200 OK to the BYE sent to the remote AS-SIP signaling appliance serving the remote IP end instrument whose call is being preempted.

5.3.4.10.3.3.2.2 Whenever an AS-SIP signaling appliance preempts an inbound call request of a served IP end instrument, the AS-SIP signaling appliance MUST NOT consider the existing call request to be terminated until the AS-SIP signaling appliance has received an acknowledgement from its local IP end instrument that the call has been terminated (e.g., in the case of a SIP end instrument receiving a 200 OK to a BYE or a 200 OK to a CANCEL possibly followed by a 487 (Request Terminated) to the INVITE) and until the AS-SIP signaling appliance has received an ACK to the 488 response code sent to the remote AS-SIP signaling appliance serving the remote IP end instrument whose call is being preempted.

NOTE: In the case in which the AS-SIP signaling appliance sends a CANCEL to its local SIP end instrument, if the local SIP end instrument is RFC 2543 compliant but not RFC 3261 compliant, it will not send a 487 (Request Terminated) and the local AS-SIP signaling appliance

will consider the call leg with the local SIP end instrument terminated upon receipt of the OK to the CANCEL.

5.3.4.10.3.3.2.3 Whenever an AS-SIP signaling appliance preempts an outbound call request of a served IP end instrument, the AS-SIP signaling appliance MUST NOT consider the existing call request to be terminated until the AS-SIP signaling appliance has received an acknowledgement from its local IP end instrument that the call has been terminated (e.g., in the case of a SIP end instrument receiving an ACK to the 488 response) and has received a 200 OK to the BYE or a 200 OK to a CANCEL from the remote AS-SIP signaling appliance serving the remote IP end instrument whose call is being preempted.

NOTE: Since RFC 2543 compliant SIP appliances do not send a 487 (Request Terminated) if the AS-SIP signaling appliance were to wait for a 487 (Request Terminated) from the far end that is not being sent, the delay until the call could technically be considered to have been cancelled is 64*T1 seconds (where T1 is defined in RFC 3261, Section 17.1.1.1). Hence we will consider the call terminated upon the receipt of the 200 OK

Network Preemption of Active Call

5.3.4.10.3.3.2.4 Whenever an AS-SIP signaling appliance performs a network preemption of an active call, then the AS-SIP signaling appliance MUST:

5.3.4.10.3.3.2.4.1 Activate the preemption tone at the local IP end instrument for a minimum of 3 seconds and then send a termination message to the local IP end instrument.

NOTE: In the case of a local SIP end instrument it is recommended that after the preemption tone the AS-SIP signaling appliance send a SIP BYE request with a Reason header whose Reason-params has the value preemption ;cause=5 ;text="Network Preemption").

5.3.4.10.3.3.2.4.2 Send a BYE request with a Reason header where the Reason-params has the value preemption;cause=5 ;text="Network Preemption" over the IP network to the AS-SIP signaling appliance serving the remote IP end instrument in the preempted call. The remote AS-SIP signaling appliance will activate the preemption tone at its remote IP end instrument for a minimum of 3 seconds and then send a termination message to its IP end instrument.

5.3.4.10.3.3.2.4.3 The AS-SIP signaling appliance that initiated the network preemption will receive a 200 (OK) response code from the remote AS-SIP signaling appliance.

Network Preemption of an Inbound Call Request

5.3.4.10.3.3.2.5 Whenever an AS-SIP signaling appliance performs a network preemption of an inbound call request (receiver is on-hook), then the AS-SIP signaling appliance MUST:

5.3.4.10.3.3.2.5.1 Conduct call termination with the local IP end instrument that deactivates the ringing tone.

NOTE: In the case of a SIP end instrument, it is recommended that the AS-SIP signaling appliance send a SIP BYE request or CANCEL request (as appropriate) with a Reason header whose reason-params has the value preemption ;cause=5 ;text="Network Preemption").

5.3.4.10.3.3.2.5.2 Send a 488 (Not Acceptable Here) response code that SHOULD include a Warning header field with warning code 370 (Insufficient Bandwidth) with a Reason header whose Reason-params has the value preemption;cause=5 ;text="Network Preemption" over the IP network to the remote AS-SIP signaling appliance serving the remote IP end instrument in the preempted call. The remote AS-SIP signaling appliance deactivates the ringback tone on the remote IP end instrument, sends a preemption tone for a minimum of 3 seconds, and conducts call termination with the remote IP end instrument.

5.3.4.10.3.3.2.5.3 The AS-SIP signaling appliance that initiated the network preemption will receive an ACK response to the 488 (Not Acceptable Here) response code from the remote AS-SIP signaling appliance.

Network Preemption of an Outbound Call Request

5.3.4.10.3.3.2.6 Whenever an AS-SIP signaling appliance performs a network preemption of an outbound call request from a locally served IP end instrument that has not received a 2xx response, then the AS-SIP signaling appliance MUST:

5.3.4.10.3.3.2.6.1 Deactivate any user signaling (e.g. ringback), activate the preemption tone for a minimum of 3 seconds, and then conduct call termination.

5.3.4.10.3.3.2.6.2 If an early dialog has been established, send a BYE or CANCEL request with a Reason header where the Reason-params has the value preemption;cause=5 ;text="Network Preemption" to the remote AS-SIP signaling appliance serving the called IP end instrument in the preempted call request. The remote AS-SIP signaling appliance will conduct call termination with its IP end instrument that deactivates the user signaling (i.e., ringing tone).

NOTE: There is no particular purpose to playing the preemption tone for 3 seconds prior to terminating the call unless the AS-SIP signaling appliance has received a 200 OK from its local SIP end instrument indicating the phone is off-hook.

5.3.4.10.3.3.2.6.3 If an early dialog has not been established, send a CANCEL request with a Reason header where the Reason-params has the value preemption;cause=5 ;text="Network Preemption" to the remote AS-SIP signaling appliance serving the called IP end instrument in the preempted call request. (Note: If the AS-SIP signaling appliance has not received any provisional response it MUST wait to receive a provisional response before sending the CANCEL. In the event the first response is a final response then the AS-SIP signaling appliance sends a BYE instead of a CANCEL) The remote AS-SIP signaling appliance will conduct call termination with its IP end instrument which deactivates the user signaling (i.e. ringing tone).

NOTE: There is no particular purpose to playing the preemption tone for 3 seconds prior to terminating the call unless the AS-SIP signaling appliance has received a 200 OK from its local SIP end instrument indicating the phone is off-hook.

5.3.4.10.3.3.2.6.4 The AS-SIP signaling appliance that initiated the network preemption will receive a 200 (OK) response code to the BYE or CANCEL request from the remote AS-SIP signaling appliance.

5.3.4.10.4 ASAC Rule Set

NOTE: This section comprises the rules governing when to increment and decrement telephony and video call counts and assumes the necessary network resources are available.

UCR 2008, Section 5.3.4.10.3.3, Network Preemption, provides the rules for what an LSC must do when incrementing a call count that would exceed a configured threshold.

UCR 2008, Section 5.3.4.11, Policing of Call Count Thresholds, provides the rules by which a softswitch polices ASAC call counts.

5.3.4.10.4.1 LSC Component of Softswitch

The LSC component of a Softswitch MUST perform ASAC call counting in accordance with the ASAC rules defined in UCR 2008, Section 5.3.4.10.4, ASAC Rule Set.

5.3.4.10.4.1.1 Empty INVITE

5.3.4.10.4.1.1.1 Unless covered by the exception set forth in Requirement 5.3.4.10.4.1.1.1.1 when an LSC either receives a SIP INVITE from a served SIP end instrument that does not

include an sdp body (empty INVITE) or generates a SIP INVITE on behalf of a non-SIP IP end instrument that does not have an sdp body then the LSC MUST classify the call request for ASAC purposes as a telephony call and increment the telephony ASAC call count (or outbound telephony call count in the case of directionalization) by one (1).

5.3.4.10.4.1.1.1.1 An LSC that receives a SIP INVITE from a served SIP end instrument that does not include an sdp body but does include a Contact header with the media feature tag 'video,' or generates a SIP INVITE on behalf of a non-SIP IP end instrument that does not have an sdp body but does include a Contact header with the media feature tag 'video,' MAY increment the video ASAC call count (or outbound video call count) by at least one (1) VSU instead of incrementing the telephony call count (or outbound telephony call count). NOTE: Depending on the outcome of the offer-answer exchange the LSC may need to modify the number of VSUs (or outbound VSUs) allocated for the call.

5.3.4.10.4.1.1.2 Upon receipt of an inbound empty INVITE intended for a directly served IP end instrument an LSC MUST classify the call request for ASAC purposes as a telephony call and increment the telephony ASAC call count (or inbound telephony call count in the case of directionalization) by one (1) UNLESS:

5.3.4.10.4.1.1.2.1 The Contact header includes the media feature tag 'video' and the LSC is capable of processing the media feature tag, in which case the LSC MAY increment the video ASAC call count (or inbound video call count in the case of directionalization) by one (1) or more VSUs. If the end instrument responds by offering video capabilities greater than the number of VSUs just allocated for the call request, then the LSC MUST increment the video call count (or inbound video call count in the case of directionalization) by the additional VSUs necessary to cover the video offer.

NOTE: If the LSC initially increments the video ASAC call count by "n" VSUs, but the called end instrument responds with an offer for a telephony call, then the LSC MUST immediately decrement the video ASAC call count (or inbound video call count in the case of directionalization) by "n" VSUs, and then increment the telephony call count (or inbound telephony call count in the case of directionalization) by one (1).

NOTE: If the LSC initially classifies the call request as a telephony call (or an inbound telephony call in the case of directionalization), but the end instrument offers audio and video capabilities, then the LSC will decrement the telephony call count (or inbound telephony call count) and increment the video call count (or inbound video call count in the case of directionalization) by the appropriate number of VSUs and send a response that includes an sdp offer of audio and video capabilities.

5.3.4.10.4.2 LSC

5.3.4.10.4.2.1 Outbound INVITE and re-INVITE

Outbound INVITE

5.3.4.10.4.2.1.1 When the LSC receives a SIP INVITE from a served SIP end instrument or receives an outbound call request from a served non-SIP IP end instrument that is intended for a destination outside the enclave and the INVITE that is forwarded or generated includes an sdp offer specifying audio capabilities then the LSC increments the telephony call count (or outbound telephony call count in the case of directionalization) by one (1) and sends the INVITE to its Softswitch.

5.3.4.10.4.2.1.1a When the LSC receives a SIP INVITE from a served SIP end instrument or receives an outbound call request from a served non-SIP IP end instrument that is intended for a destination outside the enclave and the INVITE that is forwarded or generated includes an sdp offer specifying audio and video capabilities, then the LSC increments the video call count (or outbound video call count in the case of directionalization) by the appropriate number of VSUs and sends the INVITE to its Softswitch.

Outbound re-INVITE on Existing Telephony Call

5.3.4.10.4.2.1.2 When the LSC receives a SIP re-INVITE from a served SIP end instrument or receives an outbound call request from a served non-SIP IP end instrument (that will cause the LSC to generate a re-INVITE) AND the re-INVITE is intended for a destination outside the enclave AND the re-INVITE offers audio and video capabilities AND the existing call is budgeted against the telephony call count, THEN the LSC MUST increment the video call count (or outbound video call count) by the appropriate number of VSUs.

5.3.4.10.4.2.1.2.1 If the response to the re-INVITE is either a failure response (e.g., 4xx) or a 2xx response that rejects the video offer then upon receipt of the response the LSC decrements the video call count (or outbound video call count) by the number of VSUs that had been previously incremented.

5.3.4.10.4.2.1.2.2 If the response is a 2xx that accepts the video capabilities, then the LSC decrements the telephony call count by one (1) upon receipt of the 200.

NOTE: If the LSC uses directionalization, then the LSC MUST decrement the outbound telephony call count or inbound telephony call count depending upon the classification of the original call.

5.3.4.10.4.2.1.2.3 When the LSC receives a SIP re-INVITE from a served SIP end instrument or receives an outbound call request from a served non-SIP IP end instrument (that will cause the LSC to generate a re-INVITE) that is intended for a destination outside the enclave AND the re-INVITE offers audio capabilities only AND the existing call is budgeted against the telephony call count (or the outbound telephony call count or inbound telephony call count in the case of directionalization) THEN the LSC makes no change to the telephony call count (or outbound telephony call count or inbound telephony call count).

Outbound re-INVITE on Existing Video Call

5.3.4.10.4.2.1.4 When the LSC receives a SIP re-INVITE from a served SIP end instrument or receives an outbound call request from a served non-SIP IP end instrument (that will cause the LSC to generate a re-INVITE) and the re-INVITE is intended for a destination outside the enclave AND the re-INVITE offers audio capabilities only AND the existing call is budgeted against the video call count, THEN the LSC MUST increment the telephony call count (or outbound telephony call count) by 1.

5.3.4.10.4.2.1.4.1 If the response to the re-INVITE is either a failure response (e.g., 4xx) or a 2xx response that rejects the telephony offer then upon receipt of the response the LSC decrements the telephony call count (or outbound telephony call count) by one (1).

5.3.4.10.4.2.1.4.2 If the response is a 2xx that accepts the audio capabilities, then the LSC decrements the video call count by the appropriate number of VSUs upon receipt of the 200. NOTE: If the LSC uses directionalization, then the LSC MUST decrement the outbound video call count or inbound video call count depending upon the classification of the original call.

5.3.4.10.4.2.1.5 When the LSC receives a SIP re-INVITE from a served SIP end instrument or receives an outbound call request from a served non-SIP IP end instrument (that will cause the LSC to generate a re-INVITE) that is intended for a destination outside the enclave AND the re-INVITE offers audio and video capabilities AND the existing call is budgeted against the video call count (or the outbound video call count or inbound video call count in the case of directionalization) then:

5.3.4.10.4.2.1.5.1 If the proposed video call count is greater than the current video call count, the LSC MUST increment the video call count (or if the LSC uses directionalization, then the LSC increments the outbound video call count or inbound video call count depending on the classification of the original call) by the difference in VSUs between the proposed video call count and the current video call count.

5.3.4.10.4.2.1.5.1.1 If the response to the re-INVITE is either a failure response (e.g., 4xx) or a 2xx response that rejects the video offer then upon receipt of the response the LSC decrements the video call count by the amount of VSUs it had previously added to support the re-INVITE.

NOTE: If an existing video session requests the budget allocation to be increased (i.e. requesting a higher bandwidth video session) and the request is rejected either by the originating or terminating LSC, or the terminating video EI, then the session should not be terminated, but remain at its original session budgets.

5.3.4.10.4.2.1.5.2 If the proposed video call count is less than the current video call count, the LSC does not alter the video call count until receipt of the response to the offer.

5.3.4.10.4.2.1.5.2.1 If the response to the re-INVITE is either a failure response (e.g., 4xx) or a 2xx response that rejects the video offer then upon receipt of the response the LSC makes no change to the video call count.

5.3.4.10.4.2.1.5.2.2 If the response to the re-INVITE is a 200 accepting the offer, then the LSC reduces the video call count (or if the LSC uses directionalization, then the LSC decrements the outbound video call count or inbound video call count depending upon the classification of the original call) by the difference in VSUs between the proposed video call count and the current video call count.

Outbound BYE

5.3.4.10.4.2.1.6 When an LSC sends a BYE to its Softswitch intended for an IP end instrument outside the enclave, the LSC refrains from decrementing the call count associated with the given call until the LSC receives the 200 OK response to the BYE from the far end.

5.3.4.10.4.2.2 Inbound INVITE and re-INVITE

Inbound INVITE

5.3.4.10.4.2.2.1 When an LSC receives an inbound INVITE intended for a served IP end instrument that includes an sdp body offering only audio capabilities the LSC MUST classify the call request for ASAC purposes as a telephony call and increment the telephony call count (or inbound telephony call count in the case of directionalization) by one (1).

5.3.4.10.4.2.2.2 When an LSC receives an inbound INVITE intended for a served IP end instrument that includes an sdp body offering audio and video capabilities, the LSC MUST classify the call request for ASAC purposes as a video call and increment the video call count (or inbound video count in the case of directionalization) by the appropriate number of VSUs.

NOTE: If the end instrument accepts only the audio offer and therefore the initial response to the INVITE (be it a reliable provisional 18x response or a final 200 response) includes an sdp answer accepting only the audio offer, then the LSC MUST decrement the video call count (or inbound video call count in the case of directionalization) by the number of VSUs previously incremented and increment the telephony call count (or inbound telephony call count in the case of directionalization) by one (1).

Inbound re-INVITE on Existing Telephony Call

5.3.4.10.4.2.2.4 When the LSC receives a re-INVITE from outside the enclave, offering audio and video capabilities and intended for a served IP end instrument, AND the existing call is budgeted against the telephony call count, then the LSC MUST increment the video call count (or inbound video call count) by the appropriate number of VSUs and forward the video call request to the end instrument. If the user responds by accepting the video request, then the LSC decrements the telephony call count (or in the case of directionalization decrements the outbound telephony call count or inbound telephony call count depending upon the classification of the original call) by one (1). The LSC sends (or forwards) a 200 response with an sdp answer accepting the audio and video capabilities.

5.3.4.10.4.2.2.4.1 If the user does not accept the sdp offer or, in particular, the video capabilities in the sdp offer (e.g., end user did not accept video), then the LSC decrements the video call count (or inbound video call count) by the number of VSUs that had just previously been incremented. The LSC sends (or forwards) a 200 response with an sdp answer rejecting the audio and video capabilities.

5.3.4.10.4.2.2.5 When the LSC receives a re-INVITE from outside the enclave, offering audio capabilities only and intended for a served IP end instrument, AND the existing call is budgeted against the telephony call count, then the LSC makes no change to the ASAC call counts.

Inbound re-INVITE on Existing Video Call

5.3.4.10.4.2.2.6 When the LSC receives a re-INVITE from outside the enclave, offering audio capabilities only and intended for a served IP end instrument, AND the existing call is budgeted against the video call count, then the LSC MUST increment the telephony call count (or inbound telephony call count in the case of directionalization) by one (1), and forward the telephony call request to the end instrument. If the user responds by accepting the telephony call request, then the LSC decrements the video call count (or in the case of direcitonalization decrements the outbound video call count or inbound video call count depending on the classification of the original call) by the appropriate number of VSUs. The LSC sends (or forwards) a 200 response with an sdp answer accepting the audio capabilities.

5.3.4.10.4.2.2.6.1 If the user does not accept the sdp offer of audio capabilities only, then the LSC decrements the telephony call count (or inbound telephony call count) by one (1). The LSC sends (or forwards) a 200 response with an sdp answer rejecting the new audio capabilities.

5.3.4.10.4.2.2.7 When the LSC receives a re-INVITE from outside the enclave, offering audio and video capabilities and intended for a served IP end instrument, AND the existing call is budgeted against the video call count (or the outbound video call count or inbound video call count in the case of directionalization), then:

5.3.4.10.4.2.2.7.1 If the proposed video call count is greater than the current video call count, the LSC MUST increment the video call count (or if the LSC uses directionalization, then the LSC increments the outbound video call count or inbound video call count, depending on the classification of the original call), by the difference in VSUs between the proposed video call count and the current video call count, and forwards the video call request to the end instrument. If the end instrument accepts the video change, then the LSC sends (or forwards) a 200 response with an sdp answer accepting the change in video capabilities.

5.3.4.10.4.2.2.7.1.1 If the end instrument does not accept the change in video capabilities, then the LSC decrements the video call count (or in the case of directionalization decrements the inbound video call count or outbound video call count depending on the classification of the original call) by the number of VSUs it had just added previously. The LSC sends (or forwards) a 200 response with an sdp answer rejecting the new video capabilities.

5.3.4.10.4.2.2.7.2 If the proposed video call count is less than the current video call count, the LSC forwards the video call request to the end instrument and if the end instrument accepts the video change, then the LSC reduces the video call count (or if the LSC uses directionalization, then the LSC decrements the outbound video call count or inbound video call count depending on the classification of the original call) by the difference in VSUs between the proposed video call count and the current video call count and sends (or forwards) a 200 response with an sdp answer accepting the change in video capabilities.

5.3.4.10.4.2.2.7.2.1 If the end instrument does not accept the change in video capabilities, then the LSC makes no change to the ASAC video call count and sends (or forwards) a 200 response with an sdp answer rejecting the new video capabilities.

Inbound BYE

5.3.4.10.4.2.2.8 When an LSC receives a BYE from outside the enclave intended for a served IP end instrument, the LSC forwards the BYE or an equivalent termination message to its IP end instrument, decrements the call count associated with the given call, and sends the 200 OK response to the BYE back to its Softswitch.

5.3.4.10.4.3 Softswitch

5.3.4.10.4.3.1 Outbound INVITE and re-INVITE

Outbound INVITE

5.3.4.10.4.3.1.1 When the Softswitch receives an INVITE from a served LSC that includes an sdp offer specifying audio capabilities, then the Softswitch increments the telephony call count (or outbound telephony call count in the case of directionalization) by one (1).

5.3.4.10.4.3.1.1a When the Softswitch receives a SIP INVITE from a served LSC that includes an sdp offer specifying audio and video capabilities, then the Softswitch increments the video call count (or outbound video call count in the case of directionalization) by the appropriate number of VSUs.

5.3.4.10.4.3.1.1b When the Softswitch receives a SIP INVITE from a served LSC that does not include an sdp offer (Empty INVITE), then the Softswitch increments the telephony call count (or outbound telephony call count in the case of directionalization) by one (1).

Outbound re-INVITE on Existing Telephony Call

5.3.4.10.4.3.1.2 When the Softswitch receives a re-INVITE from a served LSC AND the re-INVITE offers audio and video capabilities AND the existing call is budgeted against the telephony call count, THEN the Softswitch MUST increment the video call count (or outbound video call count) by the appropriate number of VSUs.

5.3.4.10.4.3.1.2.1 If the response to the re-INVITE is either a failure response (e.g., 4xx) or a 200 response that rejects the video offer, then upon receiving the failure response or 200 response that does not accept the video portion of the offer, the Softswitch decrements the video call count (or outbound video call count) by the number of VSUs that had been incremented previously.

5.3.4.10.4.3.1.2.2 If the response is a 200 that accepts the video capabilities, then upon receiving the 200 response the Softswitch decrements the telephony call count by one (1). NOTE: If directionalization is being used, then the Softswitch MUST decrement the outbound telephony call count or inbound telephony call count depending on the classification of the original call.

5.3.4.10.4.3.1.3 When the Softswitch receives a re-INVITE from a served LSC AND the re-INVITE offers audio capabilities only AND the existing call is budgeted against the telephony call count (or the outbound telephony call count or inbound telephony call count in the case of

directionalization) THEN the Softswitch makes no change to the telephony call count (or outbound telephony call count or inbound telephony call count).

Outbound re-INVITE on Existing Video Call

5.3.4.10.4.3.1.4 When the Softswitch receives a re-INVITE from a served LSC AND the re-INVITE offers audio capabilities only AND the existing call is budgeted against the video call count THEN the Softswitch MUST increment the telephony call count (or outbound telephony call count) by one (1).

5.3.4.10.4.3.1.4.1 If the response to the re-INVITE is either a failure response (e.g., 4xx) or a 200 response that rejects the telephony offer, then upon receiving the failure response or 200 response that rejects the telephony offer the Softswitch decrements the telephony call count (or outbound telephony call count) by one (1).

5.3.4.10.4.3.1.4.2 If the response is a 200 that accepts the audio capabilities then upon receiving the 200 answer the Softswitch decrements the video call count by the appropriate number of VSUs. NOTE: If the LSC uses directionalization then the Softswitch MUST decrement the outbound video call count or inbound video call count depending upon the classification of the original call.

5.3.4.10.4.3.1.5 When the Softswitch receives a re-INVITE from a served LSC AND the re-INVITE offers audio and video capabilities AND the existing call is budgeted against the video call count (or the outbound video call count or inbound video call count in the case of directionalization), then:

5.3.4.10.4.3.1.5.1 If the proposed video call count is greater than the current video call count the Softswitch MUST increment the video call count (or if the LSC uses directionalization then the Softswitch increments the outbound video call count or inbound video call count depending on the classification of the original call) by the difference in VSUs between the proposed video call count and the current video call count.

5.3.4.10.4.3.1.5.1.1 If the response to the re-INVITE is either a failure response (e.g., 4xx) or a 200 response that rejects the video offer then upon receiving the failure response or 200 response that rejects the video offer the Softswitch decrements the video call count by the amount of VSUs it had previously added to support the re-INVITE.

5.3.4.10.4.3.1.5.2 If the proposed video call count is less than the current video call count the Softswitch does not alter the video call count until receipt of the response to the offer.

5.3.4.10.4.3.1.5.2.1 If the response to the re-INVITE is either a failure response (e.g., 4xx) or a 200 response that rejects the video offer then upon receiving the failure response or 200 response th,at rejects the video offer the Softswitch makes no change to the video call count.

5.3.4.10.4.3.1.5.2.2 If the response to the re-INVITE is a 200 accepting the offer, then upon receiving the 200 offer acceptance the Softswitch reduces the video call count (or if the LSC uses directionalization then the Softswitch decrements the outbound video call count or inbound video call count depending on the classification of the original call) by the difference in VSUs between the proposed video call count and the current video call count.

Outbound BYE

5.3.4.10.4.3.1.6 When a Softswitch receives a BYE from its served LSC, the Softswitch takes no action with regard to the ASAC count until it receives the 200 (OK) response to the BYE whereupon the Softswitch decrements the call count associated with the call being terminated.

5.3.4.10.4.3.2 Inbound INVITE and re-INVITE

Inbound INVITE

5.3.4.10.4.3.2.1 When the Softswitch receives an INVITE intended for a served LSC, the Softswitch takes no action with regard to ASAC until it receives a response from the served LSC and proceeds as follows:

5.3.4.10.4.3.2.1.1 If the INVITE had been an empty INVITE (i.e., no sdp offer), then the Softswitch increments the telephony count (or inbound telephony count) by one (1) if one of the following occur:

- The first provisional non-failure response (e.g., 1xx greater than (>) 100) has no sdp offer
- The first provisional response has an sdp offering audio capabilities
- The first response is a final response (200) with an sdp that offers audio capabilities

NOTE: See UCR 2008, Section 5.3.4.12, Video Telephony – General Rules, for examples of how the Softswitch modifies ASAC call count when the first provisional non-failure response has no sdp offer but the subsequent 200 final response offers audio and video capabilities.

5.3.4.10.4.3.2.1.2 If the INVITE had been an empty INVITE (i.e., no sdp offer), then the Softswitch increments the video call count (or inbound video call count) by the appropriate number of VSUs if one of the following occur:

- The first provisional response has an sdp offering audio and video capabilities
- The first response is a final response (200) with an sdp that offers audio and video capabilities

5.3.4.10.4.3.2.1.3 If the INVITE had an sdp offer advertising audio capabilities only, then the Softswitch increments the telephony count (or inbound telephony count) by one (1) if one of the following occur:

- The first provisional non-failure response (e.g., 1xx greater than (>) 100) has no sdp answer
- The first provisional response has an sdp answer accepting audio capabilities
- The first response is a final response (200) with an sdp that accepts audio capabilities

5.3.4.10.4.3.2.1.4 If the INVITE had an sdp offer advertising audio and video capabilities, then the Softswitch increments the telephony count (or inbound telephony count) by one (1) if the first provisional non-failure response (e.g., 1xx greater than (>) 100) has an sdp answer accepting audio only.

5.3.4.10.4.3.2.1.5 If the INVITE had an sdp offer advertising audio and video capabilities, then the Softswitch increments the video count (or inbound video count) by the appropriate number of VSUs if one of the following occur:

- The first provisional non-failure response (e.g., 1xx greater than (>) 100) has no sdp answer
- The first provisional response has an sdp answer accepting audio and video capabilities
- The first response is a final response (200) with an sdp that accepts audio and video capabilities

NOTE: See UCR 2008, Section 5.3.4.12, Video Telephony – General Rules, for examples of how the Softswitch modifies ASAC call count when the first provisional non-failure response has no sdp answer but the subsequent 200 final response accepts audio capabilities only.

5.3.4.10.4.3.2.1.6 If the response from the LSC is a failure response (e.g., 4x, 5xx, 6xx), then the Softswitch takes not action with respect to ASAC.

Inbound re-INVITE on Existing Telephony Call

5.3.4.10.4.3.2.2 When theSoftswitch receives a re-INVITE intended for a served LSC AND the sdp offers audio and video capabilities AND the existing call is budgeted against the telephony call count THEN the Softswitch takes no action with regard to ASAC until it receives a response from the served LSC and proceeds as follows:

5.3.4.10.4.3.2.2.1 If the Softswitch receives from its served LSC a 200 with an sdp answer that accepts the audio and video capabilities, then the Softswitch increments the video call count (or inbound video call count) by the appropriate number of VSUs and decrements the telephony call count (or if the LSC uses directionalization then the Softswitch decrements the outbound telephony call count or inbound telephony call count depending on the classification of the original call) by one (1).

5.3.4.10.4.3.2.2.2 If the Softswitch receives from its served LSC a failure response or a 200 with an sdp answer that does not accept the video capabilities, then the Softswitch makes no change to the ASAC call counts.

5.3.4.10.4.3.2.3 When the Softswitch receives a re-INVITE offering audio capabilities only and it is intended for a served LSC AND the existing call is budgeted against the telephony call count, then the Softswitch takes no action with regard to ASAC and will make no change to the ASAC call counts upon receiving from the served LSC either a 200 answer that accepts the audio offer or a 200 answer that rejects the audio offer or a final failure response.

Inbound re-INVITE on Existing Video Call

5.3.4.10.4.3.2.4 When the Softswitch receives a re-INVITE intended for a served LSC that has an sdp offering audio capabilities only AND the existing call is budgeted against the video call count, then the Softswitch takes no action with regard to ASAC until it receives a response from the served LSC and proceeds as follows:

5.3.4.10.4.3.2.4.1 If the Softswitch receives from its served LSC a 200 with an sdp answer that accepts the audio offer then the Softswitch increments the telephony call count (or inbound telephony call count) by one (1) and decrements the video call count (or if the LSC uses

directionalization then the Softswitch decrements the outbound video call count or inbound video call count depending upon the classification of the original call) by the appropriate number of VSUs.

5.3.4.10.4.3.2.4.2 If the Softswitch receives from its served LSC a failure response or a 200 with an sdp answer that does not accept the video capabilities then the Softswitch makes no change to the ASAC call counts.

5.3.4.10.4.3.2.5 When the Softswitch receives a re-INVITE intended for a served LSC that offers audio and video capabilities AND the existing call is budgeted against the video call count (or the outbound video call count or inbound video call count in the case of directionalization), then the Softswitch takes no action with regard to ASAC until it receives a response from the served LSC and proceeds as follows:

5.3.4.10.4.3.2.5.1 If the Softswitch receives from its served LSC a 200 with an sdp answer that accepts the video offer then:

5.3.4.10.4.3.2.5.1.1 If the proposed video call count is greater than the current video call count the Softswitch MUST increment the video call count (or if the LSC uses directionalization then the Softswitch increments the outbound video call count or inbound video call count depending upon the classification of the original call) by the difference in VSUs between the proposed video call count and the current video call count.

5.3.4.10.4.3.2.5.1.2 If the proposed video call count is less than the current video call count then upon receipt of the 200 response the Softswitch reduces the video call count (or if the LSC uses directionalization, then the Softswitch decrements the outbound video call count or inbound video call count depending on the classification of the original call) by the difference in VSUs between the proposed video call count and the current video call count.

5.3.4.10.4.3.2.5.1.3 If the Softswitch receives from its served LSC a failure response or a 200 with an sdp answer that does not accept the video capabilities then the Softswitch makes no change to the ASAC call counts.

Inbound BYE

5.3.4.10.4.3.2.6 When a Softswitch receives a BYE intended for a served LSC, the Softswitch takes no action with regard to the ASAC count until it receives the 200 (OK) response to the BYE from its served LSC whereupon the Softswitch decrements the call count associated with the call being terminated.

5.3.4.11 Policing of Call Count Thresholds

5.3.4.11.0.1 **[FY2008-FY2012]** When a Softswitch includes an LSC component (i.e., the Softswitch serves IP end instruments) the Softswitch is NOT required to conduct policing of its LSC component.

5.3.4.11.0.2 **[FY2012+]** In the post 2012 time frame, the Softswitch will be required to conduct policing of aggregate traffic thresholds exchanged over the DISN WAN and at that time the LSC component of a Softswitch MUST be included in the aggregate policing of traffic exchanged over the DISN WAN.

5.3.4.11.0.3 A Softswitch MUST be provisioned with full knowledge of each network domain and the set of valid r-priority values for each given network domain supported by every one of its subtended LSCs.

NOTE: For the FY2008-FY2012 time frame, the only valid network domain for the SBU network is "dsn" and the valid r-priority values are '0' routine, '2' priority, '4' immediate, '6' flash, '8' flash-override.

NOTE: For the FY2008-FY2012 time frame, the only valid network domain for the Classified network is "drsn" and the valid r-priority values are '0' routine, '2' priority, '4' immediate, '6' flash, '8' flash-override, '9' flash-override-override.

5.3.4.11.1 Policing of Telephony Calls and Call Requests

5.3.4.11.1.1 For each LSC served by a given Softswitch, the Softswitch MUST be provisioned with:

- IPB (the total budget of concurrent VoIP telephony calls and call requests that the LSC is permitted over the access link at any given time)

- IPBo (the total budget of outbound VoIP telephony calls and call requests that the LSC is permitted over the access link at any given time). Outbound VoIP telephony calls refers to calls initiated by end instruments served by LSC and destined for end instruments located outside the originating B/P/C/S and reached over the WAN.

- IPBi (the total budget of inbound VoIP telephony calls and call requests that the LSC is permitted over the access link at any given time). Inbound VoIP telephony calls refers to calls initiated by external end instruments, received over the WAN and destined for a local end instrument served by the LSC.

5.3.4.11.1.2 When there is no directionalization, then IPBo = IPBi = null, and when there is directionalization, then IPBo + IPBi MUST equal IPB.

5.3.4.11.1.3 Every Softswitch MUST be provisioned with the value of the VoIP telephony call budgets IPB, IPBo, and IPBi for each LSC served by the given Softswitch. The VoIP telephony call budgets for a given Softswitch MUST be updated whenever the VoIP telephony call budget for the corresponding LSC is updated.

5.3.4.11.1.4 **[FY2012+]** Every Softswitch MUST also calculate and store the value for the aggregate telephony budgets (IPBs) for the sum of the LSCs served by the given Softswitch.

5.3.4.11.1.5 **[FY2008-FY2012]** For each LSC served by a Softswitch, the Softswitch MUST continuously maintain a current accounting of:

- IPC – the total number of current telephony calls and outstanding telephony call requests for each LSC served by the Softswitch.
- IPCo – the total number of current outbound telephony calls and outstanding outbound telephony call requests for each LSC served by the Softswitch.
- IPCi – the total number of current inbound telephony calls and outstanding inbound telephony call requests for each LSC served by the Softswitch.

5.3.4.11.1.6 **[FY2012+]** Every Softswitch MUST also continuously maintain a current accounting of the aggregate active telephony call count and outstanding number of telephony call requests for the set of LSCs served by the given Softswitch.

5.3.4.11.1.7 Every Softswitch MUST be provisioned with knowledge of any network domain ID and the associated legitimate r-priority values supported by one or more of its assigned LSCs. This information MUST be updated as new network domain IDs are added by one or more of its assigned LSCs.

Policing of Outbound Telephony Call Requests

Outbound INVITE and re-INVITE

5.3.4.11.1.8 When the Softswitch receives an outbound routine (r-priority='0')–INVITE for a telephony call (that is either an initial INVITE or a re-INVITE where the existing call is a video session) from a served LSC that exceeds the telephony budget (the new call request means IPC greater than (>) IPB if no directionalization or IPCo greater than (>) IPBo if directionalization) the Softswitch MUST respond to the LSC with a 488 (Not Acceptable Here) response code that

SHOULD include a "Warning" header field with warning code 370 (Insufficient Bandwidth). An empty INVITE is also classified as a telephony call. The Softswitch takes no action with respect to ASAC in the case of a re-INVITE for a telephony call when the existing session is also a telephony call. The Softswitch MUST notify the network management system whenever the Softswitch rejects a routine, priority, or immediate telephony call request in order to compel adherence to a telephony call count threshold (see Requirements 5.3.4.11.1.16 and 5.3.4.11.1.17).

5.3.4.11.1.9 The Softswitch takes no action with respect to ASAC in the case of a re-INVITE for a telephony call when the existing session is also a telephony call. An empty INVITE is also classified as a telephony call. When the Softswitch receives an outbound precedence INVITE (i.e. priority level greater than routine) for a telephony call (that is either an initial INVITE or a re-INVITE where the existing call is a video session) from a served LSC that exceeds the telephony budget (new call request means IPC greater than (>) IPB if no directionalization or IPCo greater than (>) IPBo if directionalization) the LSC MUST:

- In the case of "no directionalization," preempt lower precedence telephony call requests and/or telephony calls to free up the necessary resources to support the precedence call request. (See Requirement 5.3.4.10.3.3.1.1.2 for details on the selection process for preempting lower precedence call requests and calls). The Softswitch MUST notify the network management system whenever Softswitch performs a network preemption in the context of its policing function to compel adherence to a telephony call count threshold (see Requirements 5.3.4.11.1.16 and 5.3.4.11.1.17). If the Softswitch is unable to preempt a call request or call on behalf of a precedence call request then the Softswitch MUST notify the network management system (see Requirements 5.3.4.11.1.16 and 5.3.4.11.1.17)

- In the case of "directionalization," preempt lower precedence outbound telephony call requests and/or telephony calls to free up the necessary resources to support the precedence call request. (See Requirement 5.3.4.10.3.3.1.1.2 for details on the selection process for preempting lower precedence call requests and calls). The Softswitch MUST notify the network management system whenever the Softswitch performs a network preemption in the context of its policing function to compel adherence to a telephony call count threshold (see Requirements 5.3.4.11.1.16 and 5.3.4.11.1.17). If the Softswitch is unable to preempt a call request or call on behalf of a precedence call request then Softswitch MUST notify the network management system (see Requirements 5.3.4.11.1.16 and 5.3.4.11.1.17).

- NOTE: An empty INVITE is also classified as a telephony call.

5.3.4.11.1.10 When the Softswitch receives an outbound INVITE for a telephony call (that is either an initial INVITE[2] or a re-INVITE where the existing call is a video session[3]) from a served LSC that exceeds the telephony budget (new call request means IPC greater than (>) IPB if no directionalization or IPCo greater than (>) IPBo if directionalization) and the outbound INVITE either does not have a Require header or has a Require header but not the option tag 'resource-priority' and has either an unrecognized network domain OR a known network domain but an invalid value for the r-priority field, then the Softswitch MUST respond with a 488 (Not Acceptable Here) response code that SHOULD include a "Warning" header field with warning code 370 (Insufficient Bandwidth). An empty INVITE is also classified as a telephony call. The Softswitch MUST notify the network management system that a telephony call request has been rejected in order to compel adherence to a telephony call count threshold (see Requirements 5.3.4.11.1.16 and 5.3.4.11.1.17) and either an unknown network domain ID or invalid value for the r-priority field was encountered, as the case may be.

5.3.4.11.1.11 When the Softswitch receives an outbound INVITE for a telephony call (that is either an initial INVITE[4] or a re-INVITE where the existing call is a video session[5]) from a served LSC and the outbound INVITE has a Require header with the option tag 'resource-priority' and has a Resource-Priority header with an unrecognized network domain then the Softswitch MUST respond with a 417 (Unknown Resource-Priority). The Softswitch MUST notify the network management system that a telephony call request with an invalid network domain has been rejected in order to compel adherence to a telephony call count threshold (see Requirements 5.3.4.11.1.16 and 5.3.4.11.1.17) and that an unknown network domain ID was encountered.

5.3.4.11.1.12 When the Softswitch receives an outbound INVITE for a telephony call (that is either an initial INVITE[6] or a re-INVITE where the existing call is a video session[7]) from a served LSC that exceeds the telephony budget (new call request means IPC greater than (>) IPB if no directionalization or IPCo greater than (>) IPBo if directionalization) and the outbound INVITE has a Require header with the option tag 'resource-priority' and has a Resource Priority header with a known network domain but an invalid value for the r-priority field then the Softswitch MUST respond with a 488 (Not Acceptable Here) that SHOULD include a "Warning" header field with warning code 370 (Insufficient Bandwidth). The Softswitch MUST notify the network management system that a telephony call request was rejected in order to

[2] An empty INVITE is also classified as a telephony call.
[3] The Softswitch takes no action with respect to ASAC in the case of a re-INVITE for a telephony call when the existing session is also a telephony call.
[4] An empty INVITE is also classified as a telephony call.
[5] The Softswitch takes no action with respect to ASAC in the case of a re-INVITE for a telephony call when the existing session is also a telephony call.
[6] An empty INVITE is also classified as a telephony call.
[7] The Softswitch takes no action with respect to ASAC in the case of a re-INVITE for a telephony call when the existing session is also a telephony call.

compel adherence to a telephony call count threshold (see Requirements 5.3.4.11.1.16 and 5.3.4.11.1.17) and that an invalid value for the r-priority field was encountered.

Policing of Inbound Telephony Call Requests

Inbound INVITE with sdp

5.3.4.11.1.13 When a Softswitch receives an inbound initial INVITE that advertises audio capabilities for a served LSC that is already at or in excess of its configured telephony budget (new call request means IPC greater than (>) IPB if no directionalization or IPCi greater than (>) IPBi if directionalization) then the Softswitch MUST forward the INVITE to the LSC.[8] The inbound call request is NOT classified as a call request that goes against the telephony call count threshold unless and until a 1xx greater than (>) 100 or 2xx response is received by the Softswitch from the served LSC and then proceeds as follows:

5.3.4.11.1.13.1 If the INVITE (in Requirement 5.3.4.11.1.13) had a Routine (r-priority = '0'), priority AND the Softswitch receives a 1xx greater than (>) 100 or 2xx response from its served LSC then the Softswitch MUST:

- Send a 488 (Not Acceptable Here) response code to the remote initiating party of the AS-SIP INVITE that SHOULD include a "Warning" header field with warning code 370 (Insufficient Bandwidth).

- Send a CANCEL request (in the case of a 1xx) or a BYE request (in the case of a 2xx) to the local LSC.

- Notify the network management system whenever a Routine, Immediate, or Priority level telephony call request is rejected in order to compel adherence to a telephony call count threshold (see Requirements 5.3.4.11.1.16 and 5.3.4.11.1.17).

5.3.4.11.1.13.2 If the INVITE (in Requirement 5.3.4.11.1.13) had a priority greater than routine (i.e. a precedence call) AND the Softswitch receives a 1xx greater than (>) 100 or 2xx response from its served LSC then the Softswitch MUST:

- In the case of "no directionalization," preempt lower precedence telephony call requests and/or telephony calls to free up the necessary resources to support the precedence call request. (See Requirement 5.3.4.10.3.3.1.1.2 for details on the selection process for preempting lower precedence call requests

[8] The LSC has primary responsibility for ensuring that the access link is in compliance with the call count threshold.

and calls). The Softswitch MUST notify the network management system whenever the Softswitch performs a network preemption in the context of its policing function to compel adherence to a telephony call count threshold (see Requirement 5.3.4.11.1.18).[9]

- In the case of "directionalization," preempt lower precedence inbound telephony call requests and/or telephony calls to free up the necessary resources to support the precedence call request. (See Requirement 5.3.4.10.3.3.1.1.2 for details on the selection process for preempting lower precedence call requests and calls). The Softswitch MUST notify the network management system whenever the Softswitch performs a network preemption in the context of its policing function to compel adherence to a telephony call count threshold (see Requirement 5.3.4.11.1.18).[10]

5.3.4.11.1.13.3 If the INVITE (in Requirement 5.3.4.11.1.13) did not have a Require header or had a Require header but not the option tag 'resource-priority' AND the Softswitch does not recognize the network domain or recognizes the network domain but the r-priority field does not have a valid value for the given network domain and the served LSC responds with a 1xx greater than (>) 100 or 2xx then the Softswitch MUST:

- Send a 488 (Not Acceptable Here) response code to the remote initiating party of the AS-SIP INVITE that SHOULD include a "Warning" header field with warning code 370 (Insufficient Bandwidth).

- Send a CANCEL request (in the case of a 1xx) or a BYE request (in the case of a 2xx) to the local LSC.

- Notify the network management system that a telephony call request was rejected in order to compel adherence to a telephony call count threshold (see Requirements 5.3.4.11.1.16 and 5.3.4.11.1.17) and that an unknown network domain ID or an invalid value for the r-priority field was encountered, as the case may be.

5.3.4.11.1.13.4 If the INVITE (in Requirement 5.3.4.11.1.13) had a Require header with the option tag 'resource-priority' AND does not recognize the value of the network domain and the served LSC responds with a 1xx greater than (>) 100 or 2xx, then the Softswitch MUST:

[9] If the Softswitch is unable to preempt a call request or call on behalf of a precedence call request then the Softswitch MUST notify the network management system (see Requirements 5.3.4.11.1.16 and 5.3.4.11.1.17).
[10] If the Softswitch is unable to preempt a call request or call on behalf of a precedence call request then the Softswitch MUST notify the network management system (see Requirements 5.3.4.11.1.16 and 5.3.4.11.1.17).

- Send a 417 (Unknown Resource-Priority) response code to the remote initiating party.

- Send a CANCEL request (in the case of a 1xx) or a BYE request (in the case of a 2xx) to the local LSC.

- Notify the network management system that a telephony call request was rejected in order to compel adherence to a telephony call count threshold (see Requirements 5.3.4.11.1.16 and 5.3.4.11.1.17) and that an unknown network domain ID was encountered.

5.3.4.11.1.13.5 If the INVITE (in Requirement 5.3.4.11.1.13) had a Require header with the option tag 'resource-priority' AND recognizes the network domain but the r-priority field does not have a valid value for the given network domain AND the served LSC responds with a 1xx greater than (>) 100 or 2xx then the Softswitch MUST:

- Send a 488 (Not Acceptable Here) response code to the remote initiating party of the AS-SIP INVITE that SHOULD include a "Warning" header field with warning code 370 (Insufficient Bandwidth).

- Send a CANCEL request (in the case of a 1xx) or a BYE request (in the case of a 2xx) to the local LSC.

- Notify the network management system that a telephony call request was rejected in order to compel adherence to a telephony call count threshold (see Requirements 5.3.4.11.1.16 and 5.3.4.11.1.17) and notify the network management system that an invalid value for the r-priority field was encountered.

Inbound Empty INVITE

5.3.4.11.1.14 When a Softswitch receives an inbound empty INVITE for a served LSC that is already at or in excess of its configured telephony budget (new call request means IPC greater than (>) IPB if no directionalization or IPCi greater than (>) IPBi if directionalization), then the Softswitch MUST forward the INVITE to the LSC.[11]

5.3.4.11.1.14.1 If the empty INVITE (in Requirement 5.3.4.12.1.14) had a priority level of Routine (r-priority = '0') AND the Softswitch receives either a 1xx greater than (>) 100 response

[11] The LSC has primary responsibility for ensuring that the access link is in compliance with the call count threshold.

having no sdp offer, a 1xx greater than (>) 100 response with an sdp offering audio capabilities only, or a 200 response with an sdp offering audio capabilities only then the Softswitch MUST:

- Send a 488 (Not Acceptable Here) response code to the remote initiating party of the AS-SIP INVITE that SHOULD include a "Warning" header field with warning code 370 (Insufficient Bandwidth).

- Send a CANCEL request (in the case of a 1xx) or a BYE request (in the case of a 2xx) to the local LSC.

- Notify the network management system whenever a Routine, Immediate, or Priority level telephony call request is rejected in order to compel adherence to a telephony call count threshold (see Requirements 5.3.4.11.1.16 and 5.3.4.11.1.17).

5.3.4.11.1.14.2 If the empty INVITE (in Requirement 5.3.4.11.1.14) had a priority level of Routine (r-priority = '0') AND the Softswitch receives either a 1xx greater than (>) 100 response with an sdp offering audio and video or a 200 response with an sdp offering audio and video capabilities AND the VSUs required for the new video session exceeds the video budget (the new session request means VDC greater than (>) VDB if no directionalization or VDCi greater than (>) VDBi if directionalization) then the Softswitch MUST:

- Send a 488 (Not Acceptable Here) response code to the remote initiating party of the AS-SIP INVITE that SHOULD include a "Warning" header field with warning code 370 (Insufficient Bandwidth).

- Send a CANCEL request (in the case of a 1xx) or a BYE request (in the case of a 2xx) to the local LSC.

- Notify the network management system whenever a Routine, Immediate, or Priority level video session request is rejected in order to compel adherence to a telephony call count threshold (see Requirements 5.3.4.11.1.16 and 5.3.4.11.1.17).

5.3.4.11.1.14.3 If the empty INVITE (in Requirement 5.3.4.11.1.14) was a precedence call request (i.e. had a priority level greater than routine) AND the Softswitch receives either a 1xx greater than (>) 100 response having no sdp offer, a 1xx greater than (>) 100 response with an sdp offering audio capabilities only, or a 200 response with an sdp offering audio capabilities only then the Softswitch MUST:

- In the case of "no directionalization," preempt lower precedence telephony call requests and/or telephony calls to free up the necessary resources to support the precedence call request. (See Requirement 5.3.4.10.3.3.1.1.2 for details on the selection process for preempting lower precedence call requests and calls). The Softswitch MUST notify the network management system whenever the Softswitch performs a network preemption in the context of its policing function to compel adherence to a telephony call count threshold (see Requirement 5.3.4.11.1.18).[12]

- In the case of "directionalization," preempt lower precedence inbound telephony call requests and/or telephony calls to free up the necessary resources to support the precedence call request. (See Requirement 5.3.4.10.3.3.1.1.2 for details on the selection process for preempting lower precedence call requests and calls). The Softswitch MUST notify the network management system whenever the Softswitch performs a network preemption in the context of its policing function to compel adherence to a telephony call count threshold (see Requirement 5.3.4.11.1.18).[13]

5.3.4.11.1.14.4 If the empty INVITE (in Requirement 5.3.4.12.1.14) had a priority level greater than routine (i.e. a precedence call) AND the Softswitch receives either a 1xx greater than (>) 100 response with an sdp offering audio and video capabilities or a 200 response with an sdp offering both audio and video capabilities AND the VSUs required for the new video session exceeds the video budget (the new session request means VDC greater than (>) VDB if no directionalization or VDCi greater than (>) VDBi if directionalization), then the Softswitch MUST:

- In the case of "no directionalization," preempt lower precedence video session requests and/or video sessions to free up the necessary resources to support the precedence session request. (See Requirement 5.3.4.10.3.3.1.1.2 for details on the selection process for preempting lower precedence call requests and calls). The Softswitch MUST notify the network management system whenever the Softswitch performs a network preemption in the context of its policing function to compel adherence to a video session count threshold (see Requirement 5.3.4.11.2.18).[14]

[12] If the Softswitch is unable to preempt a call request or call on behalf of a precedence call request then the Softswitch MUST notify the network management system (see Requirements 5.3.4.11.1.16 and 5.3.4.11.1.17).
[13] If the Softswitch is unable to preempt a call request or call on behalf of a precedence call request then the Softswitch MUST notify the network management system (see Requirements 5.3.4.11.1.16 and 5.3.4.11.1.17).
[14] If the Softswitch is unable to preempt a call request or call on behalf of a precedence call request then the Softswitch MUST notify the network management system (see Requirements 5.3.4.11.1.16 and 5.3.4.11.2.17).

- In the case of "directionalization," preempt lower precedence outbound video session requests and/or video session to free up the necessary resources to support the precedence session request. (See Requirement 5.3.4.10.3.3.1.1.2 for details on the selection process for preempting lower precedence call requests and calls). The Softswitch MUST notify the network management system whenever the Softswitch performs a network preemption in the context of its policing function to compel adherence to a video session count threshold (see Requirement 5.3.4.11.2.18).[15]

5.3.4.11.1.14.5 If the empty INVITE (in Requirement 5.3.4.11.1.14) did not have a Require header or had a Require header but not the option tag 'resource-priority' AND the Softswitch does not recognize the network domain or recognizes the network domain but the r-priority field does not have a valid value for the given network domain and the served LSC responds with either a 1xx greater than (>) 100 having no sdp offer, a 1xx greater than (>) 100 with an sdp offering audio capabilities only, or a 200 response with an sdp offering audio capabilities only then the Softswitch MUST:

- Send a 488 (Not Acceptable Here) response code to the remote initiating party of the AS-SIP INVITE that SHOULD include a "Warning" header field with warning code 370 (Insufficient Bandwidth)

- Send a CANCEL request (in the case of a 1xx) or a BYE request (in the case of a 2xx) to the local LSC

- Notify the network management system that a telephony call request was rejected in order to compel adherence to a telephony call count threshold (see Requirements 5.3.4.11.1.16 and 5.3.4.11.1.17) and that an unknown network domain ID or an invalid value for the r-priority field was encountered, as the case may be

5.3.4.11.1.14.6 If the empty INVITE (in Requirement 5.3.4.11.1.14) did not have a Require header or had a Require header but not the option tag 'resource-priority' AND the Softswitch does not recognize the network domain or recognizes the network domain but the r-priority field does not have a valid value for the given network domain and the served LSC responds with either a 1xx greater than (>) 100 with an sdp offering audio and video capabilities or a 200 response with an sdp offering audio and video capabilities AND the VSUs required for the new video session exceeds the video budget (the new session request means VDC greater than (>)

[15] If the Softswitch is unable to preempt a call request or call on behalf of a precedence call request then the Softswitch MUST notify the network management system (see Requirements 5.3.4.11.1.16 and 5.3.4.11.2.17).

VDB if no directionalization or VDCi greater than (>) VDBi if directionalization), then the Softswitch MUST:

- Send a 488 (Not Acceptable Here) response code to the remote initiating party of the AS-SIP INVITE that SHOULD include a "Warning" header field with warning code 370 (Insufficient Bandwidth)

- Send a CANCEL request (in the case of a 1xx) or a BYE request (in the case of a 2xx) to the local LSC

- Notify the network management system that a video call request was rejected in order to compel adherence to a video session count threshold (see Requirements 5.3.4.11.2.16 and 5.3.4.11.2.17) and that an unknown network domain ID or an invalid value for the r-priority field was encountered, as the case may be

5.3.4.11.1.14.7 If the empty INVITE (in Requirement 5.3.4.11.1.14) had a Require header with the option tag 'resource-priority' AND does not recognize the value of the network domain AND the served LSC responds with either a 1xx greater than (>) 100 having no sdp offer, a 1xx greater than (>) 100 with an sdp offering audio capabilities only, or a 200 response with an sdp offering audio capabilities only then the Softswitch MUST:

- Send a 417 (Unknown Resource-Priority) response code to the remote initiating party.

- Send a CANCEL request (in the case of a 1xx) or a BYE request (in the case of a 2xx) to the local LSC.

- Notify the network management system that a telephony call request was rejected in order to compel adherence to a telephony call count threshold (see Requirements 5.3.4.11.1.16 and 5.3.4.11.1.17) and that an unknown network domain ID was encountered.

5.3.4.11.1.14.8 If the empty INVITE (in Requirement 5.3.4.11.1.14) had a Require header with the option tag 'resource-priority' AND does not recognize the value of the network domain AND the served LSC responds with either a 1xx greater than (>) 100 with an sdp offering audio and video capabilities or a 200 response with an sdp offering audio and video capabilities AND the VSUs required for the new video session exceeds the video budget [the new session request means VDC greater than (>) VDB if no directionalization or VDCi greater than (>) VDBi if directionalization), then the Softswitch MUST:

- Send a 417 (Unknown Resource-Priority) response code to the remote initiating party.

- Send a CANCEL request (in the case of a 1xx) or a BYE request (in the case of a 2xx) to the local LSC.

- Notify the network management system that a telephony call request was rejected in order to compel adherence to a video session count threshold (see Requirements 5.3.4.11.2.16 and 5.3.4.11.2.17) and that an unknown network domain ID was encountered.

5.3.4.11.1.14.9 If the empty INVITE (in Requirement 5.3.4.11.1.14) had a Require header with the option tag 'resource-priority' AND recognizes the network domain but the r-priority field does not have a valid value for the given network domain AND the served LSC responds with either a 1xx greater than (>) 100 having no sdp offer, a 1xx greater than (>) 100 with an sdp offering audio capabilities only, or a 200 response with an sdp offering audio capabilities only then the Softswitch MUST:

- Send a 488 (Not Acceptable Here) response code to the remote initiating party of the AS-SIP INVITE that SHOULD include a "Warning" header field with warning code 370 (Insufficient Bandwidth).

- Send a CANCEL request (in the case of a 1xx) or a BYE request (in the case of a 2xx) to the local LSC.

- Notify the network management system that a telephony call request was rejected in order to compel adherence to a telephony call count threshold (see Requirements 5.3.4.11.1.16 and 5.3.4.11.1.17) and notify the network management system that an invalid value for the r-priority field was encountered.

5.3.4.11.1.14.10 If the empty INVITE (in Requirement 5.3.4.11.1.14) had a Require header with the option tag 'resource-priority' AND recognizes the network domain but the r-priority field does not have a valid value for the given network domain AND the served LSC responds with either a 1xx greater than (>) 100 with an sdp offering audio and video capabilities or a 200 response with an sdp offering audio and video capabilities AND the VSUs required for the new video session exceeds the video budget [the new session request means VDC greater than (>) VDB if no directionalization or VDCi greater than (>) VDBi if directionalization) then the Softswitch MUST:

- Send a 488 (Not Acceptable Here) response code to the remote initiating party of the AS-SIP INVITE that SHOULD include a "Warning" header field with warning code 370 (Insufficient Bandwidth).

- Send a CANCEL request (in the case of a 1xx) or a BYE request (in the case of a 2xx) to the local LSC.

- Notify the network management system that a telephony call request was rejected in order to compel adherence to a video session count threshold (see Requirements 5.3.4.11.2.16 and 5.3.4.11.2.17) and notify the network management system that an invalid value for the r-priority field was encountered.

Inbound re-INVITE

5.3.4.11.1.15 When a Softswitch receives an inbound re-INVITE where the existing call is a video session) that advertises audio capabilities only for a served LSC that is already at or in excess of its configured telephony budget (new call request means IPC greater than (>) IPB if no directionalization or IPCi > IPBi if directionalization), then the Softswitch MUST forward the INVITE to the LSC.[16] The inbound call request is NOT classified as a call request that goes against the telephony call count threshold unless and until a 18x or 200 response with an sdp answer accepting the audio offer is received by the Softswitch from the served LSC and then proceeds as follows:

5.3.4.11.1.15.1 If the re-INVITE (in Requirement 5.3.4.11.1.15) had a priority level of routine (r-priority = '0') AND the Softswitch receives the 18x or 200 response in Requirement 5.3.4.12.1.15 from its served LSC, then the Softswitch MUST:

- Send a 488 (Not Acceptable Here) response code to the remote initiating party of the INVITE that SHOULD include a "Warning" header field with warning code 370 (Insufficient Bandwidth).

- Send a CANCEL request (in the case of a 18x) or a BYE request (in the case of a 200) to the local LSC.

- Notify the network management system whenever a routine, immediate, or priority level telephony call request is rejected in order to compel adherence to

[16] The LSC has primary responsibility for ensuring that the access link is in compliance with the call count threshold.

a telephony call count threshold (see Requirements 5.3.4.11.1.16 and 5.3.4.11.1.17).

5.3.4.11.1.15.2 If the re-INVITE (in Requirement 5.3.4.11.1.15) had a priority level greater than routine (i.e. a precedence call) AND the Softswitch receives the 18x or 200 response in Requirement 5.3.4.11.1.15 from its served LSC, then the Softswitch MUST:

- In the case of "no directionalization," preempt lower precedence telephony call requests and/or telephony calls to free up the necessary resources to support the precedence call request. (See Requirement 5.3.4.10.3.3.1.1.2 for details on the selection process for preempting lower precedence call requests and calls). The Softswitch MUST notify the network management system whenever the Softswitch performs a network preemption in the context of its policing function to compel adherence to a telephony call count threshold (see Requirement 5.3.4.11.1.18).[17]

- In the case of "directionalization," preempt lower precedence inbound telephony call requests and/or telephony calls to free up the necessary resources to support the precedence call request. (See Requirement 5.3.4.10.3.3.1.1.2 for details on the selection process for preempting lower precedence call requests and calls). The Softswitch MUST notify the network management system whenever the Softswitch performs a network preemption in the context of its policing function to compel adherence to a telephony call count threshold (see Requirement 5.3.4.11.1.18).[18]

5.3.4.11.1.15.3 If the re-INVITE (in Requirement 5.3.4.11.1.15) did not have a Require header or had a Require header but not the option tag 'resource-priority' AND the Softswitch does not recognize the network domain or recognizes the network domain but the r-priority field does not have a valid value for the given network domain and the served LSC responds with the 18x or the 200 in Requirement 5.3.4.11.1.15, then the Softswitch MUST:

- Send a 488 (Not Acceptable Here) response code to the remote initiating party of the AS-SIP INVITE that SHOULD include a "Warning" header field with warning code 370 (Insufficient Bandwidth).

- Send a CANCEL request (in the case of a 18x) or a BYE request (in the case of a 200) to the local AS-SIP signaling appliance.

[17] If the Softswitch is unable to preempt a call request or call on behalf of a precedence call request then the Softswitch MUST notify the network management system (see Requirements 5.3.4.11.1.16 and 5.3.4.11.1.17).
[18] If the Softswitch is unable to preempt a call request or call on behalf of a precedence call request then the Softswitch MUST notify the network management system (see Requirements 5.3.4.11.1.16 and 5.3.4.11.1.17).

- Notify the network management system that a telephony call request was rejected in order to compel adherence to a telephony call count threshold (see Requirements 5.3.4.11.1.16 and 5.3.4.11.1.17) and that an unknown network domain ID or an invalid value for the r-priority field was encountered, as the case may be.

5.3.4.11.1.15.4 If the re-INVITE (in Requirement 5.3.4.11.1.15) had a Require header with the option tag 'resource-priority' AND does not recognize the value of the network domain and the served LSC responds with the 18x or the 200 in Requirement 5.3.4.11.1.15, then the Softswitch MUST:

- Send a 417 (Unknown Resource-Priority) response code to the remote initiating party.

- Send a CANCEL request (in the case of a 18x) or a BYE request (in the case of a 200) to the local LSC.

- Notify the network management system that a telephony call request was rejected in order to compel adherence to a telephony call count threshold (see Requirements 5.3.4.11.1.16 and 5.3.4.11.1.17) and that an unknown network domain ID was encountered.

5.3.4.11.1.15.5 If the re-INVITE (in Requirement 5.3.4.11.1.15) had a Require header with the option tag 'resource-priority' AND recognizes the network domain but the r-priority field does not have a valid value for the given network domain AND the served LSC responds with the 18x or the 200 in Requirement 5.3.4.11.1.15, then the Softswitch MUST:

- Send a 488 (Not Acceptable Here) response code to the remote initiating party of the AS-SIP INVITE that SHOULD include a "Warning" header field with warning code 370 (Insufficient Bandwidth).

- Send a CANCEL request (in the case of a 18x) or a BYE request (in the case of a 200) to the local LSC.

- Notify the network management system that a telephony call request was rejected in order to compel adherence to a telephony call count threshold (see Requirements 5.3.4.11.1.16 and 5.3.4.11.1.17) and notify the network management system that an invalid value for the r-priority field was encountered.

Notification to Network Management System

5.3.4.11.1.16 The Softswitch MUST notify the Network Management System whenever a routine or precedence telephony call request is rejected in order to compel adherence to a telephony call count threshold pursuant to the policing function or whenever a telephony call request or telephony call is preempted pursuant to the policing function.[19]

5.3.4.11.1.17 The notification to the network management system regarding the rejection of a telephony call request pursuant to the Softswitch policing function MUST include:

- The date and time of the rejection of the telephony call request
- The calling party number and called party number of the rejected call request
- The precedence level of the rejected call request
- The identity of the LSC whose telephony call count threshold is being protected
- The direction of the call request (inbound or outbound)

5.3.4.11.1.18 The notification to the network management system regarding the preemption of a telephony call request or telephony call pursuant to the Softswitch policing function MUST include:

- The date and time of receipt of the precedence call request
- The calling party number and called party number of the precedence call request
- The precedence level of the precedence call request
- The date and time of the preemption of the telephony call request or call
- The calling party number and called party number of the preempted call request or call
- The precedence level of the preempted call request or call

[19] The network management requirements will dictate the nature of the notification (e.g., SNMP trap or alarm) and the specific format of the notification.

- The identity of the LSC whose telephony call count threshold is being protected

- The direction of the call request (inbound or outbound)

Operational Adjustments

Although outside the scope of this specification, it should be noted that the telephony call count threshold at the Softswitch MAY be set to a value slightly above the mandated telephony call count threshold for the corresponding LSC. This procedure creates a safety margin for avoidance of call rejection or preemption due to the possibility of transient race conditions.

5.3.4.11.2 Policing of Video Sessions and Session Requests

5.3.4.11.2.1 **[FY2008-FY2012]** Video sessions are budgeted in terms of video session units (VSU) whereby one VSU equals 500Kbps and bandwidth for video sessions is allocated in multiples of VSUs.

5.3.4.11.2.2 For each LSC served by a given Softswitch, the Softswitch MUST be provisioned with:

- VDB (the total budget of VSUs that the LSC is permitted to concurrently allocate for video sessions and video session requests over the access link at any given time)

- VDBo (the total budget of outbound VSUs that the LSC is permitted to concurrently allocate for video sessions and video session requests over the access link at any given time)

- VDBi (the total budget of inbound VSUs that the LSC is permitted to concurrently allocate for video sessions and video session requests over the access link at any given time)

5.3.4.11.2.3 When there is no directionalization, then VDPBo = VDBi = null and when there is directionalization, then VDBo + VDBi MUST equal VPB.

5.3.4.11.2.4 Every Softswitch MUST be provisioned with the value of the VoIP video session budgets VDB, VDBo, and VDBi for each LSC served by the given Softswitch. The VoIP video session budgets for a given Softswitch MUST be updated whenever the VoIP video session budget for the corresponding LSC is updated.

5.3.4.11.2.5 **[After FY2012]** Every Softswitch MUST also calculate and store the value for the aggregate video budgets (VDBs) for the sum of the LSCs served by the given Softswitch.

5.3.4.11.2.6 **[FY2008-FY2012]** For each LSC served by a Softswitch, the Softswitch MUST continuously maintain a current accounting of:

- VDC – the total number of VSUs being consumed by the current video sessions and reserved for outstanding video session requests for each LSC served by the Softswitch

- VDCo – the total number of VSUs being consumed by the current outbound video sessions and reserved for outstanding outbound video session requests for each signaling appliance served by the Softswitch

- VDCi – the total number of VSUs being consumed by the current inbound video sessions and reserved for outstanding inbound video session requests for each LSC served by the Softswitch

5.3.4.11.2.7 **[FY2012+]** Every Softswitch MUST also continuously maintain a current accounting of the aggregate number of VSUs being consumed by current video sessions and reserved for outstanding video session requests for the set of LSCs served by the given Softswitch.

5.3.4.11.2.8 Every Softswitch MUST be provisioned with knowledge of the network domain IDs and the associated legitimate r-priority values supported by one or more of its assigned LSCs. This information MUST be updated as new network domain IDs are added by one or more of its assigned LSCs.

Policing of Outbound Video Session Requests

5.3.4.11.2.9 When the Softswitch receives an outbound routine (r-priority='0') INVITE from a served LSC offering audio and video capabilities that exceeds the video budget (or outbound video budget in the case of directionalization) or receives a re-INVITE offering a video session from a served LSC that exceeds the video budget[20] then the Softswitch MUST respond to the LSC with a 488 (Not Acceptable Here) response code that SHOULD include a "Warning" header field with warning code 370 (Insufficient Bandwidth). The Softswitch MUST notify the

[20] For a re-INVITE, in the case of directionalization: if the existing call is a telephony call then the new video session is applied to the outbound video session count; if the existing call is an outbound video session then policing occurs when the new video session request uses more VSUs than the current video session and the additional VSUs would exceed VDB_o; if the existing session is an inbound video session then policing occurs when the new video session request uses more VSUs than the current video session and the additional VSUs would exceed VDB_i.

network management system whenever the Softswitch rejects a routine, priority, or immediate video session request in order to compel adherence to a video count threshold (see Requirements 5.3.4.11.2.16 and 5.3.4.11.2.17).

5.3.4.11.2.10 When the Softswitch receives an outbound INVITE with a priority greater than routine (i.e. a precedence call) from a served LSC offering audio and video capabilities that exceeds the video budget (or outbound video budget in the case of directionalization) or receives a re-INVITE offering a video session from a served LSC that exceeds the video budget[21] the Softswitch MUST:

- In the case of "no directionalization," to free up the necessary resources to support the precedence session request. (See Requirement 5.3.4.10.3.3.1.1.2 for details on the selection process for preempting lower precedence session requests and sessions). The Softswitch MUST notify the network management system whenever the Softswitch performs a network preemption in the context of its policing function to compel adherence to a video count threshold (see Requirement 5.3.4.11.2.18).[22]

- In the case of "directionalization" where the INVITE is either an initial INVITE or a re-INVITE whose existing call is a telephony call then preempt lower precedence outbound video session requests and/or video sessions to free up the necessary resources to support the precedence session request. (See Requirement 5.3.4.10.3.3.1.1.2 for details on the selection process for preempting lower precedence session requests and sessions). The Softswitch MUST notify the network management system whenever the Softswitch performs a network preemption in the context of its policing function to compel adherence to a video count threshold (see Requirement 5.3.4.11.2.18).[23]

- In the case of "directionalization" where the INVITE is a re-INVITE and the existing call is an outbound video session then preempt lower precedence outbound video session requests and/or video sessions to free up the necessary resources to support the precedence session request. (See Requirement

[21] For a re-INVITE, in the case of directionalization: if the existing call is a telephony call then the new video session is applied to the outbound video session count; if the existing call is an outbound video session then policing occurs when the new video session request uses more VSUs than the current video session and the additional VSUs would exceed VDB_o; if the existing session is an inbound video session then policing occurs when the new video session request uses more VSUs than the current video session and the additional VSUs would exceed VDB_i
[22] If the Softswitch is unable to preempt a call request or call on behalf of a precedence call request then the Softswitch MUST notify the network management system (see Requirements 5.3.4.11.2.16, 5.3.4.11.2.17)
[23] If the Softswitch is unable to preempt a call request or call on behalf of a precedence call request then the Softswitch MUST notify the network management system (see Requirements 5.3.4.11.2.16 and 5.3.4.11.2.17).

5.3.4.10.3.3.1.1.2 for details on the selection process for preempting lower precedence session requests and sessions). The Softswitch MUST notify the network management system whenever the Softswitch performs a network preemption in the context of its policing function to compel adherence to a video count threshold (see Requirement 5.3.4.11.2.18).[24]

- In the case of "directionalization" where the INVITE is a re-INVITE and the existing call is an inbound video session then preempt lower precedence inbound video session requests and/or video sessions to free up the necessary resources to support the precedence session request. (See Requirement 5.3.4.10.3.3.1.1.2 for details on the selection process for preempting lower precedence session requests and sessions). The Softswitch MUST notify the network management system whenever the Softswitch performs a network preemption in the context of its policing function to compel adherence to a video count threshold (see Requirement 5.3.4.11.2.18).[25]

5.3.4.11.2.11 When the Softswitch receives an outbound INVITE from a served LSC offering audio and video capabilities that exceeds the video budget (or outbound video budget in the case of directionalization) or receives a re-INVITE offering a video session from a served LSC that exceeds the video budget[26] and the outbound INVITE (or re-INVITE) either does not have a Require header or has a Require header but not the option tag 'resource-priority' and has either an unrecognized network domain OR a known network domain but an invalid value for the r-priority field, then the Softswitch MUST respond to the LSC with a 488 (Not Acceptable Here) response code that SHOULD include a "Warning" header field with warning code 370 (Insufficient Bandwidth). The Softswitch MUST notify the network management system that a video session request was rejected in order to compel adherence to a video count threshold (see Requirements 5.3.4.11.2.16 and 5.3.4.11.2.17) and that either an unknown network domain ID or an invalid value for the r-priority field was encountered, as the case may be.

5.3.4.11.2.12 When the Softswitch receives an outbound INVITE from a served LSC offering audio and video capabilities or receives a re-INVITE offering a video session from a served LSC and the outbound INVITE (or re-INVITE) has a Require header with the option tag 'resource-priority' and has a Resource Priority header with an unrecognized network domain then the

[24] If the Softswitch is unable to preempt a call request or call on behalf of a precedence call request then the Softswitch MUST notify the network management system (see Requirements 5.3.4.11.2.16 and 5.3.4.11.2.17).
[25] If the Softswitch is unable to preempt a call request or call on behalf of a precedence call request then the Softswitch MUST notify the network management system (see Requirements 5.3.4.11.2.16 and 5.3.4.11.2.17).
[26] For a re-INVITE, in the case of directionalization: if the existing call is a telephony call then the new video session is applied to the outbound video session count; if the existing call is an outbound video session then policing occurs when the new video session request uses more VSUs than the current video session and the additional VSUs would exceed VDB_o; if the existing session is an inbound video session then policing occurs when the new video session request uses more VSUs than the current video session and the additional VSUs would exceed VDB_i.

Softswitch MUST respond with a 417 (Unknown Resource-Priority). The Softswitch MUST notify the network management system that a video session request was rejected in order to compel adherence to a video count threshold (see Requirements 5.3.4.11.2.16 and 5.3.4.11.2.17) and that an unknown network domain ID was encountered.

5.3.4.11.2.13 When the Softswitch receives an outbound INVITE from a served LSC offering audio and video capabilities that exceeds the video budget (or outbound video budget in the case of directionalization) or receives a re-INVITE offering a video session from a served LSC that exceeds the video budget[27] and the outbound INVITE (or re-INVITE) has a Require header with the option tag 'resource-priority' and has a Resource Priority header with a known network domain but an invalid value for the r-priority field then the Softswitch MUST respond with a 488 (Not Acceptable Here) that SHOULD include a "Warning" header field with warning code 370 (Insufficient Bandwidth). The Softswitch MUST notify the network management system that a video session request was rejected in order to compel adherence to a video count threshold (see Requirements 5.3.4.11.2.16 and 5.3.4.11.2.17) and that an invalid value for the r-priority field was encountered.

NOTE: Outbound empty INVITEs are classified as telephony calls and their policing is covered in Requirements 5.3.4.11.1.8 through 5.3.4.11.1.12.

Policing of Inbound Video Session Requests

Inbound INVITE

5.3.4.11.2.14 When a Softswitch receives an inbound INVITE that advertises audio and video capabilities for a served LSC that is already at or in excess of its configured budget (new session request means VDC greater than (>) VDB if no directionalization or VDCi greater than (>) VDBi if directionalization) then the Softswitch MUST forward the INVITE to the LSC[28]. The inbound call request is NOT classified as a call request that goes against the video call count threshold (or telephony call count threshold] unless and until a 1xx greater than (>) 100 or 2xx response is received by the Softswitch from the served LSC and then proceeds as follows:

5.3.4.11.2.14.1 In the event the INVITE (in Requirement 5.3.4.11.2.14) had a priority level greater than routine (i.e. a precedence call) AND the Softswitch receives a 1xx >100 response or

[27] For a re-INVITE, in the case of directionalization: if the existing call is a telephony call then the new video session is applied to the outbound video session count;if the existing call is an outbound video session then policing occurs when the new video session request uses more VSUs than the current video session and the additional VSUs would exceed VDB_o; if the existing session is an inbound video session then policing occurs when the new video session request uses more VSUs than the current video session and the additional VSUs would exceed VDB_i.
[28] The LSC has primary responsibility for ensuring that the access link is in compliance with the call count threshold.

2xx response with an sdp answer that accepts audio and video capabilities or a 1xx greater than (>) 100 response with no sdp answer from its served LSC then the Softswitch MUST:

- Send a 488 (Not Acceptable Here) response code to the remote initiating party of the INVITE that SHOULD include a "Warning" header field with warning code 370 (Insufficient Bandwidth).

- Send a CANCEL request (in the case of a 1xx) or a BYE request (in the case of a 2xx) to the local LSC.

- Notify the network management system whenever a routine, priority, or immediate level video session request is rejected in order to compel adherence to a video count threshold (see Requirements 5.3.4.11.2.16 and 5.3.4.11.2.17).

5.3.4.11.2.14.2 In the event the INVITE (in Requirement 5.3.4.11.2.14) had a priority level greater than routine (i.e. a precedence call) AND the Softswitch receives a 1xx greater than (>) 100 response or 2xx response with an sdp answer that accepts audio and video capabilities from its served LSC or a 1xx greater than (>) 100 response with no sdp answer then the Softswitch MUST:

- In the case of "no directionalization," preempt lower precedence video session requests and/or video sessions to free up the necessary resources to support the precedence session request. (See Requirement 5.3.4.10.3.3.1.1.2 for details on the selection process for preempting lower precedence session requests and sessions). The Softswitch MUST notify the network management system whenever the Softswitch performs a network preemption in the context of its policing function to compel adherence to a video count threshold (see Requirement 5.3.4.11.2.18).[29]

- In the case of "directionalization," preempt lower precedence inbound video session requests and/or video sessions to free up the necessary resources to support the precedence session request. (See Requirement 5.3.4.10.3.3.1.1.2 for details on the selection process for preempting lower precedence session requests and sessions). The Softswitch MUST notify the network management system whenever the Softswitch performs a network preemption in the context of its policing function to compel adherence to a video count threshold (see Requirement 5.3.4.11.2.18).

[29] If the Softswitch is unable to preempt a call request or call on behalf of a precedence call request then Softswitch MUST notify the network management system (see Requirements 5.3.4.11.2.16, 5.3.4.11.2.17)

5.3.4.11.2.14.3 In the event the INVITE (in Requirement 5.3.4.11.2.14) did not have a Require header or had a Require header but not the option tag 'resource-priority' AND the Softswitch does not recognize the network domain or recognizes the network domain but the r-priority field does not have a valid value for the given network domain and the served LSC responds with a 1xx greater than (>) 100 response or 2xx with an sdp answer that accepts either audio and video capabilities or a 1xx greater than (>) 100 response with no sdp answer then the Softswitch MUST:

- Send a 488 (Not Acceptable Here) response code to the remote initiating party of the re- INVITE that SHOULD include a "Warning" header field with warning code 370 (Insufficient Bandwidth).

- Send a CANCEL request (in the case of a 1xx) or a BYE request (in the case of a 2xx) to the local AS-SIP signaling appliance.

- Notify the network management system that a video session request was rejected in order to compel adherence to a video count threshold (see Requirements 5.3.4.11.2.16 and 5.3.4.11.2.17) and that either an unknown network domain ID or an invalid value for the r-priority field was encountered, as the case may be.

5.3.4.11.2.14.4 In the event the INVITE (in Requirement 5.3.4.11.2.14) had a Require header with the option tag 'resource-priority' AND does not recognize the value of the network domain and the served LSC responds with a 1xx greater than (>) 100 or 2xx with an sdp answer that accepts audio and video capabilities or a 1xx greater than (>) 100 response with no sdp answer then the Softswitch MUST:

- Send a 417 (Unknown Resource-Priority) response code to the remote initiating party.

- Send a CANCEL request (in the case of a 1xx) or a BYE request (in the case of a 2xx) to the local AS-SIP signaling appliance.

- Notify the network management system that a video session request was rejected in order to compel adherence to a video count threshold (see Requirements 5.3.4.11.2.16 and 5.3.4.11.2.17) and that an unknown network domain ID was encountered

5.3.4.11.2.14.5 In the event the INVITE (in Requirement 5.3.4.11.2.14) had a Require header with the option tag 'resource-priority' AND recognizes the network domain but the r-priority field does not have a valid value for the given network domain AND the served LSC responds

with a 1xx greater than (>) 100 or 2xx with an sdp answer that accepts audio and video capabilities or a 1xx greater than (>) 100 response with no sdp answer then the Softswitch MUST:

- Send a 488 (Not Acceptable Here) response code to the remote initiating party of the re-INVITE that SHOULD include a "Warning" header field with warning code 370 (Insufficient Bandwidth).

- Send a CANCEL request (in the case of a 1xx) or a BYE request (in the case of a 2xx) to the local LSC.

- Notify the network management system that a video session request was rejected in order to compel adherence to a video count threshold (see Requirements 5.3.4.11.2.16 and 5.3.4.11.2.17) and that an invalid value for the r-priority field was encountered.

5.3.4.11.2.14.6 In the event the INVITE (in Requirement 5.3.4.11.2.14) had a routine priority level AND the Softswitch receives a 1xx >100 response or 2xx response with an sdp answer that accepts audio capabilities only from its served LSC then the Softswitch MUST verify whether the call request would cause IPC to exceed IPB (or in the case of directionalization if IPCi would exceed IPBi). If the call request would cause the call count to exceed the telephony call count threshold then the Softswitch MUST:

- Send a 488 (Not Acceptable Here) response code to the remote initiating party of the INVITE that SHOULD include a "Warning" header field with warning code 370 (Insufficient Bandwidth).

- Send a CANCEL request (in the case of a 1xx) or a BYE request (in the case of a 2xx) to the local LSC.

- Notify the network management system whenever a routine, priority, or immediate level telephony request is rejected in order to compel adherence to a telephony count threshold (see Requirements 5.3.4.11.1.16 and 5.3.4.11.1.17)

5.3.4.11.2.14.7 If the INVITE (in Requirement 5.3.4.11.2.14) had a priority level greater than routine (i.e. a precedence call) AND the Softswitch receives a 1xx >100 response or 2xx response with an sdp answer that accepts audio capabilities only from its served LSC then the Softswitch MUST verify whether the call request would cause IPC to exceed IPB (or in the case of directionalization if IPCi would exceed IPBi). If the call request would cause the call count to exceed the telephony call count threshold then the Softswitch MUST:

- In the case of "no directionalization," preempt lower precedence telephony call requests and/or telephony calls to free up the necessary resources to support the precedence call request. (See Requirement 5.3.4.10.3.3.1.1.2 for details on the selection process for preempting lower precedence call requests and calls). The Softswitch MUST notify the network management system whenever the Softswitch performs a network preemption in the context of its policing function to compel adherence to a telephony call count threshold (see Requirement 5.3.4.11.1.18).[30]

- In the case of "directionalization," preempt lower precedence inbound telephony call requests and/or telephony calls to free up the necessary resources to support the precedence call request. (See Requirement 5.3.4.10.3.3.1.1.2 for details on the selection process for preempting lower precedence call requests and calls). The Softswitch MUST notify the network management system whenever the Softswitch performs a network preemption in the context of its policing function to compel adherence to a telephony call count threshold (see Requirement 5.3.4.11.1.18).[31]

NOTE: The policing of inbound empty INVITEs is covered in Requirement 5.3.4.11.1.14.

Inbound re-INVITE

5.3.4.11.2.15 When a Softswitch receives an inbound re-INVITE for a video session for a served LSC that is already at or in excess of its configured budget[32] then the Softswitch MUST forward the re-INVITE to the LSC[33]. The inbound re-INVITE is NOT classified as a call request that goes against the video call count threshold (or telephony call count threshold] unless and until a 1xx >100 response or 200 response is received by the Softswitch from the served LSC and then proceeds as follows:

5.3.4.11.2.15.1 In the event the re-INVITE (in Requirement 5.3.4.11.2.15) had a routine priority level AND the Softswitch receives a 1xx or 200 response with an sdp answer accepting the video

[30] If the Softswitch is unable to preempt a call request or call on behalf of a precedence call request then the Softswitch MUST notify the network management system (see Requirements 5.3.4.11.1.16, 5.3.4.11.1.17)
31 If the Softswitch is unable to preempt a call request or call on behalf of a precedence call request then the Softswitch MUST notify the network management system (see Requirements 5.3.4.11.1.16, 5.3.4.11.1.17)
32 For a re-INVITE, in the case of directionalization: if the existing call is a telephony call then the new video session is applied to the inbound video session count; if the existing call is an outbound video session then policing occurs when the new video session request uses more VSUs than the current video session and the additional VSUs would exceed VDBo; if the existing session is an inbound video session then policing occurs when the new video session request uses more VSUs than the current video session and the additional VSUs would exceed VDB_i.
33 The LSC has primary responsibility for ensuring that the access link is in compliance with the call count threshold.

offer or a 1xx greater than (>) 100 response with no sdp answer from its served LSC then the Softswitch MUST:

- Send a 488 (Not Acceptable Here) response code to the remote initiating party of the AS-SIP INVITE that SHOULD include a "Warning" header field with warning code 370 (Insufficient Bandwidth).

- Send a CANCEL request (in the case of a 1xx) or a BYE request (in the case of a 2xx) to the local LSC.

- Notify the network management system whenever a routine, priority, or immediate level video session request is rejected in order to compel adherence to a video count threshold (see Requirements 5.3.4.11.2.16 and 5.3.4.11.2.17).

5.3.4.11.2.15.2 In the event the re-INVITE (in Requirement 5.3.4.11.2.15) had a priority level greater than routine (i.e. a precedence call) AND the Softswitch receives a 1xx or 200 response with an sdp answer accepting the video offer or a 1xx greater than (>) 100 response with no sdp answer from its served LSC then the Softswitch MUST:

- In the case of "no directionalization," preempt lower precedence video session requests and/or video sessions to free up the necessary resources to support the precedence session request. (See Requirement 5.3.4.10.3.3.1.1.2 for details on the selection process for preempting lower precedence session requests and sessions). The Softswitch MUST notify the network management system whenever the Softswitch performs a network preemption in the context of its policing function to compel adherence to a video count threshold (see Requirement 5.3.4.11.2.18).[34]

- In the case of "directionalization" when the existing call is a telephony call then preempt lower precedence inbound video session requests and/or video sessions to free up the necessary resources to support the precedence session request. (See Requirement 5.3.4.10.3.3.1.1.2 for details on the selection process for preempting lower precedence session requests and sessions). The Softswitch MUST notify the network management system whenever the Softswitch performs a network preemption in the context of its policing function to compel adherence to a video count threshold (see Requirement 5.3.4.11.2.18).[35]

[34] If the Softswitch is unable to preempt a call request or call on behalf of a precedence call request then Softswitch MUST notify the network management system (see Requirements 5.3.4.11.2.16, 5.3.4.11.2.17)
[35] If the Softswitch is unable to preempt a call request or call on behalf of a precedence call request then Softswitch MUST notify the network management system (see Requirements 5.3.4.11.2.16, 5.3.4.11.2.17)

- In the case of "directionalization" when the existing call is an outbound video session then preempt lower precedence outbound video session requests and/or video sessions to free up the necessary resources to support the precedence session request. (See Requirement 5.3.4.10.3.3.1.1.2 for details on the selection process for preempting lower precedence session requests and sessions). The Softswitch MUST notify the network management system whenever the Softswitch performs a network preemption in the context of its policing function to compel adherence to a video count threshold (see Requirement 5.3.4.11.2.18).[36]

- In the case of "directionalization" when the existing call is an inbound video session then preempt lower precedence inbound video session requests and/or video sessions to free up the necessary resources to support the precedence session request. (See Requirement 5.3.4.10.3.3.1.1.2 for details on the selection process for preempting lower precedence session requests and sessions). The Softswitch MUST notify the network management system whenever the Softswitch performs a network preemption in the context of its policing function to compel adherence to a video count threshold (see Requirement 5.3.4.11.2.18).[37]

5.3.4.11.2.15.3 In the event the re-INVITE (in Requirement 5.3.4.11.2.15) did not have a Require header or had a Require header but not the option tag 'resource-priority' AND the Softswitch does not recognize the network domain or recognizes the network domain but the r-priority field does not have a valid value for the given network domain and the Softswitch receives a 1xx or 200 response having an sdp answer accepting the video offer or a 1xx greater than (>) 100 response with no sdp answer from the served LSC then the Softswitch MUST:

- Send a 488 (Not Acceptable Here) response code to the remote initiating party of the re- INVITE that SHOULD include a "Warning" header field with warning code 370 (Insufficient Bandwidth).

- Send a CANCEL request (in the case of a 1xx) or a BYE request (in the case of a 2xx) to the local AS-SIP signaling appliance.

- Notify the network management system that a video session request was rejected in order to compel adherence to a video count threshold (see Requirements 5.3.4.11.2.16 and 5.3.4.11.2.17) and that either an unknown network domain ID or an invalid value for the r-priority field was encountered, as the case may be.

[36] If the Softswitch is unable to preempt a call request or call on behalf of a precedence call request then Softswitch MUST notify the network management system (see Requirements 5.3.4.11.2.16, 5.3.4.11.2.17).
[37] If the Softswitch is unable to preempt a call request or call on behalf of a precedence call request then Softswitch MUST notify the network management system (see Requirements 5.3.4.11.2.16, 5.3.4.11.2.17).

5.3.4.11.2.15.4 In the event the re-INVITE (in Requirement 5.3.4.11.2.15) had a Require header with the option tag 'resource-priority' AND does not recognize the value of the network domain and the served LSC responds with a 1xx or 200 having an sdp answer accepting the video offer or a 1xx greater than (>) 100 response with no sdp answer then the Softswitch MUST:

- Send a 417 (Unknown Resource-Priority) response code to the remote initiating party.

- Send a CANCEL request (in the case of a 1xx) or a BYE request (in the case of a 2xx) to the local AS-SIP signaling appliance.

- Notify the network management system that a video session request was rejected in order to compel adherence to a video count threshold (see Requirements 5.3.4.11.2.16 and 5.3.4.11.2.17) and that an unknown network domain ID was encountered.

5.3.4.11.2.15.5 In the event the re-INVITE (in Requirement 5.3.4.11.2.15) had a Require header with the option tag 'resource-priority' AND recognizes the network domain but the r-priority field does not have a valid value for the given network domain AND the served LSC responds with a 1xx or 200 having an sdp answer accepting the video offer or a 1xx greater than (>) 100 response with no sdp answer then the Softswitch MUST:

- Send a 488 (Not Acceptable Here) response code to the remote initiating party of the re-INVITE that SHOULD include a "Warning" header field with warning code 370 (Insufficient Bandwidth).

- Send a CANCEL request (in the case of a 1xx) or a BYE request (in the case of a 2xx) to the local LSC.

- Notify the network management system that a video session request was rejected in order to compel adherence to a video count threshold (see Requirements 5.3.4.11.2.16 and 5.3.4.11.2.17) and that an invalid value for the r-priority field was encountered

5.3.4.11.2.15.6 In the event the re-INVITE (in Requirement 12.2.15) had a routine priority level AND the Softswitch receives a 1xx >100 response or 2xx response with an sdp answer that accepts audio capabilities only from its served LSC then the Softswitch MUST verify whether the re-INVITE would cause IPC to exceed IPB (or if IPCi would exceed IPBi in the case of directionalization). If the re-INVITE would cause the call count to exceed the telephony call count threshold then the Softswitch MUST:

- Send a 488 (Not Acceptable Here) response code to the remote initiating party of the INVITE that SHOULD include a "Warning" header field with warning code 370 (Insufficient Bandwidth).

- Send a CANCEL request (in the case of a 1xx) or a BYE request (in the case of a 2xx) to the local LSC.

- Notify the network management system whenever a routine, priority, or immediate level telephony request is rejected in order to compel adherence to a telephony count threshold (see Requirements 5.3.4.11.1.16 and 5.3.4.11.1.17).

5.3.4.11.2.15.7 In the event the re-INVITE (in Requirement 5.3.4.11.2.15) had a priority level greater than routine (i.e. a precedence call) AND the Softswitch receives a 1xx >100 response or 2xx response with an sdp answer that accepts audio capabilities only from its served LSC then the Softswitch MUST verify whether the re-INVITE would cause IPC to exceed IPB (or if IPCi would exceed IPBi in the case of directionalization). If the re-INVITE would cause the call count to exceed the telephony call count threshold then the Softswitch MUST:

- In the case of "no directionalization," preempt lower precedence telephony call requests and/or telephony calls to free up the necessary resources to support the precedence call request. (See Requirement 5.3.4.10.3.3.1.1.2 for details on the selection process for preempting lower precedence call requests and calls). The Softswitch MUST notify the network management system whenever the Softswitch performs a network preemption in the context of its policing function to compel adherence to a telephony call count threshold (see Requirement 5.3.4.11.1.18).[38]

- In the case of "directionalization," preempt lower precedence inbound telephony call requests and/or telephony calls to free up the necessary resources to support the precedence call request. (See Requirement 5.3.4.10.3.3.1.1.2 for details on the selection process for preempting lower precedence call requests and calls). The Softswitch MUST notify the network management system whenever the Softswitch performs a network preemption in the context of its policing function to compel adherence to a telephony call count threshold (see Requirement 5.3.4.11.1.18).[39]

[38] If the Softswitch is unable to preempt a call request or call on behalf of a precedence call request then the Softswitch MUST notify the network management system (see Requirements 5.3.4.11.1.16, 5.3.4.11.1.17)
[39] If the Softswitch is unable to preempt a call request or call on behalf of a precedence call request then the Softswitch MUST notify the network management system (see Requirements 5.3.4.11.1.16, 5.3.4.11.1.17)

Notification to Network Management System

5.3.4.11.2.16 The Softswitch MUST notify the Network Management System whenever a routine or precedence video session request is rejected in order to compel adherence to a video count threshold pursuant to the policing function or whenever a video session request or video session is preempted pursuant to the policing function.[40]

5.3.4.11.2.17 The notification to the network management system regarding the rejection of a video session request pursuant to Softswitch policing function MUST include:

- The date and time of the rejection of the video session request
- The calling party number and called party number of the rejected session request
- The precedence level of the rejected session request
- The identity of the AS-SIP signaling appliance whose video count threshold is being protected
- The direction of the session request (inbound or outbound)

5.3.4.11.2.18 The notification to the network management system regarding the preemption of a video session request or video session pursuant to the Softswitch policing function MUST include:

- The date and time of receipt of the precedence session request
- The calling party number and called party number of the precedence session request
- The precedence level of the precedence session request
- The date and time of the preemption of the video session request or session
- The calling party number and called party number of the preempted session request or call

[40] The network management requirements will dictate the nature of the notification (e.g., SNMP trap or alarm) and the specific format of the notification.

- The precedence level of the preempted session request or session
- The identity of the AS-SIP signaling appliance whose video count threshold is being protected
- The direction of the session request (inbound or outbound)

Operational Adjustments

Although outside the scope of this specification it should be noted that the video count threshold at the Softswitch MAY be set to a value slightly above the mandated video count threshold for the corresponding AS-SIP signaling appliance. This procedure creates a safety margin for avoidance of call rejection or preemption due to the possibility of transient race conditions.

5.3.4.12 Video Telephony – General Rules

5.3.4.12.1 Caller

5.3.4.12.1.1 Video telephony end instruments MUST, as the default configuration, require an end user wishing to place a call that includes video, to affirmatively signal the intention to include video to the end instrument every time the caller wishes to engage in a video telephony call. The interactive mechanism by which the caller signals this intention to include video is left to the vendors.[41]

5.3.4.12.1.1.1 When the caller affirmatively signals an intention to make a video telephony call and the initial INVITE includes an sdp offering audio and video capabilities and the initial sdp answer accepts both audio and video capabilities then the caller is not required to again signal his/her intention to the end instrument to conduct a video telephony call upon receipt of the sdp answer.

5.3.4.12.1.1.2 When the caller affirmatively signals an intention to make a video telephony call and the initial INVITE includes an sdp offering audio and video capabilities and the initial sdp answer accepts audio but not video capabilities then the call will take the form of an audio call and in order for the caller to attempt to convert the audio call to a video telephony call the caller MUST again affirmatively signal to the end instrument an intention to include video. A re-INVITE with an sdp offering audio and video capabilities will then be sent to the destination end instrument.

[41] Examples include pressing a physical button or switch, clicking on a virtual soft button, or selecting the video telephony option from a display menu when either entering the dial string or selecting the intended recipient from an electronic address book.

5.3.4.12.1.1.3 When the caller affirmatively signals an intention to make a video telephony call and the initial INVITE does not include an sdp offer (Empty INVITE) then if the initial sdp offer received from the called party includes both audio and video capabilities the caller's end instrument can accept the audio and video capabilities without prompting the caller to again affirmatively signal an intention to conduct a video telephony call.[42]

5.3.4.12.1.1.4 When the caller affirmatively signals an intention to make a video telephony call and the initial INVITE does not include an sdp offer (Empty INVITE) then if the sdp offer received from the called party includes only audio capabilities but not video capabilities then the calling end instrument accepts the audio capabilities and in order for the caller to convert the audio call to a video telephony call the caller MUST again affirmatively signal to the end instrument the intention to include video. A re-INVITE with an sdp offering audio and video capabilities will then be sent to the destination end instrument.

5.3.4.12.1.2 Every time a caller requests a video telephony call and the video portion of the telephony call is successfully established then the video telephony end instrument MUST provide the user with an affirmative confirmation that the video is enabled either prior to, or upon successful completion of, session establishment. The affirmative confirmation MUST take the form of both an audio and a visual signal to the caller. NOTE: The intent of this requirement is to ensure that the caller is fully cognizant that video is being transmitted.

Callee

5.3.4.12.1.3 When an INVITE with an sdp offer that includes both audio and video capabilities is received by an LSC serving a destination end instrument that supports video telephony then when the call request is received by the destination end instrument the destination end instrument MUST indicate to the callee that a telephony call requesting video connectivity has been received. As the default configuration, the callee MUST affirmatively signal to the end instrument a desire to accept a video telephony call (as opposed to an audio call) in order for the end instrument to accept a video request and for the destination LSC to respond with an sdp answer that includes video capabilities in addition to audio capabilities.

5.3.4.12.1.3.1 If the callee initially accepts an audio call then the callee MUST affirmatively signal to the EI a desire to add video to the call if the callee wishes to convert the audio call into a video telephony call. A re-INVITE MUST then be sent to the originating LSC/end instrument offering both audio and video capabilities.

[42] The caller has just affirmatively indicated an intention to engage in a video relephony call prior to the transmission of the empty INVITE.

5.3.4.12.1.3.1.1 Upon receipt of the re-INVITE from the callee offering audio and video capabilities, the calling IP end instrument MUST notify the caller that there has been a request to upgrade the existing call to a video telephony call and the caller MUST affirmatively signal to the end instrument a desire to accept the upgrade of the call to video telephony in order for the calling party's end instrument to accept the audio and video capabilities.

5.3.4.12.1.3.2 If the callee affirmatively signals to the end instrument a desire to accept the video component of the call only after the transmission of an sdp answer accepting only audio capbabilities then a re-INVITE MUST be sent to the originating LSC/end instrument offering both audio and video capabilities.

5.3.4.12.1.3.2.1 Upon receipt of the re-INVITE from the callee offering audio and video capabilities, the calling IP end instrument MUST notify the caller that there has been a request to upgrade the existing call to a video telephony call and the caller MUST affirmatively signal to the end instrument a desire to accept the upgrade of the call to video telephony in order for the calling party's end instrument to accept the audio and video capabilities.

5.3.4.12.1.4 When an LSC serving a destination IP end instrument receives an INVITE lacking an sdp offer (Empty INVITE) and the destination end instrument supports video telephony, then the destination end instrument MAY offer the callee the option to affirmatively signal to the end instrument a desire to select a video telephony call.

5.3.4.12.1.4.1 If the callee affirmatively signals to the end instrument a desire to select a video telephony call after the transmission of a response with an sdp offer having audio capabilities only then the LSC (or the SIP end instrument] MUST wait until the initial INVITE has completed and then send a re-INVITE to the originating LSC/end instrument offering both audio and video capabilities.

5.3.4.12.1.4.1.1 Upon receipt of the re-INVITE from the callee offering audio and video capabilities, the calling IP end instrument MUST notify the caller that there has been a request to upgrade the existing call to a video telephony call and the caller MUST affirmatively signal to the end instrument a desire to accept the upgrade of the call to video telephony in order for the calling party's end instrument to accept the audio and video capabilities.

5.3.4.12.1.5 Every time a callee accepts a video telephony call and the video portion of the telephony call is successfully established then the video telephony end instrument MUST provide the user with an affirmative confirmation that the video is enabled either prior to or upon successful session establishment. The affirmative confirmation MUST take the form of both an audio and a visual signal to the callee. NOTE: The intent of this requirement is to ensure that the callee is fully cognizant that video is being transmitted.

5.3.4.12.2 IP-to-IP Video Telephony Call Flows

This section furnishes a representative set of two-party video telephony call flows whereby the originating end instrument is IP and located at one base, the terminating end instrument is IP and located at another base, and AS-SIP signaling is employed over the DISN WAN to conduct call set-up, maintenance, and termination.

Section 5.3.4.12.2.1 and Section 5.3.4.12.2.2 detail call flows in which the INVITE includes an sdp offer of audio and video capabilities.

Section 5.3.4.12.2.3 and Section 5.3.4.12.2.4 detail call flows in which the INVITE does not include an sdp offer (Empty INVITE) and wherein the originating LSC and terminating LSC do not add or process audio and video media feature tags that may be located in the Contact header of the INVITE.

Section 5.3.4.12.2.5 and Section 5.3.4.12.2.6 detail call flows in which the INVITE does not include an sdp offer (Empty INVITE) and wherein the originating LSC adds the audio and video media feature tags and the terminating LSC processes the audio and video media feature tags. It should be noted that the call flows in Figure 5.3.4-5 and Figure 5.3.4-7 and the call flows in Figure 5.3.4-6 and Figure 5.3.4-8 are identical except for the sequence of the ASAC call count events conducted by the LSCs.

In the case of IP-to-IP calls when the INVITE includes an sdp offer, then the sdp answer is provided in the 200 response, and when the INVITE does not have an sdp offer (Empty INVITE), the sdp offer is made in the 200 response and the sdp answer is made in the ACK request. The appendix to this specification details the IP-TDM call flows wherein an INVITE with an sdp offer receives an sdp answer in the first non-failure, reliable provisional response, and an INVITE that does not have an sdp offer (Empty INVITE) receives an sdp offer in the first non-failure, reliable provisional response and the sdp answer is transmitted in the PRACK message. These rules enable the originating LSC to identify whether the recipient EI is served by the DSN IP network or the DSN TDM network, and therefore alerts the originating LSC either to arrange for the EI to play tones and announcements locally or to instruct the EI to listen for early media instead.

5.3.4.12.2.1 INVITE with sdp Video Offer Accepted in 200 with sdp Answer

Party A affirmatively signals to its EI an intention to request a video telephony call. This is reflected in the INVITE that includes an sdp offer of audio and video capabilities, shown in Figure 5.3.4-3, INVITE with sdp Video Offer Accepted in 200 with sdp Answer. Party B is notified by its EI that a video telephony call is being requested. Party B affirmatively signals its end instrument to accept the video telephony offer prior to sending the 200 response.

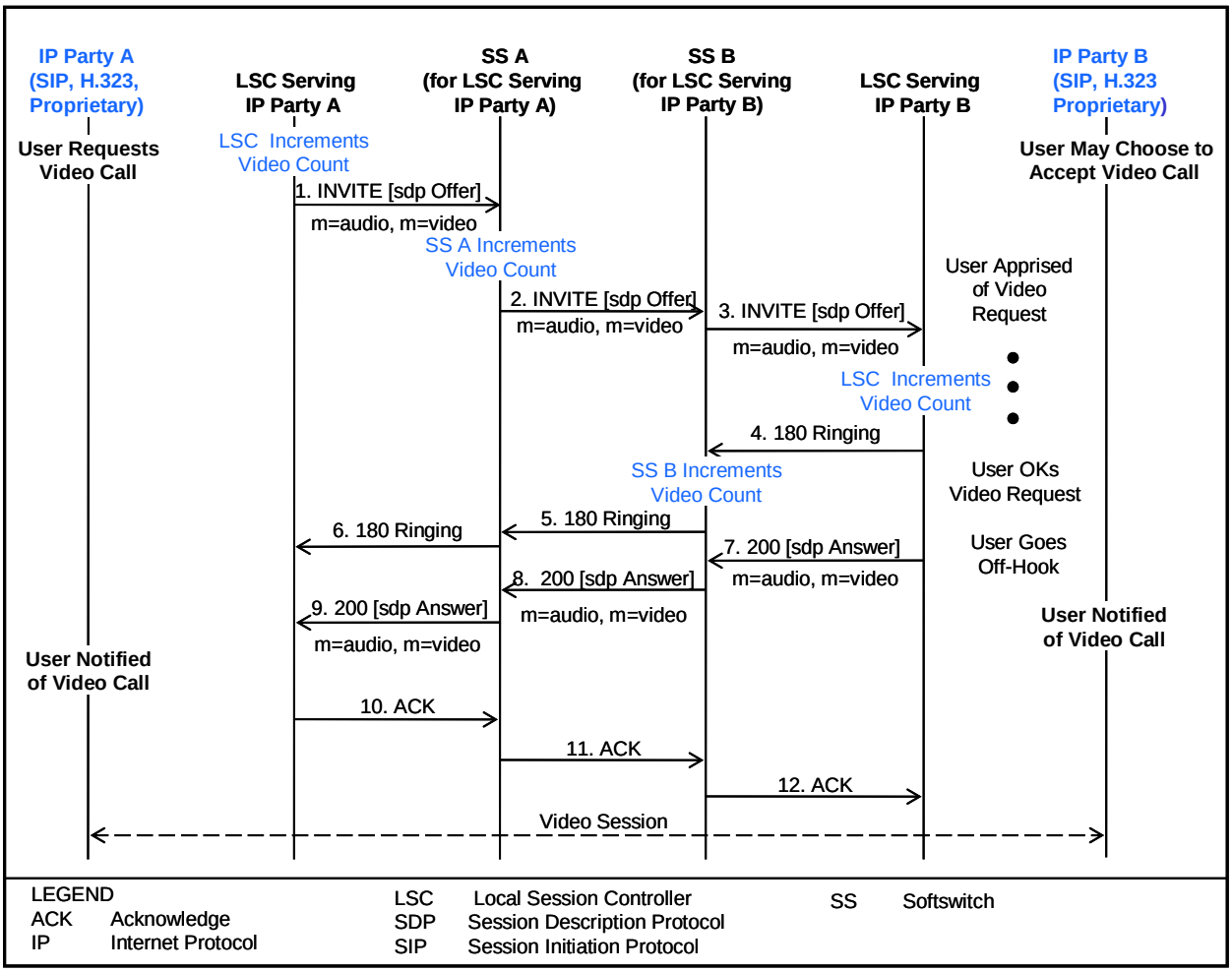


Figure 5.3.4-3. INVITE with sdp Video Offer Accepted in 200 with sdp Answer

STEP	INSTRUCTION
1, 2, 3	Party A affirmatively signals to its end instrument a desire to initiate a video telephony call. Upon receiving an initial call request message from IP Party A (not depicted in Figure 5.3.4-3), the LSC serving IP Party A either generates and sends an INVITE with an sdp offering audio and video capabilities to Softswitch A or forwards an INVITE with an sdp offering audio and video capabilities (created by SIP EI A) to Softswitch A. Softswitch A forwards the INVITE across the WAN to Softswitch B (which is assigned to the LSC serving IP Party B). Softswitch B forwards the INVITE to the LSC serving IP Party B. When the LSC serving IP Party B sends the INVITE or other call request message to the EI serving IP Party B, then Party B is notified by the called EI that a video telephone call has been requested so that Party B has the opportunity to indicate affirmatively to the EI a desire to accept a video call.

STEP	INSTRUCTION
	NOTE: Signaling between the EI serving IP Party A and the LSC serving IP Party A is not depicted. NOTE: Signaling between the LSC serving IP Party B and the EI serving IP Party B is not depicted.
	ASAC Prior to sending 1, LSC A increments video count. Upon receiving 2, Softswitch A increments video count. Upon receiving 3, LSC B increments video count.
4, 5, 6	Assuming the EI is not busy, the LSC serving IP Party B sends a 180 (Ringing) to Softswitch B. It forwards the 180 (Ringing) to Softswitch A, which forwards the 180 (Ringing) to the LSC serving IP Party A. NOTE: Signaling between the EI serving IP Party B and the LSC serving IP Party B is not depicted. NOTE: Signaling between the LSC serving IP Party A and the EI serving IP Party A is not depicted. **ASAC** Upon receiving 4, Softswitch B increments video count.
7, 8, 9	Party B affirmatively signals to its EI an intention to accept a video telephone call. When IP Party B goes off hook (i.e., answers the call), the LSC serving IP Party B sends a 200 (OK) with an sdp answer accepting audio and video capabilities to Softswitch B. Softswitch B forwards the 200 (OK) to Softswitch A, which forwards the 200 (OK) to the LSC serving IP Party A. EI B notifies Party B that a video call has been established. NOTE: Signaling between the EI serving IP Party B and the LSC serving IP Party B is not depicted. In addition, signaling between the LSC serving IP Party A and the EI serving IP Party A is not depicted.
10, 11, 12	EI A notifies Party A that a video call has been established. The LSC serving IP Party A sends an ACK to Softswitch A. It forwards the ACK to Softswitch B, which forwards the ACK to the LSC serving IP Party B. NOTE: Signaling between the EI serving IP Party A and the LSC serving IP Party A is not depicted. In addition, signaling between the LSC serving IP Party B and the EI serving IP Party B is not depicted.

5.3.4.12.2.2 INVITE with sdp Video Offer – Called Party Accepts Video after 200 Response

Party A affirmatively signals its EI an intention to request a video telephony call. This is reflected in the INVITE that includes an sdp offer of audio and video capabilities, shown in Figure 5.3.4-4. Party B is apprised of the video telephony call request and does not signal its EI to accept the video telephony offer until after the 200 response is sent. Party B's EI sends a re-INVITE (or equivalent) offering audio and video capabilities pursuant to Party B's affirmative signal to engage in a video call. Upon receipt of the INVITE with the sdp offer, Party A's EI notifies Party A of the offer to add video to the call. Party A affirmatively signals a desire to add video. An ACK with an sdp answer accepting audio and video capabilities is sent back to the LSC serving IP Party B.

STEP	INSTRUCTION
1, 2, 3	Party A affirmatively signals to end instrument a desire to initiate a video telephony call Upon receiving an initial call request message from IP Party A (not depicted in the call flow diagram), the LSC serving IP Party A either generates and sends an INVITE with an sdp offering audio and video capabilities to Softswitch A or forwards an INVITE with an sdp offering audio and video capabilities (created by SIP EI A) to Softswitch A. Softswitch A forwards the INVITE across the WAN to Softswitch B (which is assigned to the LSC serving IP Party B). Softswitch B forwards the INVITE to the LSC serving IP Party B. When LSC serving IP Party B sends an INVITE or other call request message to the EI serving IP Party B then party B is notified by the called end instrument that a video telephone call has been requested so that party B has the opportunity to affirmatively indicate to the end instrument a desire to accept a video call. NOTE: Signaling between the EI serving IP Party A and the LSC serving IP Party A is not depicted. In addition, signaling between the LSC serving IP Party B and the EI serving IP Party B is not depicted. However, it should be noted that **ASAC** Prior to sending 1, LSC A increments video count. Upon receiving 2, Softswitch A increments video count. Upon receiving 3, LSC B increments video count.

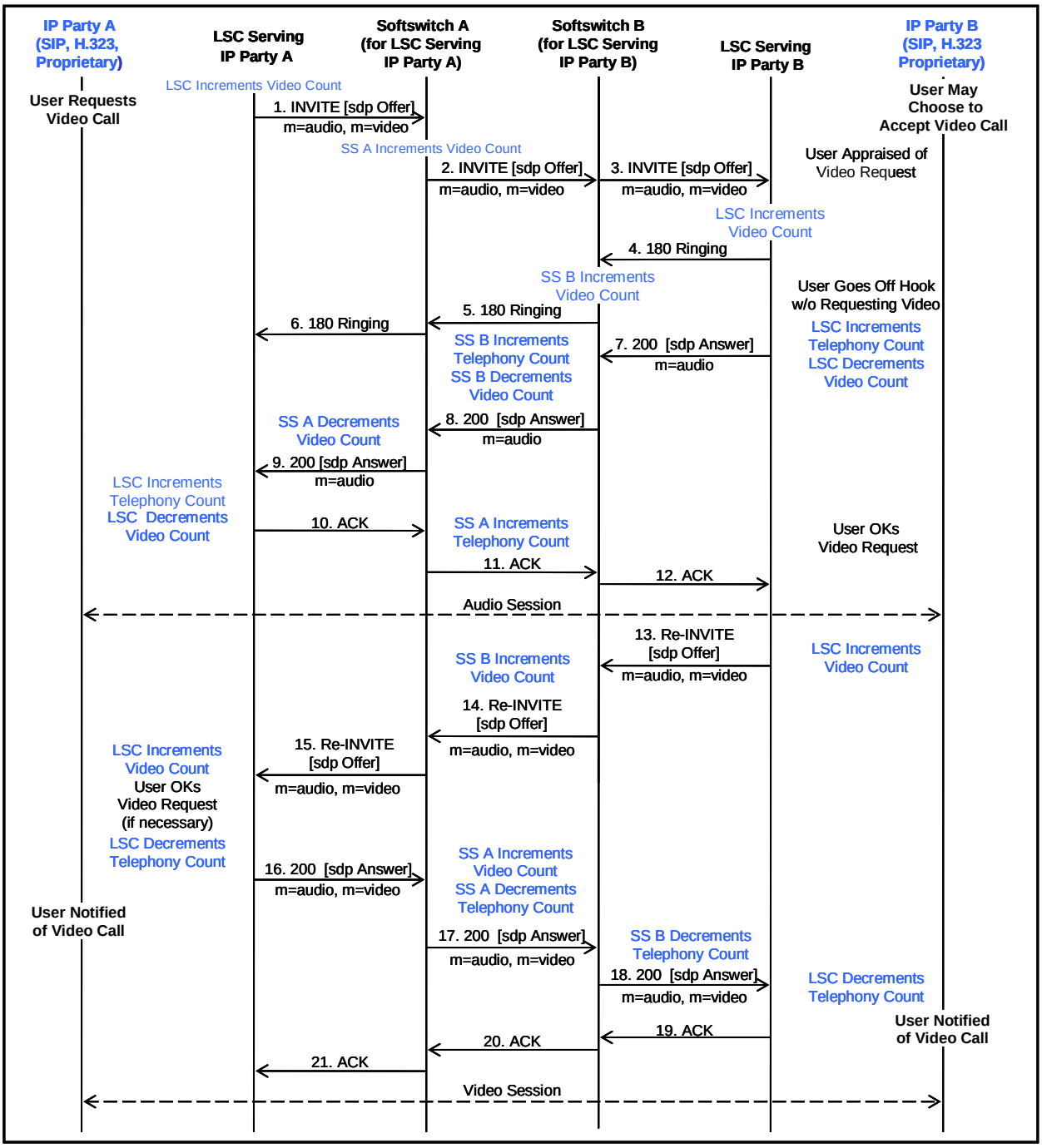


Figure 5.3.4-4. INVITE with sdp Video Offer – Called Party Accepts Video after 200 Response

STEP	INSTRUCTION
4, 5, 6	Assuming the end instrument is not busy, the LSC serving IP Party B sends a 180 (Ringing) to Softswitch B. It forwards the 180 (Ringing) to Softswitch A, which forwards the 180 (Ringing) to the LSC serving IP Party A. NOTE: Signaling between the EI serving IP Party B and the LSC serving IP Party B is not depicted. In addition, signaling between the LSC serving IP Party A and the EI serving IP Party A is not depicted. **ASAC** Upon receiving 4, Softswitch B increments video count.
7, 8, 9	Party B does NOT affirmatively signal to its EI a desire to accept a video telephone call When IP Party B goes off hook (i.e., answers the call), the LSC serving IP Party B sends a 200 (OK) with an sdp answer accepting audio capabilities to Softswitch B. Softswitch B forwards the 200 (OK) to Softswitch A, which forwards the 200 (OK) to the LSC serving IP Party A. NOTE: Signaling between the EI serving IP Party B and the LSC serving IP Party B is not depicted. In addition, signaling between the LSC serving IP Party A and the EI serving IP Party A is not depicted. **ASAC** Prior to sending 7, LSC B increments telephony count and decrements video count. Upon receiving 7, Softswitch B increments telephony count and decrements video count. Upon receiving 8, Softswitch A decrements video count. Upon receiving 9, LSC A increments telephony count.
10, 11, 12	The LSC serving IP Party A sends an ACK to Softswitch A. It forwards the ACK to Softswitch B, which forwards the ACK to the LSC serving IP Party B. NOTE: Signaling between the EI serving IP Party A and the LSC serving IP Party A is not depicted. In addition, signaling between the LSC serving IP Party B and the EI serving IP Party B is not depicted. **ASAC** Prior to sending 10, LSC A decrements video count. Upon receiving 10, Softswitch A increments telephony count.

STEP	INSTRUCTION
13, 14, 15	Party B affirmatively signals to its end instrument a desire to add video to the existing call Upon receiving a call request/change message (re-INVITE in the case of a SIP EI) (not depicted in the call flow diagram), the LSC serving IP Party B either generates and sends a re-INVITE with an sdp offering audio and video capabilities to Softswitch B, or forwards a re-INVITE with an sdp offering audio and video capabilities (created by SIP EI B) to Softswitch B. Softswitch B forwards the re-INVITE across the WAN to Softswitch A (which is assigned to the LSC serving IP Party A). Softswitch A forwards the INVITE to the LSC serving IP Party A. When the LSC serving IP Party A sends the re-INVITE or equivalent call request message to the EI serving IP Party A, then Party A is notified by the end instrument that Party A is being requested to turn the existing call into a video telephony call. NOTE: Signaling between the EI serving IP Party B and the LSC serving IP Party B is not depicted. In addition, signaling between the LSC serving IP Party A and the EI serving IP Party A is not depicted. **ASAC** Prior to sending 13, LSC B increments video count. Upon receiving 13, Softswitch B increments video count. Upon receiving 15, LSC A increments video count.
16, 17, 18	Party A affirmatively signals its EI of Party A's intention to convert the call to a video telephony call. Upon receiving a positive response from Party A's EI, the LSC serving IP Party A either generates and sends a 200 (OK) with an sdp answer accepting audio and video capabilities to Softswitch A or forwards a 200 (OK) with an sdp answer accepting audio and video capabilities (created by SIP EI A) to Softswitch A. Softswitch A forwards the 200 (OK) across the WAN to Softswitch B. Softswitch B forwards the 200 (OK) to the LSC serving IP Party B. EI A notifies Party A that a video call has been established. NOTE: Signaling between the EI serving IP Party A and the LSC serving IP Party A is not depicted. In addition, signaling between the LSC serving IP Party B and the EI serving IP Party B is not depicted. **ASAC** Prior to sending 16, LSC A decrements telephony count. Upon receiving 16, Softswitch A increments video count and decrements telephony count. Upon receiving 17, Softswitch B decrements telephony count. Upon receiving 18, LSC B decrements telephony count.

STEP	INSTRUCTION
19, 20, 21	EI B notifies Party B that a video call has been established. The LSC serving IP Party B sends an ACK to Softswitch B. It forwards the ACK to Softswitch A, which forwards the ACK to the LSC serving IP Party A. NOTE: Signaling between the EI serving IP Party B and the LSC serving IP Party B is not depicted. In addition, signaling between the LSC serving IP Party A and the EI serving IP Party A is not depicted.

5.3.4.12.2.3 Empty INVITE – Caller Requests Video; Called Party Offers Video (Media Feature Tags NOT Used)

Party A affirmatively signals to its EI an intention to request a video telephony call. An Empty INVITE, shown in Figure 5.3.4-5, is sent to the LSC serving IP Party B. When Party B's EI receives the Empty INVITE (or equivalent call request) Party B's EI MAY offer Party B the option of requesting a video telephony call. Party B affirmatively signals its EI of its intention to offer a video telephony call and the 200 (OK) includes an sdp offer that includes audio and video capabilities. Party A's EI accepts the audio and video capabilities and an ACKwith an sdp answer having audio and video capabilities is sent back over the DISN WAN to IP Party B.

STEP	INSTRUCTION
1, 2, 3	Party A affirmatively signals to end instrument an intention to initiate a video telephony call Upon receiving an initial call request message from IP Party A (not depicted in the call flow diagram), the LSC serving IP Party A either generates and sends an Empty INVITE to Softswitch A or forwards an Empty INVITE (created by SIP EI A) to Softswitch A. Softswitch A forwards the Empty INVITE across the WAN to Softswitch B (which is assigned to the LSC serving IP Party B). Softswitch B forwards the Empty INVITE to the LSC serving IP Party B. When the LSC serving IP Party B sends an Empty INVITE or other call request message to the IP EI serving Party B, then the EI MAY apprise Party B of the option of requesting a video call. NOTE: Signaling between the EI serving IP Party A and the LSC serving IP Party A is not depicted. In addition, signaling between the LSC serving IP Party B and the EI serving IP Party B is not depicted. **ASAC** Prior to sending 1, LSC A increments telephony count. Upon receiving 2, Softswitch A increments telephony count. Upon receiving 3, LSC B increments telephony count.

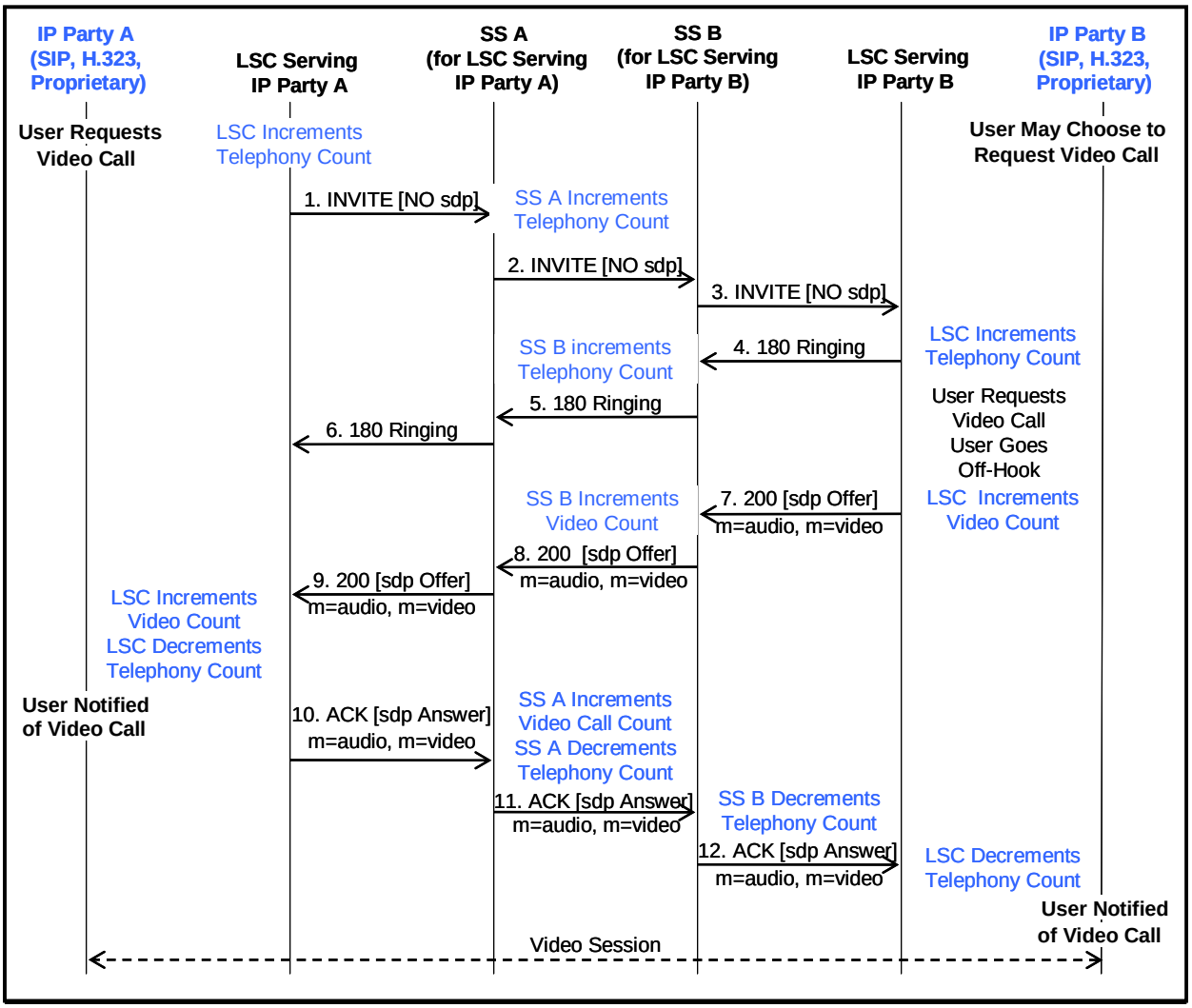


Figure 5.3.4-5. Empty INVITE – Caller Requests Video; Called Party Offers Video (Media Feature Tags NOT Used)

STEP	INSTRUCTION
4, 5, 6	Assuming the end instrument is not busy, the LSC serving IP Party B sends a 180 (Ringing) to Softswitch B. It forwards the 180 (Ringing) to Softswitch A, which forwards the 180 (Ringing) to the LSC serving IP Party A. NOTE: Signaling between the EI serving IP Party B and the LSC serving IP Party B is not depicted. In addition, signaling between the LSC serving IP Party A and the EI serving IP Party A is not depicted. **ASAC** Upon receiving 4, Softswitch B increments telephony count.

7, 8, 9	Party B affirmatively signals to its EI an intention to engage in a video telephone call. When IP Party B goes off hook (i.e., answers the call), the LSC serving IP Party B sends a 200 (OK) with an sdp offer of audio and video capabilities to Softswitch B. Softswitch B forwards the 200 (OK) to Softswitch A, which forwards the 200 (OK) to the LSC serving IP Party A. NOTE: Signaling between the EI serving IP Party B and the LSC serving IP Party B is not depicted. In addition, signaling between the LSC serving IP Party A and the EI serving IP Party A is not depicted. **ASAC** Prior to sending 7, LSC B increments video count. Upon receiving 7, Softswitch B increments video count. Upon receiving 9, LSC A increments video count.
10, 11, 12	Since the caller had affirmatively signaled to the EI a desire to engage in a video telephone call and the initial offer from the remote side is a video telephone offer, then the EI will accept the video telephone offer. EI A notifies Party A that a video call has been established. The LSC serving IP Party A sends an ACK with an sdp answer accepting audio and video capabilities to Softswitch A. It forwards the ACK to Softswitch B, which forwards the ACK to the LSC serving IP Party B. EI B notifies party B that a video call has been established. NOTE: Signaling between the EI serving IP Party A and the LSC serving IP Party A is not depicted. In addition, signaling between the LSC serving IP Party B and the EI serving IP Party B is not depicted. **ASAC** Prior to sending 10, LSC A decrements telephony count. Upon receiving 10, Softswitch A increments video count and decrements telephony count. Upon receiving 11, Softswitch B decrements telephony count. Upon receiving 12, LSC B decrements telephony count.

5.3.4.12.2.4 Empty INVITE – Caller Requests Video; Called Party Offers Audio; Caller Again Requests Video (Media Feature Tags NOT Used)

Party A affirmatively signals to its EI an intention to request a video telephony call. An Empty INVITE is sent to the LSC serving IP Party B. When party B's EI receives the Empty INVITE (or equivalent call request) party B's EI MAY offer Party B the option of requesting a video telephony call. This is illustrated in Figure 5.3.4-6. Party B does NOT signal its EI to offer a video telephony call and the 200 (OK) includes an sdp offer with audio capabilities only. Party

A's EI accepts the audio offer and an ACK with an sdp answer accepting audio capability is sent back over the DISN WAN to IP Party B. Party A again affirmatively signals its EI that it would like to add video to the telephony call and a re-INVITE with an sdp offer of audio and video capabilities is sent to IP Party B. Party B's EI notifies IP Party B of the request to add video. Party B affirmatively signals its EI to accept the video telephony upgrade and a 200 (OK) with an sdp answer accepting audio and video capabilities is sent over the DISN WAN to IP party A.

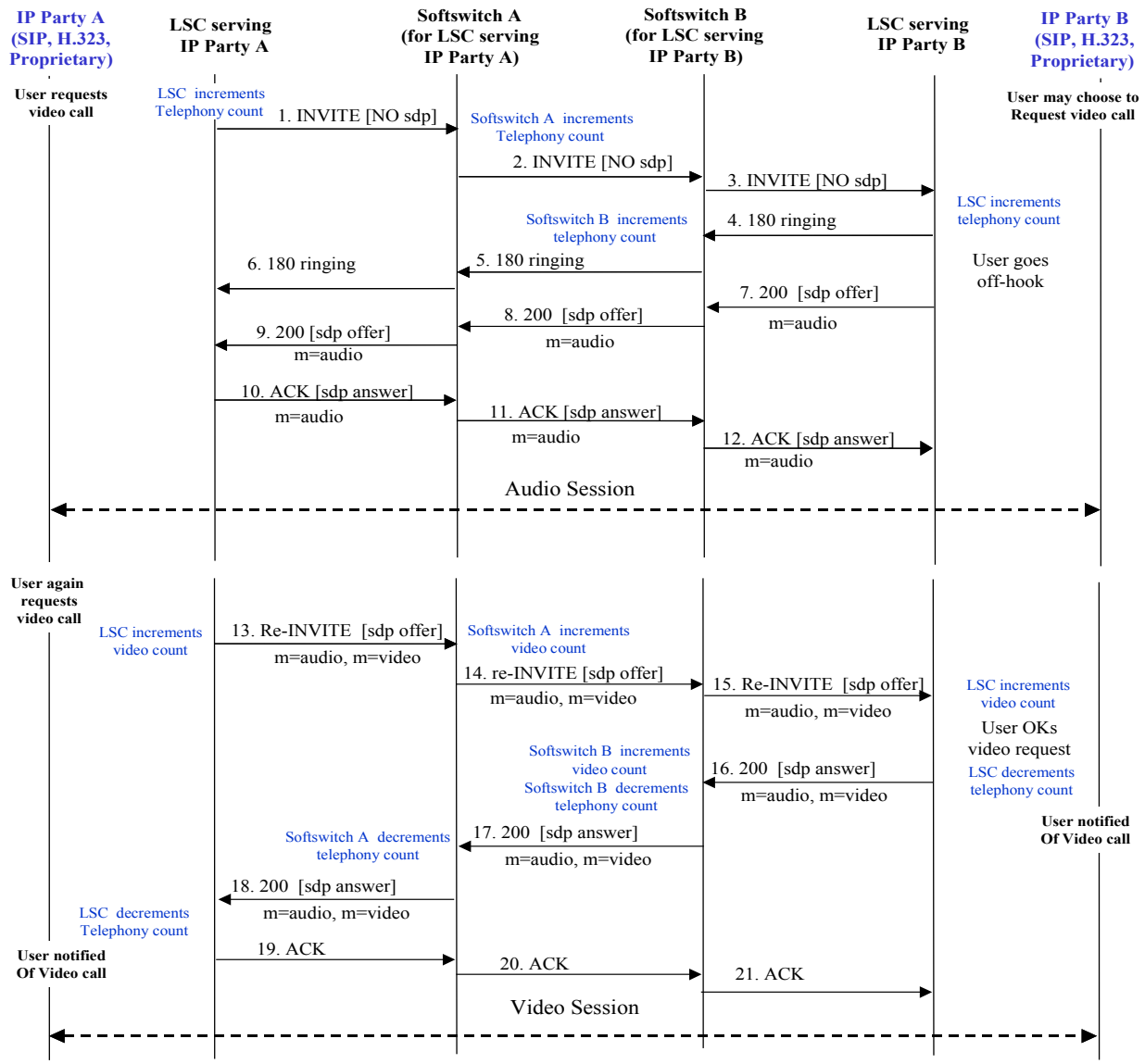


Figure 5.3.4-6. Empty INVITE – Caller Requests Video; Called Party Offers Audio; Caller Again Requests Video (Media Feature Tags NOT Used)

STEP	INSTRUCTION
1, 2, 3	Party A affirmatively signals to its EI an intention to initiate a video telephony call. Upon receiving an initial call request message from IP Party A (not depicted in the call flow diagram), the LSC serving IP Party A either generates and sends an Empty INVITE to Softswitch A or forwards an Empty INVITE (created by SIP EI A) to Softswitch A. Softswitch A forwards the Empty INVITE across the WAN to Softswitch B (which is assigned to the LSC serving IP Party B). Softswitch B forwards the Empty INVITE to the LSC serving IP Party B. When the LSC serving IP Party B sends an Empty INVITE or other call request message to the IP EI serving Party B, then the EI MAY apprise Party B of the option of requesting a video call. NOTE: Signaling between the EI serving IP Party A and the LSC serving IP Party A is not depicted. In addition, signaling between the LSC serving IP Party B and the EI serving IP Party B is not depicted. **ASAC** Prior to sending 1, LSC A increments telephony count. Upon receiving 1, Softswitch A increments telephony count. Upon receiving 3, LSC B increments telephony count.
4, 5, 6	Assuming the end instrument is not busy, the LSC serving IP Party B sends a 180 (Ringing) to Softswitch B. It forwards the 180 (Ringing) to Softswitch A, which forwards the 180 (Ringing) to the LSC serving IP Party A. NOTE: Signaling between the EI serving IP Party B and the LSC serving IP Party B is not depicted. In addition, signaling between the LSC serving IP Party A and the EI serving IP Party A is not depicted. **ASAC** Upon receiving 4, Softswitch B increments telephony count.
7, 8, 9	Party B does NOT signal to its EI an intention to engage in a video telephone call. When IP Party B goes off hook (i.e., answers the call), the LSC serving IP Party B sends a 200 (OK) with an sdp offer of audio capabilities to Softswitch B. Softswitch B forwards the 200 (OK) to Softswitch A, which forwards the 200 (OK) to the LSC serving IP Party A. NOTE: Signaling between the EI serving IP Party B and the LSC serving IP Party B is not depicted. In addition, signaling between the LSC serving IP Party A and the EI serving IP Party A is not depicted.

STEP	INSTRUCTION
10, 11, 12	Party A's EI accepts the audio telephone offer. The LSC serving IP Party A sends an ACK with an sdp answer accepting audio capability to Softswitch A. It forwards the ACK to Softswitch B, which forwards the ACK to the LSC serving IP Party B. NOTE: Signaling between the EI serving IP Party A and the LSC serving IP Party A is not depicted. In addition, signaling between the LSC serving IP Party B and the EI serving IP Party B is not depicted.
13, 14, 15	Party A affirmatively signals to its EI an intention to add video to the telephony call. Upon receiving call request/change message from IP Party A (not depicted in the call flow diagram), the LSC serving IP Party A either generates and sends a re-INVITE with an sdp offering audio and video capabilities to Softswitch A or forwards a re-INVITE with an sdp offering audio and video capabilities (created by SIP EI A) to Softswitch A. Softswitch A forwards the re-INVITE across the WAN to Softswitch B (which is assigned to the LSC serving IP Party B). Softswitch B forwards the INVITE to the LSC serving IP Party B. When the LSC serving IP Party B sends the re-INVITE or equivalent call request message to the EI serving IP Party B, then Party B is notified by the end instrument that a video offer is being made, and Party B has the opportunity to affirmatively signal to the end instrument a desire to turn the existing call into a video telephony call. NOTE: Signaling between the EI serving IP Party A and the LSC serving IP Party A is not depicted. In addition, signaling between the LSC serving IP Party B and the EI serving IP Party B is not depicted. **ASAC** Prior to sending 13, LSC A increments video count. Upon receiving 13, Softswitch A increments video count. Upon receiving 15, LSC B increments video count.
16, 17, 18	Party B affirmatively signals its EI that Party B wishes to convert the call to a video telephony call. The LSC serving IP Party B either generates and sends a 200 (OK) with an sdp answer accepting audio and video capabilities to Softswitch B or forwards a 200 (OK) with an sdp answer accepting audio and video capabilities (created by SIP EI B) to Softswitch B. Softswitch B forwards the 200 (OK) across the WAN to Softswitch A. Softswitch A forwards the INVITE to the LSC serving IP Party B. Party B's EI notifies Party B that video has been added to the call. NOTE: Signaling between the EI serving IP Party B and the LSC serving IP Party B is not depicted. In addition, signaling between the LSC serving IP Party A and the EI serving IP Party A is not depicted.

STEP	INSTRUCTION
	ASAC Prior to sending 16, LSC B decrements telephony count. Upon receiving 16, Softswitch B increments video count and decrements telephony count. Upon receiving 17, Softswitch A decrements telephony count. Upon receiving 18, LSC A decrements telephony count.
19, 20, 21	Party A's EI notifies Party A that video has been added to the call. The LSC serving IP Party A sends an ACK to Softswitch A. It forwards the ACK to Softswitch B, which forwards the ACK to the LSC serving IP Party B. NOTE: Signaling between the EI serving IP Party A and the LSC serving IP Party AB is not depicted. In addition, signaling between the LSC serving IP Party B and the EI serving IP Party B is not depicted.

5.3.4.12.2.5 Empty INVITE – Caller Requests Video; Called party Offers Video (Media Feature Tags Used by Originating LSC and Terminating LSC)

The AS-SIP message sequence in this call flow is identical to that of Section 5.3.4.12.2.3, Empty INVITE – Caller Requests Video; Called Party Offers Video (Media Feature Tags NOT Used). The use of media feature tags by the LSCs alters the specific ASAC actions taken during the course of session establishment; however, the ASAC end state is the same as for Section 5.3.4.12.2.3 (see Figure 5.3.4-7, Empty INVITE – Caller Requests Video; Called Party Offers Video (Media Feature Tags Used by Originating LSC and Terminating LSC)).

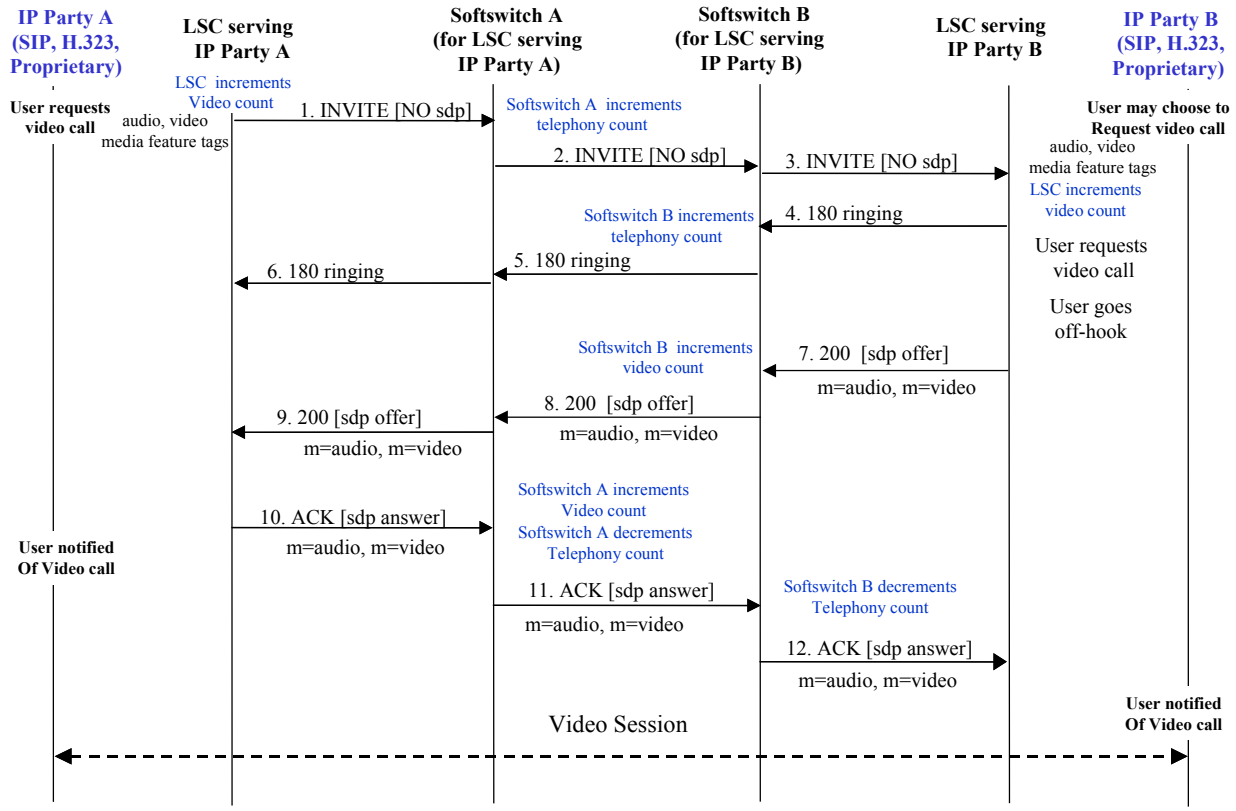


Figure 5.3.4-7. Empty INVITE – Caller Requests Video; Called Party Offers Video (Media Feature Tags Used by Originating LSC and Terminating LSC)

STEP	INSTRUCTION
1, 2, 3	Party A affirmatively signals to end instrument an intention to initiate a video telephony call. Upon receiving an initial call request message from IP Party A (not depicted in the call flow diagram), the LSC serving IP Party A either generates and sends an Empty INVITE to Softswitch A or forwards an Empty INVITE (created by SIP EI A) to Softswitch A. Softswitch A forwards the Empty INVITE across the WAN to Softswitch B (which is assigned to the LSC serving IP Party B). Softswitch B forwards the Empty INVITE to the LSC serving IP Party B. When the LSC serving IP Party B sends an Empty INVITE or other call request message to the IP EI serving party B, then the EI MAY apprise Party B of the option of requesting a video call. NOTE: Signaling between the EI serving IP Party A and the LSC serving IP Party A is not depicted. In addition, signaling between the LSC serving IP Party B and the EI serving IP Party B is not depicted.

STEP	INSTRUCTION
	ASAC Prior to sending 1, LSC A increments video count. Upon receiving 2, Softswitch A increments telephony count. Upon receiving 3, LSC B increments video count.
4, 5, 6	Assuming the end instrument is not busy, the LSC serving IP Party B sends a 180 (Ringing) to Softswitch B. It forwards the 180 (Ringing) to Softswitch A, which forwards the 180 (Ringing) to the LSC serving IP Party A. NOTE: Signaling between the EI serving IP Party B and the LSC serving IP Party B is not depicted. In addition, signaling between the LSC serving IP Party A and the EI serving IP Party A is not depicted. **ASAC** Upon receiving 4, Softswitch B increments telephony count.
7, 8, 9	Party B affirmatively signals to its EI an intention to engage in a video telephone call. When IP Party B goes off hook (i.e., answers the call), the LSC serving IP Party B sends a 200 (OK) with an sdp offer of audio and video capabilities to Softswitch B. Softswitch B forwards the 200 (OK) to Softswitch A, which forwards the 200 (OK) to the LSC serving IP Party A. NOTE: Signaling between the EI serving IP Party B and the LSC serving IP Party B is not depicted. In addition, signaling between the LSC serving IP Party A and the EI serving IP Party A is not depicted. **ASAC** Upon receiving 7, Softswitch B increments video count.

10, 11, 12	Since the caller had affirmatively signaled to the EI a desire to engage in a video telephone call and the initial offer from the remote side is a video telephone offer, then the EI will accept the video telephone offer. EI A notifies Party A that a video call has been established. The LSC serving IP Party A sends an ACK with an sdp answer accepting audio and video capabilities to Softswitch A. It forwards the ACK to Softswitch B, which forwards the ACK to the LSC serving IP Party B. EI B notifies Party B that a video call has been established. NOTE: Signaling between the EI serving IP Party A and the LSC serving IP Party A is not depicted. In addition, signaling between the LSC serving IP Party B and the EI serving IP Party B is not depicted. **ASAC** Upon receiving 10, Softswitch A increments video count and decrements telephony count. Upon receiving 11, Softswitch B decrements telephony count.

5.3.4.12.2.6 Empty INVITE – Caller Requests Video; Called Party Offers Audio – Calling Party Again Requests Video (Media Feature Tags Used by Originating LSC and Terminating LSC)

The AS-SIP message sequence in this call flow is identical to that of Section 5.3.4.12.2.4, Empty INVITE – Caller Requests Video; Called Party Offers Audio; Caller Again Requests Video (Media Feature Tags NOT Used). The use of media feature tags by the LSCs alters the specific ASAC actions taken during the course of session establishment; however, the ASAC end state is the same as for Section 5.3.4.12.2.4 (see Figure 5.3.4-8).

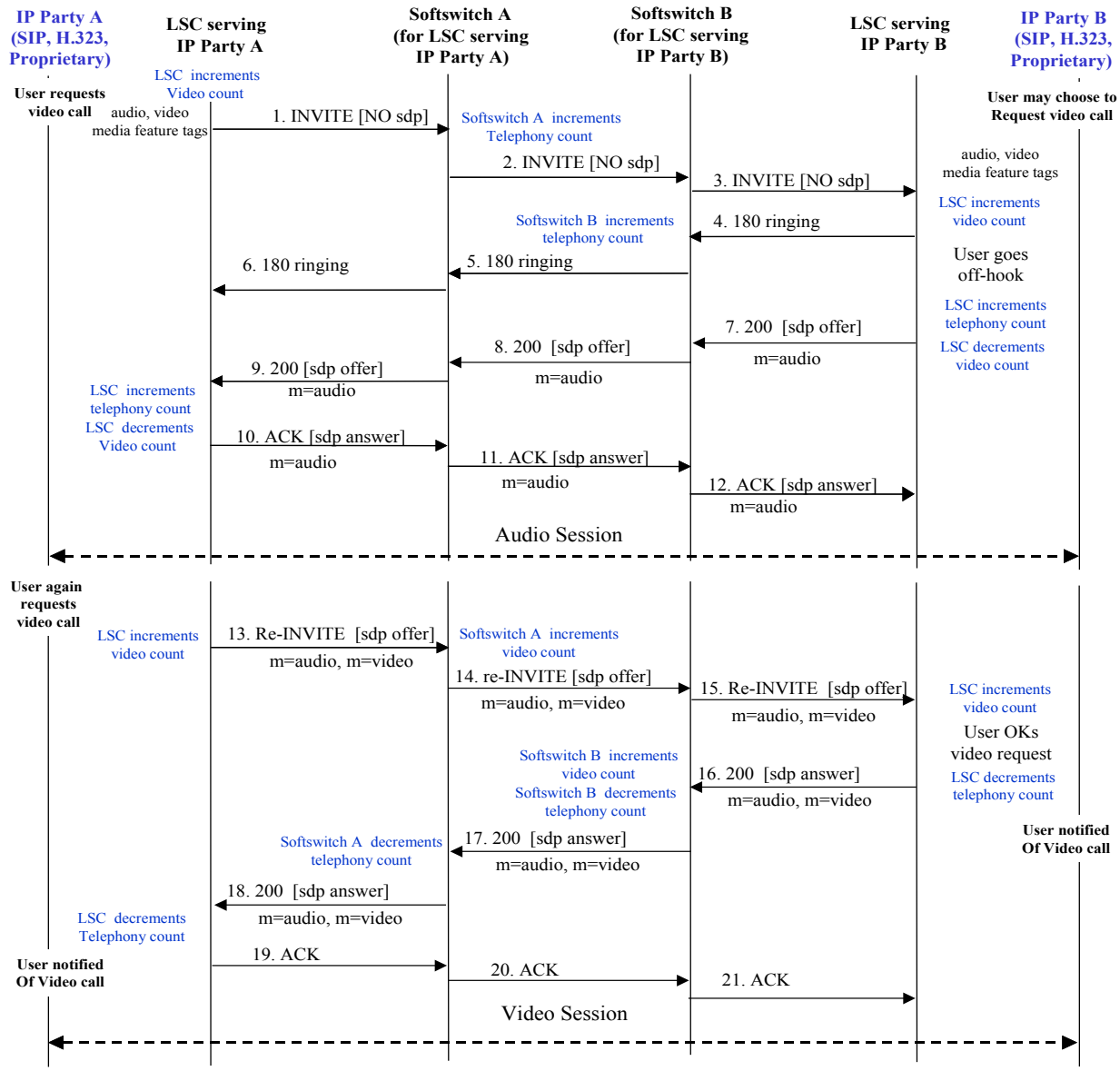


Figure 5.3.4-8. Empty INVITE – Caller Requests Video; Called Party Offers Audio – Calling Party Again Requests Video (Media Feature Tags Used by Originating LSC and Terminating LSC)

STEP	INSTRUCTION
1, 2, 3	Party A affirmatively signals to its EI an intention to initiate a video telephony call. Upon receiving an initial call request message from IP Party A (not depicted in the call flow diagram), the LSC serving IP Party A either generates and sends an Empty INVITE to Softswitch A or forwards an Empty INVITE (created by SIP EI A) to Softswitch A. Softswitch A forwards the Empty INVITE across the WAN to Softswitch B (which is assigned to the LSC serving IP Party B). Softswitch B forwards the Empty INVITE to the LSC serving IP Party B. When LSC serving IP Party B sends an Empty INVITE or other call request message to the IP EI serving Party B, then the EI MAY apprise Party B of the option of requesting a video call. NOTE: Signaling between the EI serving IP Party A and the LSC serving IP Party A is not depicted. In addition, signaling between the LSC serving IP Party B and the EI serving IP Party B is not depicted. **ASAC** Prior to sending 1, LSC A increments video count. Upon receiving 1, Softswitch A increments telephony count. Upon receiving 3, LSC B increments video count.
4, 5, 6	Assuming the end instrument is not busy, the LSC serving IP Party B sends a 180 (Ringing) to Softswitch B. It forwards the 180 (Ringing) to Softswitch A, which forwards the 180 (Ringing) to the LSC serving IP Party A. NOTE: Signaling between the EI serving IP Party B and the LSC serving IP Party B is not depicted. In addition, signaling between the LSC serving IP Party A and the EI serving IP Party A is not depicted. **ASAC** Upon receiving 4, Softswitch B increments telephony count.

STEP	INSTRUCTION
7, 8, 9	Party B does NOT signal to its EI an intention to engage in a video telephone call. When IP Party B goes off hook (i.e., answers the call), the LSC serving IP Party B sends a 200 (OK) with an sdp offer of audio capabilities to Softswitch B. Softswitch B forwards the 200 (OK) to Softswitch A, which forwards the 200 (OK) to the LSC serving IP Party A. NOTE: Signaling between the EI serving IP Party B and the LSC serving IP Party B is not depicted. In addition, signaling between the LSC serving IP Party A and the EI serving IP Party A is not depicted. **ASAC** Prior to sending 7, LSC B increments telephony count and decrements video count. Upon receiving 9, LSC A increments telephony count.
10, 11, 12	Party A's EI accepts the audio telephone offer. The LSC serving IP Party A sends an ACK with an sdp answer accepting audio capability to Softswitch A. It forwards the ACK to Softswitch B, which forwards the ACK to the LSC serving IP Party B. NOTE: Signaling between the EI serving IP Party A and the LSC serving IP Party A is not depicted. In addition, signaling between the LSC serving IP Party B and the EI serving IP Party B is not depicted. **ASAC** Prior to sending 10, LSC A decrements video count.
13, 14, 15	Party A affirmatively signals to its EI an intention to add video to the telephony call. Upon receiving call request/change message from IP Party A (not depicted in the call flow diagram), the LSC serving IP Party A either generates and sends a re-INVITE with an sdp offering audio and video capabilities to Softswitch A or forwards a re-INVITE with an sdp offering audio and video capabilities (created by SIP EI A) to Softswitch A. Softswitch A forwards the re-INVITE across the WAN to Softswitch B (which is assigned to the LSC serving IP Party B). Softswitch B forwards the INVITE to the LSC serving IP Party B. When the LSC serving IP Party B sends the re-INVITE or equivalent call request message to the EI serving IP Party B, then Party B is notified by the end instrument that a video offer is being made, and Party B has the opportunity to affirmatively signal to the end instrument a desire to turn the existing call into a video telephony call. NOTE: Signaling between the EI serving IP Party A and the LSC serving IP Party A is not depicted. In addition, signaling between the LSC serving IP Party B and the EI serving IP Party B is not depicted.

STEP	INSTRUCTION
	ASAC Prior to sending 13, LSC A increments video count. Upon receiving 13, Softswitch A increments video count. Upon receiving 15, LSC B increments video count.
16, 17, 18	Party B affirmatively signals its EI that Party B wishes to convert the call to a video telephony call. The LSC serving IP Party B either generates and sends a 200 (OK) with an sdp answer accepting audio and video capabilities to Softswitch B or forwards a 200 (OK) with an sdp answer accepting audio and video capabilities (created by SIP EI B) to Softswitch B. Softswitch B forwards the 200 (OK) across the WAN to Softswitch A. Softswitch A forwards the INVITE to the LSC serving IP Party B. Party B's EI notifies Party B that video has been added to the call. NOTE: Signaling between the EI serving IP Party B and the LSC serving IP Party B is not depicted. In addition, signaling between the LSC serving IP Party A and the EI serving IP Party A is not depicted. **ASAC** Prior to sending 16, LSC B decrements telephony count. Upon receiving 16, Softswitch B increments video count and decrements telephony count. Upon receiving 17, Softswitch A decrements telephony count. Upon receiving 18, LSC A decrements telephony count.
19, 20, 21	Party A's EI notifies Party A that video has been added to the call. The LSC serving IP Party A sends an ACK to Softswitch A. It forwards the ACK to Softswitch B, which forwards the ACK to the LSC serving IP Party B. NOTE: Signaling between the EI serving IP Party A and the LSC serving IP Party AB is not depicted. In addition, signaling between the LSC serving IP Party B and the EI serving IP Party B is not depicted.

5.3.4.12.3 IP-to-IP Video Conference Unit Call Flows

5.3.4.12.3.1 VCU INVITE with sdp Video Offer

The originating LSC sends an INVITE that includes an sdp offer of audio and video capabilities on behalf of video conferencing unit (VCU) A. The terminating LSC responds with a 200 sdp answer accepting audio and video capabilities on behalf of VCU B (see Figure 5.3.4-9).

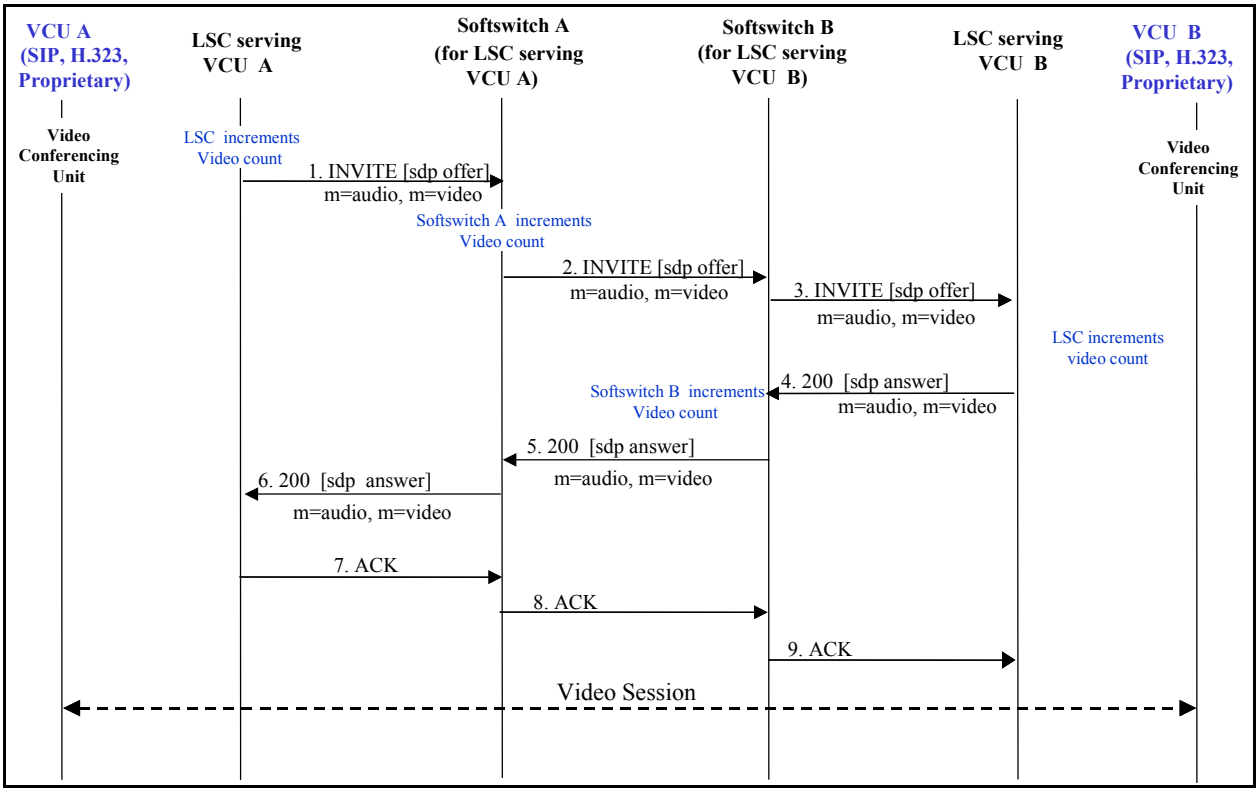


Figure 5.3.4-9. VCU INVITE with sdp Video Offer

STEP	INSTRUCTION
1, 2, 3	Upon receiving an initial call request message from VCU A (not depicted in the call flow diagram), the LSC serving VCU A either generates and sends an INVITE with an sdp offer for audio and video capabilities to Softswitch A or forwards an INVITE with an sdp offer for audio and video capabilities (created by VCU A) to Softswitch A. Softswitch A forwards the INVITE across the WAN to Softswitch B (which is assigned to the LSC serving VCU B). Softswitch B forwards the INVITE to the LSC serving VCU B. NOTE: Signaling between VCU A and the LSC serving VCU A is not depicted. In addition, signaling between the LSC serving VCU B and VCU B is not depicted. **ASAC** Prior to sending 1, LSC A increments video count. Upon receiving 2, Softswitch A increments video count. Upon receiving 3, LSC B increments video count.
4, 5, 6	When VCU B answers the call, the LSC serving VCU B sends a 200 (OK) with an sdp answer accepting audio and video capabilities to Softswitch B. Softswitch B forwards the 200 (OK) to Softswitch A, which forwards the 200 (OK) to the LSC serving VCU A. NOTE: Signaling between VCU B and the LSC serving VCU B is not depicted. In addition, signaling between the LSC serving VCU A and VCU A is not depicted. **ASAC** Upon receiving 4, Softswitch B increments video count.
7, 8, 9	The LSC serving VCU A sends an ACK to Softswitch A. It forwards the ACK to Softswitch B, which forwards the ACK to the LSC serving VCU B. NOTE: Signaling between VCU A and the LSC serving VCU A is not depicted. In addition, signaling between the LSC serving VCU B and VCU B is not depicted.

5.3.4.12.3.2 VCU Empty INVITE (Media Feature Tags NOT Used)

The originating LSC sends an Empty INVITE. The terminating LSC responds with a 200 sdp offer of audio and video capabilities on behalf of VCU B. VCU A accepts audio and video capabilities and the originating LSC responds with an ACK request that includes an sdp answer accepting the audio and video capabilities (see Figure 5.3.4-10, VCU Empty INVITE (Media Feature Tags NOT Used).

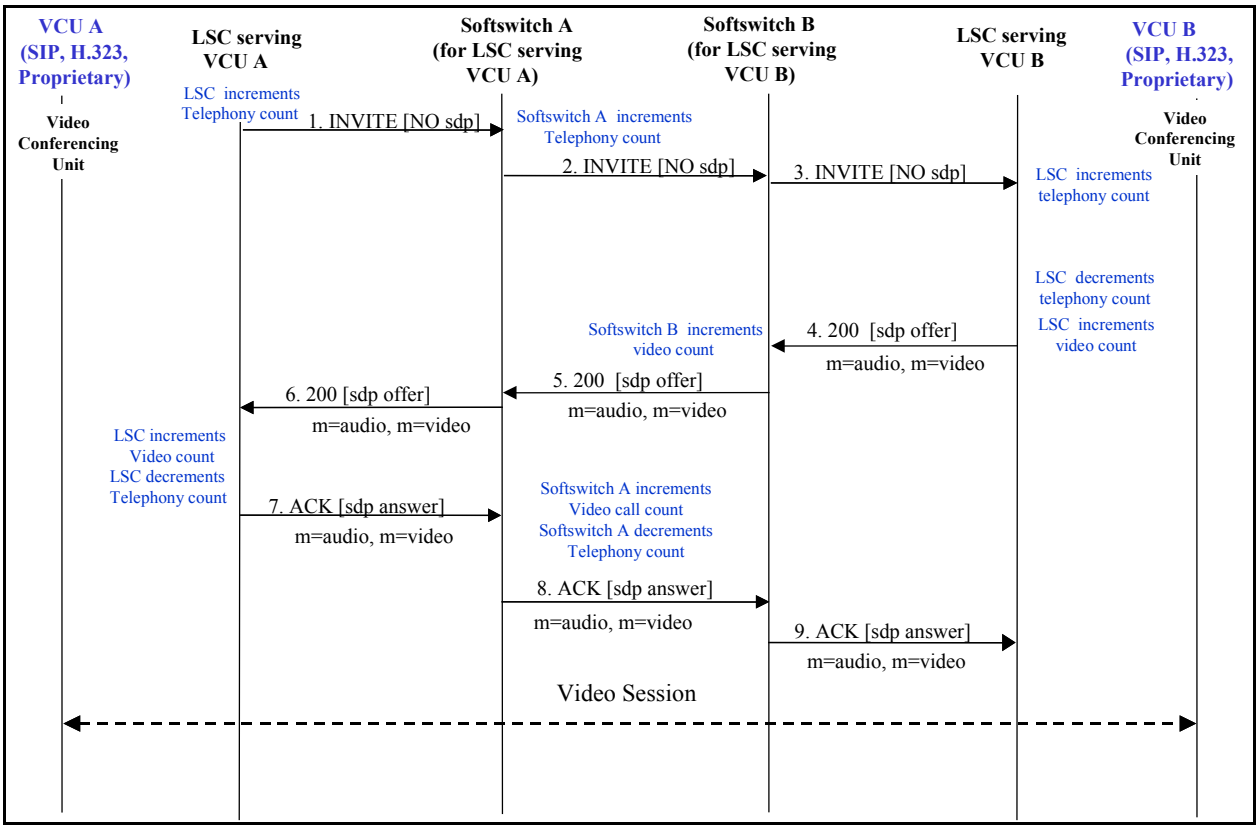


Figure 5.3.4-10. VCU Empty INVITE (Media Feature Tags NOT Used)

STEP	INSTRUCTION
1, 2, 3	Upon receiving an initial call request message from VCU A (not depicted in the call flow diagram), the LSC serving VCU A either generates and sends an Empty INVITE to Softswitch A or forwards an Empty INVITE (created by VCU A) to Softswitch A. Softswitch A forwards the Empty INVITE across the WAN to Softswitch B (which is assigned to the LSC serving VCU B). Softswitch B forwards the Empty INVITE to the LSC serving VCU B. NOTE: Signaling between VCU A and the LSC serving VCU A is not depicted. In addition, signaling between the LSC serving VCU B and VCU B is not depicted. **ASAC** Prior to sending 1, LSC A increments telephony count. Upon receiving 2, Softswitch A increments telephony count. Upon receiving 3, LSC B increments telephony count.

STEP	INSTRUCTION
4, 5, 6	VCU B answers the call and the LSC serving VCU B sends a 200 (OK) with an sdp offer for audio and video capabilities to Softswitch B. Softswitch B forwards the 200 (OK) to Softswitch A, which forwards the 200 (OK) to the LSC serving VCU A. NOTE: Signaling between VCU B and the LSC serving VCU B is not depicted. In addition, signaling between the LSC serving VCU A and VCU A is not depicted. **ASAC** Prior to sending 4, LSC B decrements telephony count and increments video count. Upon receiving 4, Softswitch B increments video count. Upon receiving 6, LSC A increments video count.
7, 8, 9	VCU A accepts the video offer and the LSC serving VCU A sends an ACK with an sdp answer accepting audio and video capabilities to Softswitch A. It forwards the ACK to Softswitch B, which forwards the ACK to the LSC serving VCU B. NOTE: Signaling between VCU A and the LSC serving VCU A is not depicted. In addition, signaling between the LSC serving VCU B and VCU B is not depicted. **ASAC** Prior to sending 7, LSC A decrements telephony count. Upon receiving 7, Softswitch A increments video count and decrements telephony count.

5.3.4.12.3.3 VCU Empty INVITE (Media Feature Tags Used by Originating LSC and Terminating LSC)

The AS-SIP message sequence in this call flow is identical to that of Section 5.3.4.12.3.2, VCU Empty INVITE (Media Feature Tags NOT Used). The use of media feature tags by the LSCs alters the specific ASAC actions taken during the course of session establishment; however, the ASAC end state is the same as for Section Section 5.3.4.12.3.2 (see Figure 5.3.4-11, VCU Empty INVITE (Mediai Feature Tags Used by Originating LSC and Terminating LSC).

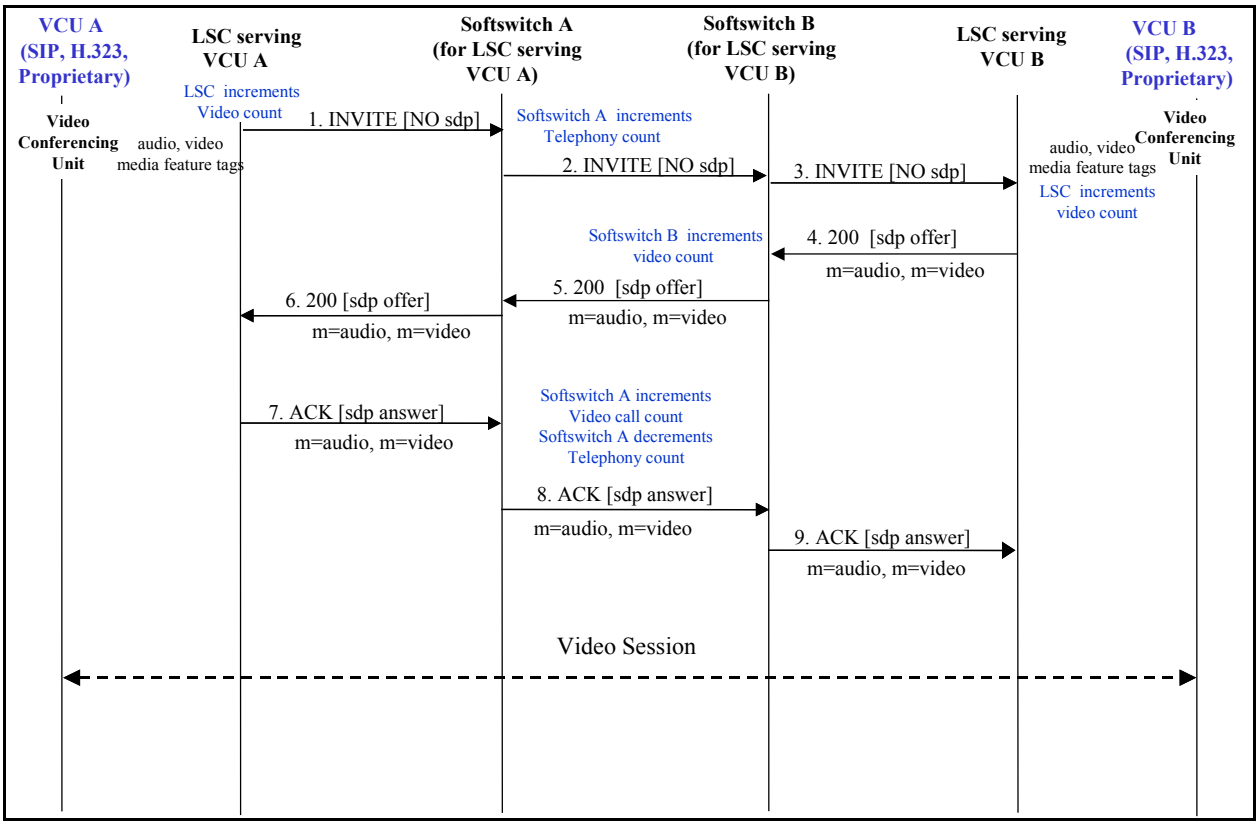


Figure 5.3.4-11. VCU Empty INVITE (Media Feature Tags Used by Originating LSC and Terminating LSC)

STEP	INSTRUCTION
1, 2, 3	Upon receiving an initial call request message from VCU A (not depicted in the call flow diagram), the LSC serving VCU A either generates and sends an Empty INVITE to Softswitch A or forwards an Empty INVITE (created by VCU A) to Softswitch A. Softswitch A forwards the Empty INVITE across the WAN to Softswitch B (which is assigned to the LSC serving VCU B). Softswitch B forwards the Empty INVITE to the LSC serving VCU B. NOTE: Signaling between VCU A and the LSC serving VCU A is not depicted. In addition, signaling between the LSC serving VCU B and VCU B is not depicted. **ASAC** Prior to sending 1, LSC A increments video count. Upon receiving 2, Softswitch A increments telephony count. Upon receiving 3, LSC B increments video count.

STEP	INSTRUCTION
4, 5, 6	VCU B answers the call and the LSC serving VCU B sends a 200 (OK) with an sdp offer for audio and video capabilities to Softswitch B. Softswitch B forwards the 200 (OK) to Softswitch A, which forwards the 200 (OK) to the LSC serving VCU A. NOTE: Signaling between VCU B and the LSC serving VCU B is not depicted. In addition, signaling between the LSC serving VCU A and VCU A is not depicted. **ASAC** Upon receiving 4, Softswitch B increments video count.
7, 8, 9	VCU A accepts the video offer and the LSC serving VCU A sends an ACK with an sdp answer accepting audio and video capabilities to Softswitch A. It forwards the ACK to Softswitch B, which forwards the ACK to the LSC serving VCU B. NOTE: Signaling between VCU A and the LSC serving VCU A is not depicted. In addition, signaling between the LSC serving VCU B and VCU B is not depicted. **ASAC** Upon receiving 7, Softswitch A increments video count and decrements telephony count.

5.3.4.13 Calling Services

5.3.4.13.1 Introduction

Many calling features are traditional to the TDM network and the PSTN. Within the PSTN, some calling features are required by law and regulated by the Federal Communications Commission (FCC). This specification is used within the context of a private network and thus is not necessarily subject to the same laws and regulations.

The focus of this specification is on the signaling-related functions and interfaces supported by the signaling appliances belonging to the DISN WAN or interfacing with the DISN WAN. This document places no restrictions on the line-side signaling method employed between AS-SIP signaling appliances and the IP end instruments served by those AS-SIP signaling appliances. The IP telephony signaling employed by and with the end instrument may be SIP, H.323, or proprietary. The only requirements on the line side are of a functional nature relating to the user experience (for example, the sequence of events experienced by a user of an IP end instrument when a call is to be preempted). In every case, the primary call flow diagram and description depicts and details the signaling flow across the DISN WAN but not between the signaling across the LAN between the AS-SIP signaling appliance serving an IP end instrument and the end instrument. In some cases, a secondary call flow diagram is provided that does depict SIP signaling down to the SIP end instrument in order to enhance the reader's understanding of the given call flow. However, it is the AS-SIP message sequences across the WAN that are

governed by this section. When depicted, the SIP message flows across the LAN are merely instructional.

The call flow diagrams assume the two-tier hierarchical architecture whereby for incoming or outgoing calls to be established across the DISN WAN, the LSC at a B/P/C/S exchanges its AS-SIP messages with a network-controlled Softswitch.

Call features 1, 2 3, 4, and 5 are required for the near-term open loop architecture. The near-term open loop architecture also requires AS-SIP to support the fax and modem services.

5.3.4.13.2 Point-to-Point Call

Signaling requirements for point-to-point calls are described for the following three call conditions:

- No reliable provisional response, no preconditions
- Segmented precondition
- End-to-end precondition

5.3.4.13.2.1 IP-to-IP Call Type

5.3.4.13.2.1.1 Figure 5.3.4-12, Successful Basic IP-to-IP Call (No Reliable Provisional Responses, No Preconditions), depicts the sequence of AS-SIP messages between the AS-SIP signaling appliance serving IP Party A and the AS-SIP signaling appliance serving IP Party B employed to establish and then tear down a telephony session between the parties. The call flow diagram does not depict reliable provisional responses or the use of preconditions.

Call Establishment

STEP	INSTRUCTION
1, 2, 3	Upon receiving an initial call request message from IP Party A (not depicted in the call flow diagram), the LSC serving IP Party A sends an INVITE to its assigned Softswitch (Softswitch A). Softswitch A forwards the INVITE across the WAN to the Softswitch B (which is assigned to the LSC serving IP Party B). Softswitch B forwards the INVITE to the LSC serving IP Party B. NOTE: Signaling between the EI serving IP Party A and the LSC serving IP Party A is not depicted. In addition, signaling between the LSC serving IP Party B and the EI serving IP Party B is not depicted.

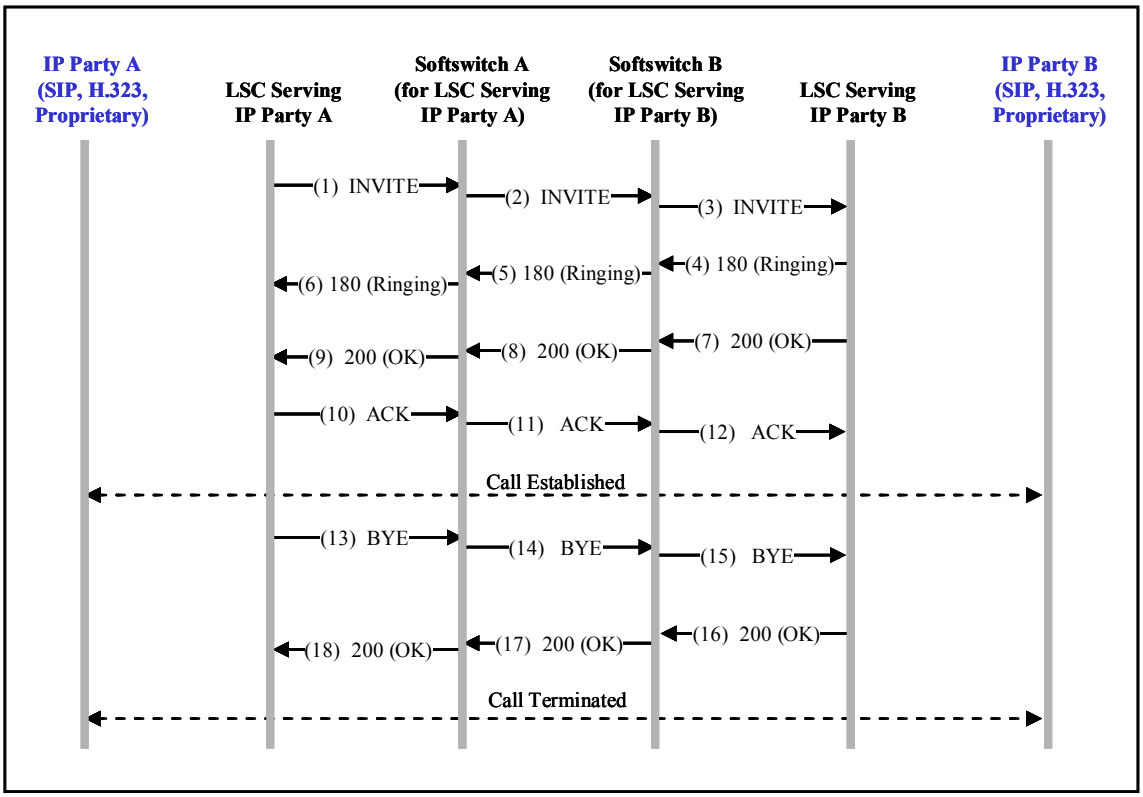


Figure 5.3.4-12. Successful Basic IP-to-IP Call (No Reliable Provisional Responses, No Preconditions)

STEP	INSTRUCTION
4, 5, 6	Assuming the end instrument is not busy, the LSC serving IP Party B sends a 180 (Ringing) to Softswitch B. It forwards the 180 (Ringing) to Softswitch A, which forwards the 180 (Ringing) to the LSC serving IP Party A. NOTE: Signaling between the EI serving IP Party B and the LSC serving IP Party B is not depicted. In addition, signaling between the LSC serving IP Party A and the EI serving IP Party A is not depicted.
7, 8, 9	When IP Party B goes off hook (i.e., answers the call), the LSC serving IP Party B sends a 200 (OK) to Softswitch B. It forwards the 200 (OK) to Softswitch A, which forwards the 200 (OK) to the LSC serving IP Party A. NOTE: Signaling between the EI serving IP Party B and the LSC serving IP Party B is not depicted. In addition, signaling between the LSC serving IP Party A and the EI serving IP Party A is not depicted.

STEP	INSTRUCTION
10, 11, 12	The LSC serving IP Party A sends an ACK to Softswitch A. It forwards the ACK to Softswitch B, which forwards the ACK to the LSC serving IP Party B. NOTE: Signaling between the EI serving IP Party A and the LSC serving IP Party A is not depicted. In addition, signaling between the LSC serving IP Party B and the EI serving IP Party B is not depicted.

Call Release

STEP	INSTRUCTION
13, 14, 15	The LSC serving IP Party A sends a BYE to Softswitch A. It forwards the BYE to Softswitch B, which forwards the BYE to the LSC serving IP Party B. NOTE: Signaling between the EI serving IP Party A and the LSC serving IP Party A that initiated the call release is not depicted. In addition, signaling between the LSC serving IP Party B and the EI serving IP Party B is not depicted.
16, 17, 18	The LSC serving IP Party B sends a 200 (OK) to Softswitch B. It forwards the 200 (OK) to Softswitch A, which forwards the 200 (OK) to the LSC serving IP Party A. NOTE: Signaling between the EI serving IP Party B and the LSC serving IP Party B is not depicted. In addition, signaling between the LSC serving IP Party A and the EI serving IP Party A is not depicted.

5.3.4.13.2.1.2 Reserved.

5.3.4.13.2.1.3 Figure 5.3.4-13, Successful Basic IP-to-IP Call (End-to-End Precondition), depicts the sequence of AS-SIP messages between the AS-SIP signaling appliance serving IP Party A and the AS-SIP signaling appliance serving IP Party B for establishing a telephony session, employing a status-type end-to-end precondition.

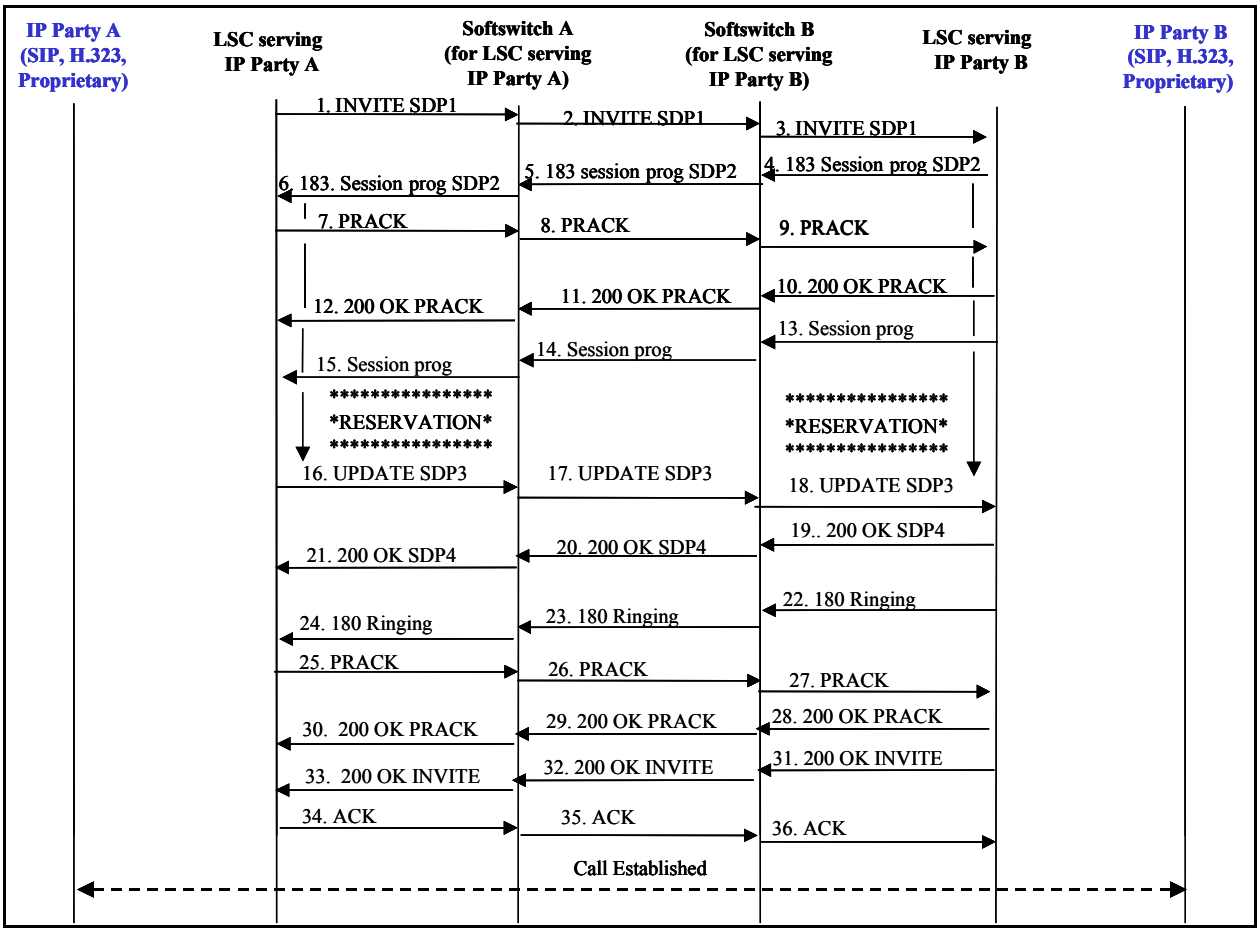


Figure 5.3.4-13. Successful Basic IP-to-IP Call (End-to-End Precondition)

Call Establishment

STEP	INSTRUCTION
1, 2, 3	Upon receiving an initial call request message from IP Party A (not depicted in the call flow diagram), the LSC serving IP Party A sends an INVITE to its assigned Softswitch (Softswitch A). The INVITE contains an end-to-end (e2e) precondition offer using SDP attributes described in RFC 3312. The precondition offer includes, at a minimum, a media ("m=") line, a connection ("c=") line, at least one current-status line, and at least one desired-status line. Softswitch A forwards the INVITE to Softswitch B that is assigned to the LSC serving IP Party B. Softswitch B forwards the INVITE to the LSC serving IP Party B.
4, 5, 6	The LSC serving IP Party B sends a 183 (Session Progress) to Softswitch B with an answer to the e2e precondition offer that includes, at a minimum, a media ("m=") line, a connection ("c=") line, at least one current-status line, at least one desired-status line, and at least one confirm-status line. Softswitch B forwards the 183 (Session Progress) to

STEP	INSTRUCTION
	Softswitch A, which forwards the 183 (Session Progress) to the LSC serving IP Party A. The LSC serving IP Party A and IP Party B attempt to reserve the resources needed to fulfill the preconditions.
7, 8, 9	The LSC serving IP Party A sends a PRACK to Softswitch A. It forwards the PRACK to Softswitch B, which forwards the PRACK to the LSC serving IP Party B.
10, 11, 12	The LSC serving IP Party B sends a 200 (OK) PRACK to Softswitch B. It forwards the 200 (OK) PRACK to Softswitch A, which forwards the 200 (OK) PRACK to the LSC serving IP Party A.
13, 14, 15	The LSC serving IP party B sends a 183 Session Progress with no sdp immediately after sending the 200 OK PRACK in order to notify the originating AS-SIP signaling appliance (LSC serving IP party A) that there is no early media and ring back must be generated locally.
16, 17, 18	When the LSC serving IP Party A receives confirmation that it has met its precondition (e.g., receives an RSVP RESV message), the LSC serving IP Party A sends an UPDATE to Softswitch A with an updated offer reflecting compliance with its part of the precondition. The updated precondition offer includes, at a minimum, a media (“m=”) line, a connection (“c=”) line, at least one current-status line, and at least one desired-status line. Softswitch A forwards the UPDATE to Softswitch B, which forwards the UPDATE to the LSC serving IP Party B.
19, 20, 21	The LSC serving IP Party B receives confirmation that it has met its precondition (e.g., receives RSVP RESV message) and sends a 200 (OK) UPDATE to Softswitch B with an updated precondition answer reflecting compliance with its part of the precondition as well as the most recent updated information from the UPDATE offer. The updated answer includes, at a minimum, a media (“m=”) line, a connection (“c=”) line, at least one current-status line, and at least one desired-status line. Softswitch B forwards the 200 (OK) UPDATE to Softswitch A, which forwards the 200 (OK) UPDATE to the LSC serving IP Party A.
22, 23, 24	The preconditions have been met so the LSC serving IP Party B notifies the IP EI of a pending call and sends a 180 (Ringing) to Softswitch B. It forwards the 180 (Ringing) to Softswitch A, which forwards the 180 (Ringing) to the LSC serving IP Party A. NOTE: Signaling between the LSC serving IP Party B and the IP EI serving IP Party B is not depicted. In addition, signaling between the LSC serving IP Party A and the EI serving Party A is not depicted.
25, 26, 27	The LSC serving IP Party A sends a PRACK to Softswitch A. It forwards the PRACK to Softswitch B, which forwards the PRACK to the LCC serving IP Party B. NOTE: Signaling between the IP EI serving IP Party A and the LSC serving IP Party A is not depicted. In addition, signaling between the LSC serving IP Party B and the EI serving IP Party B is not depicted.

STEP	INSTRUCTION
28, 29, 30	The LSC serving IP Party B sends a 200 (OK) PRACK to Softswitch B. It forwards the 200 (OK) PRACK to Softswitch A, which forwards the 200 (OK) PRACK to the LSC serving IP Party A. NOTE: Signaling between the EI serving IP Party B and the LSC serving IP Party B is not depicted. In addition, signaling between the LSC serving IP Party A and the EI serving IP Party A is not depicted.
31, 32, 33	The LSC serving IP Party B sends a 200 (OK) INVITE to Softswitch B. It forwards the 200 (OK) INVITE to Softswitch A, which forwards the 200 (OK) INVITE to the LSC serving IP Party A. NOTE: Signaling between the IP EI serving IP Party B and the LSC serving IP Party B is not depicted. In addition, signaling between the LSC serving IP Party A and the EI serving IP Party A is not depicted.
34, 35, 36	The LSC serving IP Party A sends an ACK to Softswitch A. It sends the ACK to Softswitch B, which forwards the ACK to the LSC serving IP Party B. NOTE: Signaling between the IP EI serving IP Party A and the LSC serving IP Party A is not depicted. In addition, signaling between the LSC serving IP Party B and the EI serving IP Party B is not depicted.

5.3.4.13.2.1.4 Figure 5.3.4-14, Successful Basic IP-to-IP Call (Segmented Precondition), depicts the sequence of AS-SIP messages between the AS-SIP signaling appliance serving IP Party A and the AS-SIP signaling appliance serving IP Party B for establishing a telephony session, employing a segmented precondition.

Call Establishment

STEP	INSTRUCTION
1, 2, 3	Upon receiving an initial call request message from IP Party A (not depicted in call flow diagram), the LSC serving IP Party A satisfies its local precondition before sending an INVITE to its assigned Softswitch (Softswitch A). The INVITE contains a segmented precondition offer using SDP attributes described in RFC 3312. The precondition offer includes, at a minimum, a media ("m=") line, a connection ("c=") line, at least two current-status lines (local and remote), and at least two desired-status lines (local and remote). Softswitch A forwards the INVITE to Softswitch B (which is assigned to the LSC serving IP Party B). Softswitch B forwards the INVITE to the LSC serving IP Party B.
4, 5, 6	The LSC serving IP party B sends a 183 Session Progress with no sdp prior to sending the 180 ringing with the answer to the segmented precondition offer in order to notify the originating AS-SIP signaling appliance (LSC serving IP party A) that there is no early media and ring back must be generated locally.

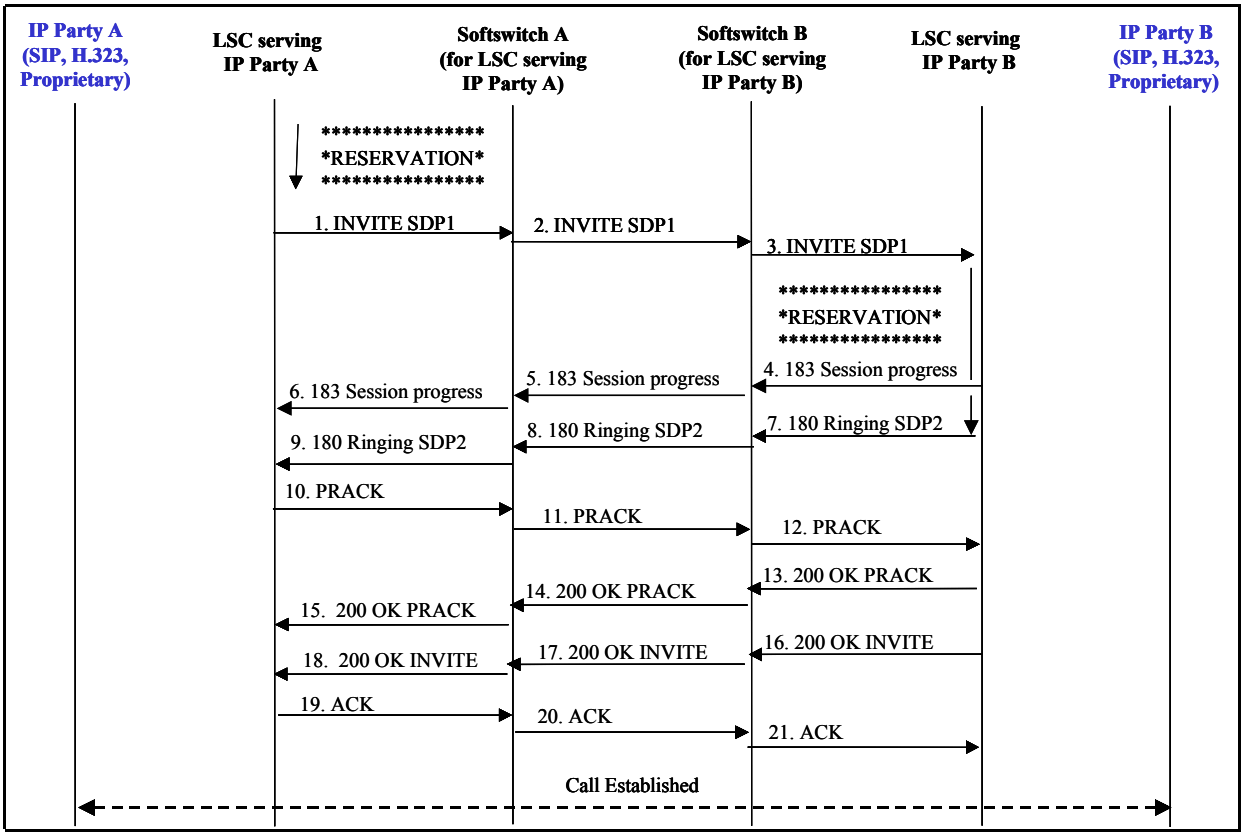


Figure 5.3.4-14. Successful Basic IP-to-IP Call (Segmented Precondition)

STEP	INSTRUCTION
7, 8, 9	The LSC serving IP Party B satisfies its local precondition, notifies the IP end instrument of the pending call, and sends a 180 (Ringing) with an answer to the segmented precondition offer that includes, at a minimum, a media ("m=") line, a connection ("c=") line, at least two current-status lines, and at least two desired-status lines to Softswitch B. Softswitch B forwards the 180 (Ringing) to Softswitch A, which forwards the 180 (Ringing) to the LSC serving IP Party A. NOTE: Signaling between the LSC serving IP Party B and the EI serving IP Party B is not depicted. In addition, signaling between the LSC serving IP Party A and the EI serving Party A is not depicted.
10, 11, 12	The LSC serving IP Party A sends a PRACK to Softswitch A. It forwards the PRACK to Softswitch B, which forwards the PRACK to the LSC serving IP Party B.
13, 14, 15	The LSC serving IP Party B sends a 200 (OK) PRACK response to Softswitch B. It forwards the 200 (OK) PRACK to Softswitch A, which forwards the 200 (OK) PRACK to the LSC serving IP Party A.

STEP	INSTRUCTION
16, 17, 18	The LSC serving IP Party B sends a 200 (OK) INVITE to Softswitch B. It forwards the 200 (OK) INVITE to Softswitch A, which forwards the 200 (OK) INVITE to the LSC serving IP Party A. NOTE: Signaling between the IP EI serving IP Party B and the LSC serving IP Party B is not depicted. In addition, signaling between the LSC serving IP Party A and the EI serving IP Party A is not depicted.
19, 20, 21	The LSC serving IP Party A sends an ACK to Softswitch A. It forwards the ACK to Softswitch B, which forwards the ACK to the LSC serving IP Party B. NOTE: Signaling between the IP EI serving IP Party A and the LSC serving IP Party A is not depicted. In addition, signaling between the LSC serving IP Party B and the EI serving IP Party B is not depicted.

5.3.4.13.3 Call Hold

Party A and Party B are engaged in a conversation. Party A places the call on hold. Later, Party A resumes the call (removes the call from hold).

5.3.4.13.3.1 IP-to-IP Call Type

5.3.4.13.3.1.1 Figure 5.3.4-15, IP-to-IP Call Hold, depicts the sequence of AS-SIP messages between the AS-SIP signaling appliance serving IP Party A and the AS-SIP signaling appliance serving IP Party B that are employed to place the current call on hold and then to resume the call.

Call Hold

STEP	INSTRUCTION
1, 2, 3	In response to a request on the part of IP party A, the LSC serving Party A sends a mid-call INVITE to the assigned Softswitch (Softswitch A). The INVITE includes the attribute line "a=sendonly" or "a=inactive" if the stream had been a sendrecv media stream or "a=inactive" if the stream had been a recvonly stream. Softswitch A forwards the mid-call INVITE to Softswitch B, which is assigned to the LSC serving IP Party B. Softswitch B forwards the mid-call INVITE to the LSC serving IP Party B. NOTE: The SIP UA MAY also support establishing a call hold by sending a mid-call INVITE that includes a session description, which is the same as in the original request, but the "c" destination addresses for the media streams to be put on hold are set to zero: c=IN IP4 0.0.0.0.

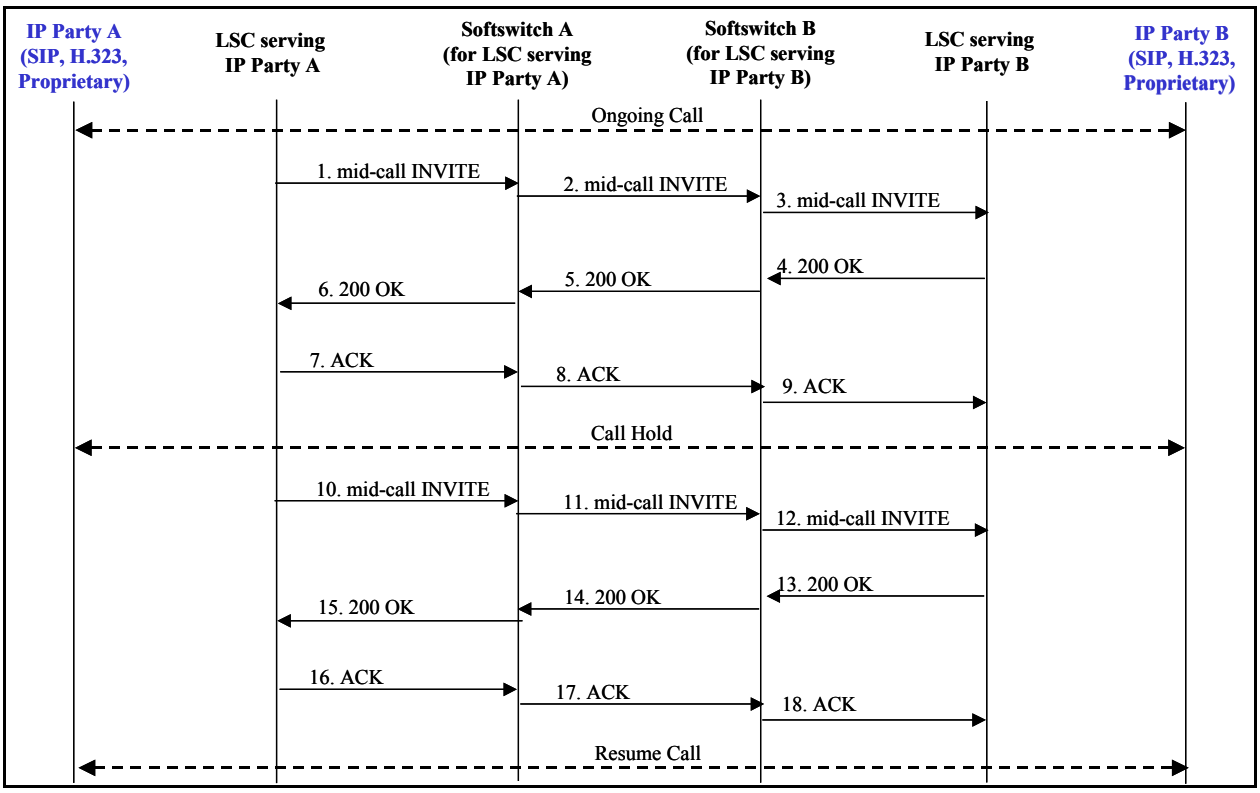


Figure 5.3.4-15. IP-to-IP Call Hold

STEP	INSTRUCTION
	NOTE: Signaling between the EI serving IP Party A and the LSC serving IP Party A is not depicted. In addition, signaling between the LSC serving IP Party B and the EI serving IP Party B and is not depicted.
4, 5, 6	The LSC serving IP Party B sends a 200 (OK) to Softswitch B. It forwards the 200 (OK) to Softswitch A, which forwards the 200 (OK) to the LSC serving IP Party A. NOTE: Signaling between the EI serving IP Party B and the LSC serving IP Party B is not depicted. In addition, signaling between the LSC serving IP Party A and the EI serving IP Party A is not depicted.
7, 8, 9	The LSC serving IP Party A sends an ACK to Softswitch A. It forwards the ACK to Softswitch B, which forwards the ACK to the LSC serving IP Party B. NOTE: Signaling between the LSC serving IP Party B and the EI serving IP Party B is not depicted.

The call is now on hold.

Call Resume

STEP	INSTRUCTION
10, 11, 12	In response to a request on the part of IP Party A, the LSC serving Party A sends a mid-call re-INVITE to Softswitch A. It forwards the mid-call re-INVITE to Softswitch B, which forwards the mid-call re-INVITE to the LSC serving IP Party B. The re-INVITE includes the attribute line "a=sendrecv" if the stream had originally been a sendrecv media stream or "a=recvonly" if the stream had been a recvonly stream. NOTE: In the case of a call hold established by setting the "c" destination address to 0.0.0.0, another re-INVITE with the original address parameter terminates the call hold. NOTE: Signaling between the EI serving IP Party A and the LSC serving IP Party A is not depicted. In addition, signaling between the LSC serving IP Party B and the EI serving IP Party B and is not depicted.
13, 14, 15	The LSC serving IP Party B sends a 200 (OK) to Softswitch B. It forwards the 200 (OK) to Softswitch A, which forwards the 200 (OK) to the LSC serving IP Party A. NOTE: Signaling between the EI serving IP Party B and the LSC serving IP Party B is not depicted. In addition, signaling between the LSC serving IP Party A and the EI serving IP Party A is not depicted.
16, 17, 18	The LSC serving IP Party A sends an ACK to Softswitch A. It forwards the ACK to Softswitch B, which forwards the ACK to the LSC serving IP Party B NOTE: Signaling between the EI serving IP Party A and the LSC serving IP Party A is not depicted. In addition, signaling between the LSC serving IP Party B and the EI serving IP Party B is not depicted.

The call is now resumed.

Figure 5.3.4-16, SIP-SIP Call Hold (End-to-End SIP Signaling) (for Illustrative Purposes), at the end of this section, offers an illustrative example of the end-to-end call signaling to the end instruments assuming the end instruments are both standard SIP end instruments.

5.3.4.13.4 Call Waiting

Party A and Party B are engaged in a conversation. Call waiting consists of one party placing the other party on hold while either accepting or resuming a call with a third party.

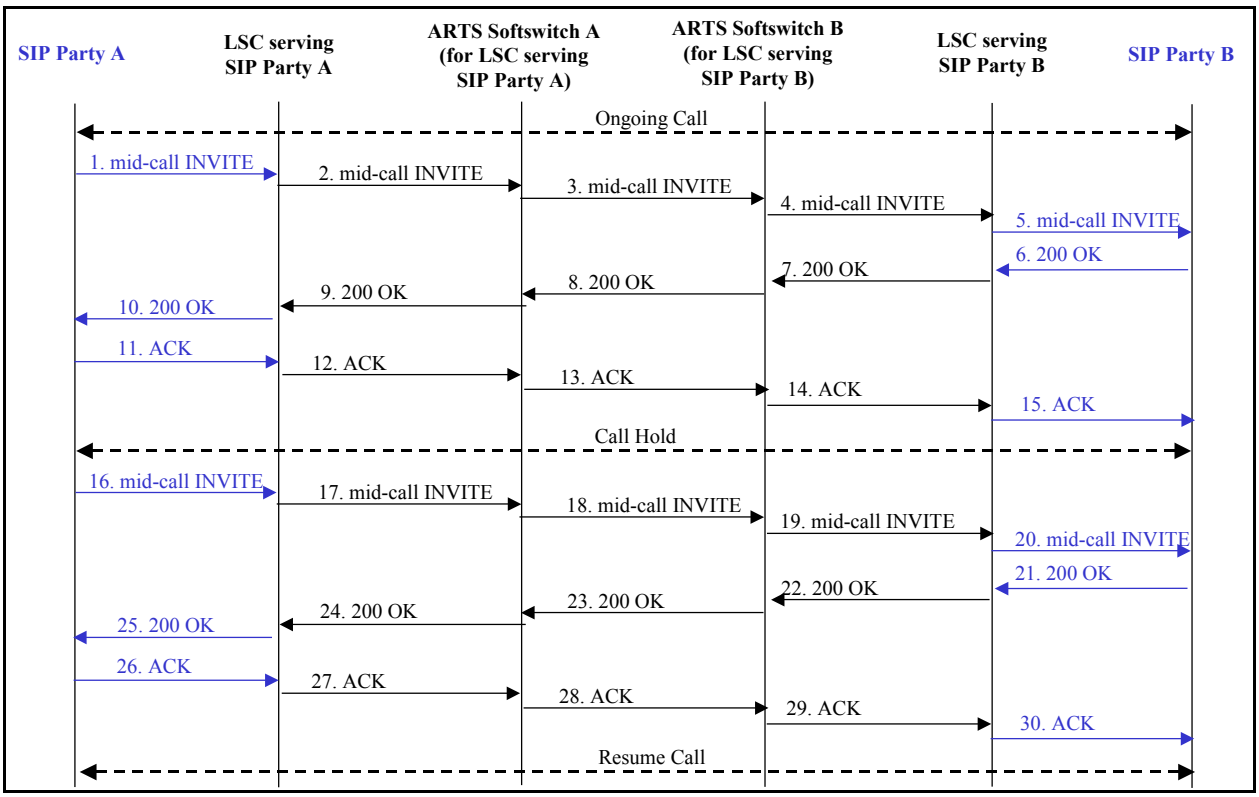


Figure 5.3.4-16. SIP-SIP Call Hold (End-to-End SIP Signaling) (For Illustrative Purposes)

5.3.4.13.4.1 IP-to-IP Call Type

5.3.4.13.4.1.1 Figure 5.3.4-17, IP-to-IP Call Waiting, depicts the sequence of AS-SIP messages between the AS-SIP signaling appliance serving IP Party A and the AS-SIP signaling appliance serving IP Party B that are employed to place the current call on hold in order to accept a call from a third Party C, and to terminate the call with the third Party C in order to resume the original call.

Due to real estate constraints, the Softswitches have been omitted deliberately from the call flow diagram.

NOTE: There are other variations of call waiting, such as placing the current call on hold, answering a call from a third Party C, placing the call with the third Party C on hold, resuming the original call, and terminating the original call and resuming the call with the third Party C. However, the basic elements of call waiting involve the serial implementation of call hold and call resume as portrayed in Figure 5.3.4-17.

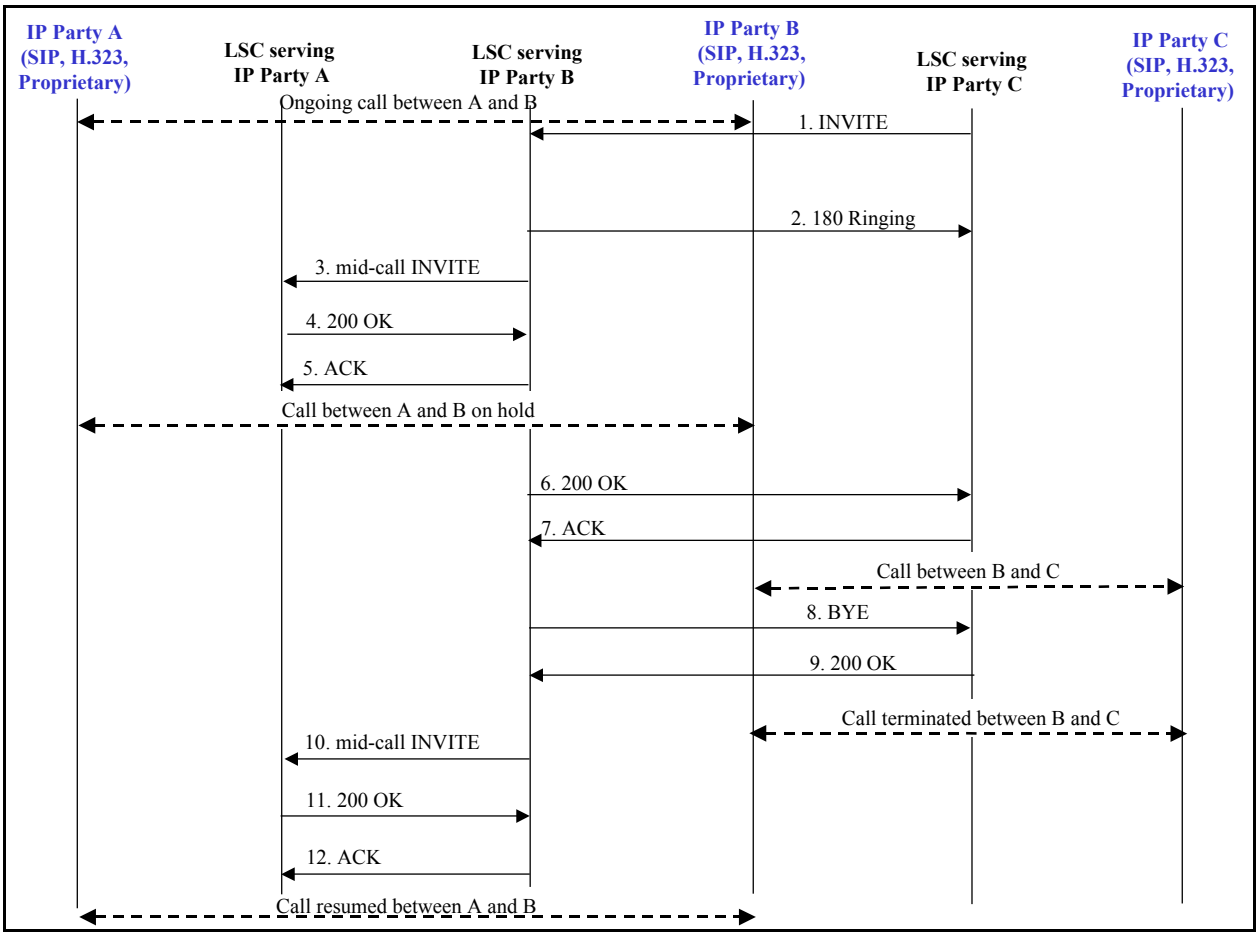


Figure 5.3.4-17. IP-to-IP Call Waiting

STEP	INSTRUCTION
1	Upon receiving an initial call request message from IP Party C (not depicted in call flow diagram), the LSC serving IP Party C sends an INVITE to the LSC serving IP Party B. NOTE: Signaling between the EI serving IP Party C and the LSC serving IP Party C is not depicted. In addition, signaling between the LSC serving IP Party B and the end instrument serving party B is not depicted.
2	The LSC serving IP Party B instructs the end instrument for IP Party B to alert the user of an incoming call request (i.e., call waiting tone) and sends a 180 (Ringing) to the LSC serving IP Party C. NOTE: Signaling between the LSC serving IP Party B and the EI serving IP Party B is not depicted. In addition, signaling between the LSC serving IP Party C and the end instrument serving Party C is not depicted.

STEP	INSTRUCTION
3	In response to a request on the part of IP Party B, the LSC serving IP Party B sends a mid-call INVITE to the LSC serving IP Party A with the attribute line "a=sendonly" or "a=inactive" if the stream had been a sendrecv media stream or "a=inactive" if the stream had been a recvonly stream (i.e., Party B initiates a call hold with Party A). NOTE: Party B MAY also support establishing a call hold by sending a mid-call INVITE that includes a session description that is the same as in the original request, but the "c" destination addresses for the media streams to be put on hold are set to zero: c=IN IP4 0.0.0.0. NOTE: Signaling between the EI serving IP Party B and the LSC serving IP Party B is not depicted. In addition, signaling between the LSC serving IP Party A and the EI serving IP Party A is not depicted.
4	The LSC serving IP Party A sends a 200 (OK) to the LSC serving IP Party B. NOTE: Signaling between the EI serving IP Party A and the LSC serving IP Party A is not depicted. In addition, signaling between the LSC serving IP Party B and the EI serving IP Party B is not depicted.
5	The LSC serving IP Party B sends an ACK to the LSC serving IP Party A. NOTE: Signaling between the EI serving IP Party B and the LSC serving IP Party B is not depicted. In addition, signaling between the LSC serving IP Party A and the EI serving IP Party A is not depicted.

The call between IP Party B and IP Party A is now on hold.

STEP	INSTRUCTION
6	The LSC for IP Party B sends a 200 (OK) to the LSC for IP Party C. NOTE: Signaling between the EI serving IP Party B and the LSC serving IP Party B is not depicted. In addition, signaling between the LSC serving IP Party C and the EI serving IP Party C is not depicted.
7	The LSC for IP Party C sends an ACK to the LSC for IP Party B. NOTE: Signaling between the EI serving IP Party C and the LSC serving IP Party C is not depicted. In addition, signaling between the LSC serving IP Party B and the EI serving IP Party B is not depicted.

The call between IP Party C and IP Party B is now established.

STEP	INSTRUCTION
8	When IP Party B terminates the session with IP Party C, then the LSC serving IP Party B sends a BYE to the LSC serving IP Party C. NOTE: Signaling between the EI serving IP Party B and the LSC serving IP Party B that initiated the call release is not depicted. In addition, signaling between the LSC serving IP Party C and the EI serving IP Party C is not depicted.
9	The LSC serving IP Party C sends a 200 (OK) to the LSC serving IP Party B. NOTE: Signaling between the EI serving IP Party C and the LSC serving IP Party C is not depicted. In addition, ignaling between the LSC serving IP Party B and the EI serving IP Party B is not depicted.

The call between IP Party C and IP Party B is now terminated.

STEP	INSTRUCTION
10	The LSC serving IP Party B sends a mid-call re-INVITE to the LSC for IP Party A that includes the attribute line "a=sendrecv" if the stream had originally been a sendrecv media stream or "a=recvonly" if the stream had been a recvonly stream. NOTE: In the case of a call hold established by setting the "c" destination address to 0.0.0.0, another re-INVITE with the original address parameter terminates the call hold. NOTE: Signaling between the EI serving IP Party B and the LSC serving IP Party B is not depicted. In addition, signaling between the LSC serving IP Party A and the EI serving IP Party A and is not depicted.
11	The LSC serving IP Party A sends a 200 (OK) to the LSC serving IP Party B. NOTE: Signaling between the EI serving IP Party A and the LSC serving IP Party A is not depicted. In addition, signaling between the LSC serving IP Party B and the EI serving IP Party B is not depicted.
12	The LSC serving IP Party B sends an ACK to the LSC serving IP Party A. NOTE: Signaling between the EI serving IP Party B and the LSC serving IP Party B is not depicted. In addition, signaling between the LSC serving IP Party A and the EI serving IP Party A and is not depicted.

The call between IP Party A and IP Party B is now resumed.

Figure 5.3.4-18, SIP-SIP Call Waiting (End-to-End SIP Signaling) (For Illustrative Purposes), at the end of this section, offers an illustrative example of the end-to-end call signaling to the end instruments assuming the end instruments are both standard SIP end instruments.

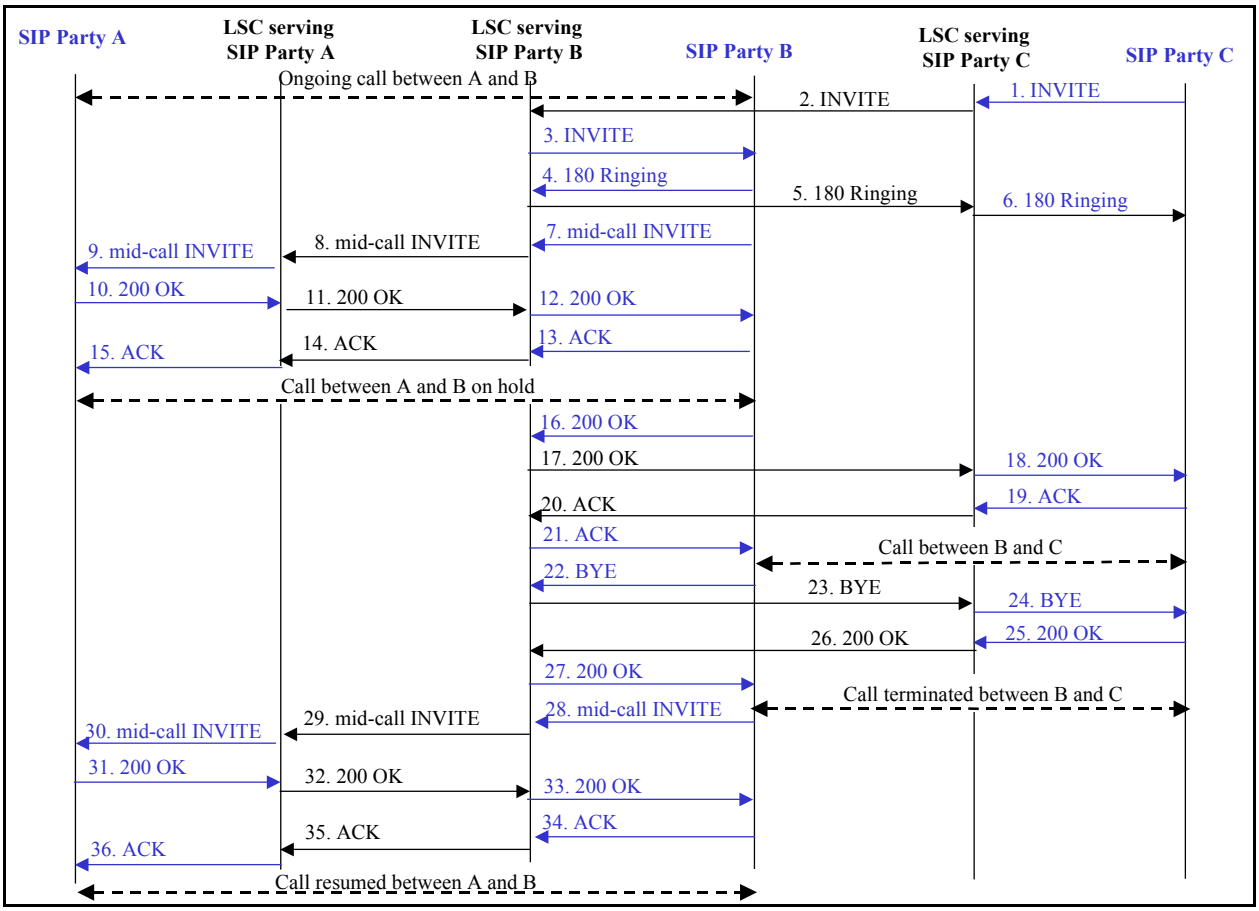


Figure 5.3.4-18. SIP-SIP Call Waiting (End-to-End SIP Signaling) (For Illustrative Purposes)

5.3.4.13.5 Call Forward (Unconditional)

A user instructs that call requests to a particular phone number be routed to a different predefined phone number. In the following call flow diagrams, user B has instructed that call requests addressed to B's phone number at location 1 be rerouted to a different phone number for an end instrument at location 2.

NOTE: It is important to note that when the LSC forwards an inbound call to a forwarded-to party the LSC remains in the call signaling path. When the forwarded-to party is located at an external enclave reached over the DISN WAN then the LSC allocates (2) call counts from the

call count budget for the duration of the call even though no bearer traffic related to the given call actually transits the access link to the enclave at which the LSC is located.

5.3.4.13.5.1 IP-to-IP Call Type

5.3.4.13.5.1.1 Figure 5.3.4-19, IP-to-IP Call Forward (Unconditional), depicts the sequence of AS-SIP messages involved in the unconditional forwarding of a call request intended for IP Party B at location 1 to a forwarded phone number (SIP URI) corresponding to an IP end instrument at location 2.

Due to real estate constraints, the Softswitches assigned to the LSC serving IP Party A, IP Party B at location 1, and IP Party B at location 2 have been deliberately omitted from the call flow diagram.

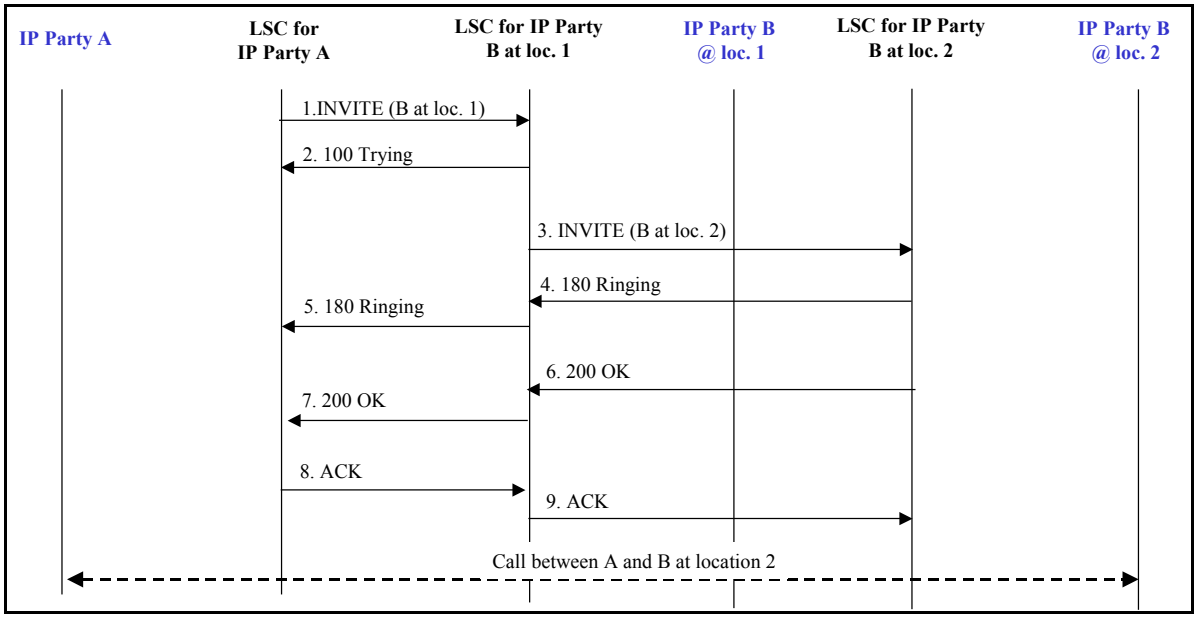


Figure 5.3.4-19. IP-to-IP Call Forward (Unconditional)

Call Forward

STEP	INSTRUCTION
1	The LSC serving IP Party A sends an INVITE to the LSC serving IP Party B at location 1. NOTE: Signaling between the IP EI serving IP Party A and the LSC serving IP Party A is not depicted.

STEP	INSTRUCTION
2	The LSC serving IP Party B at location 1 sends a 100 Trying to the LSC serving IP Party A. NOTE: Signaling between the LSC serving IP Party A and party A's IP end instrument is not depicted.
3	Background: User B has instructed the LSC previously that all calls intended for the phone number (SIP URI) associated with user B at location 1 be forwarded temporarily to another number (SIP URI) corresponding to an end instrument at location 2. The LSC serving IP Party B at location 1 rewrites the Request URI and sends the INVITE to the LSC serving IP Party B at location 2.
4, 5	The LSC serving IP Party B at location 2 sends a 180 (Ringing) to the LSC serving IP Party B at location 1, which forwards the 180 (Ringing) to the LSC serving IP Party A. NOTE: Signaling between the IP EI serving IP Party B at location 2 and the LSC serving IP Party B at location 2 is not depicted. In addition, signaling between the LSC serving IP Party A and the IP EI serving IP Party A is not depicted.
6, 7	The LSC serving IP Party B at location 2 sends a 200 (OK) to the LSC serving IP Party B at location 1, which forwards the 200 (OK) to the LSC serving IP Party A. NOTE: Signaling between the IP EI serving IP Party B at location 2 and the LSC serving IP Party B at location 2 is not depicted. In addition, signaling between the LSC serving IP Party A and the IP EI serving IP Party A is not depicted.
8, 9	The LSC serving IP Party A sends an ACK to the LSC serving IP Party B at location 1, which forwards the ACK to the LSC serving IP Party B at location 2. NOTE: Signaling between the IP EI serving IP Party A and the LSC serving IP Party A is not depicted. In addition, signaling between the LSC serving IP Party B at location 2 and the IP EI serving IP Party B at location 2 is not depicted.

The forwarded call is now established between IP Party A and IP Party B at location 2.

Figure 5.3.4-20, SIP-SIP Call Forward (Unconditional) (End-to-End SIP Signaling Depicted for Illustrative Purposes Only), offers an illustrative example of the end-to-end call signaling for the SIP-SIP call forwarding case assuming the IP end instruments are SIP end instruments.

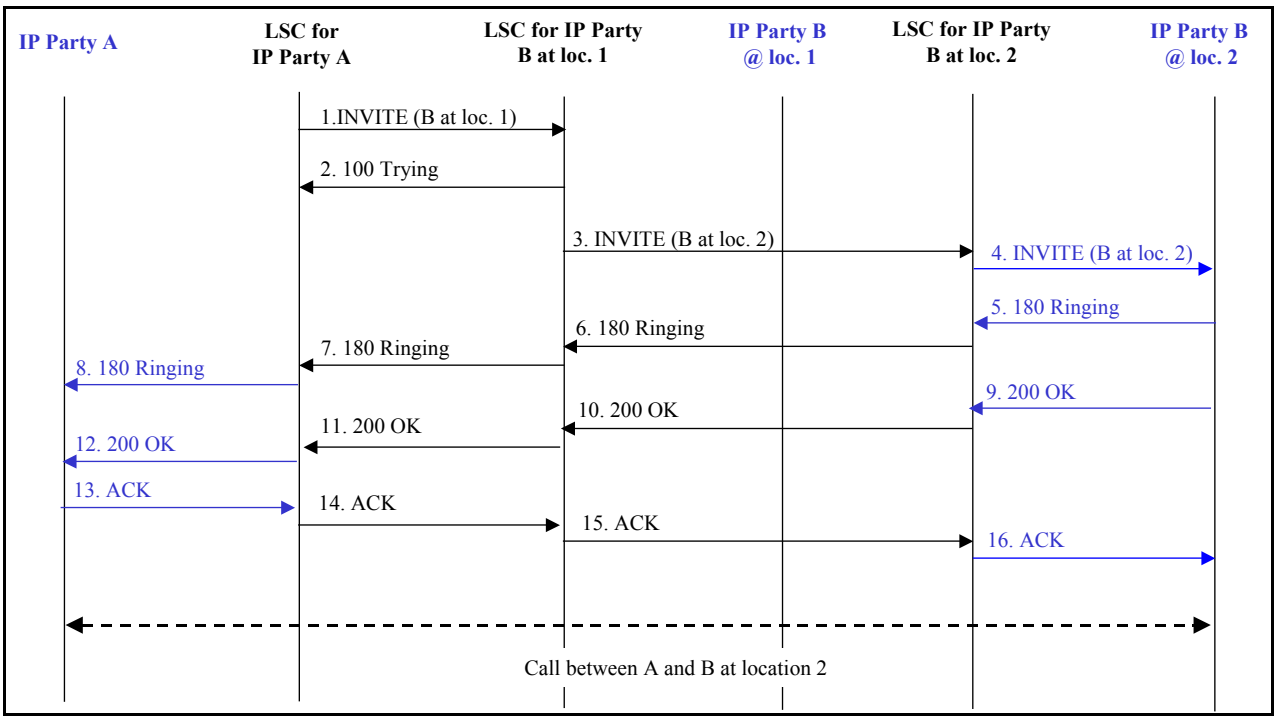


Figure 5.3.4-20. SIP-SIP Call Forward (Unconditional)
(End-to-End SIP Signaling Depicted for Illustrative Purposes Only)

5.3.4.13.6 Call Forward (No Answer)

A user instructs that call requests to a particular phone number be routed to a different predefined phone number in the event the call is not answered within some number of rings (No Answer). In the following call flow diagrams, user B has instructed that call requests addressed to B's phone number at location 1, which receive no reply, be rerouted to a different phone number for an end instrument at location 2.

As specified in Section 5.3.4.7.6, SIP URI and Mapping of Telephony Number into SIP URI, the addressing format for the SIP messages MUST be a SIP URI having a userinfo part that either is a number from the DSN worldwide numbering plan with the appropriate phone-context descriptor or an E.164 encoded phone number and having a 'user=phone' field appended to the URI.

NOTE: It is important to note that when the LSC forwards an inbound call to a forwarded-to party the LSC remains in the call signaling path. When the forwarded-to party is located at an external enclave reached over the DISN WAN then the LSC allocates (2) call counts from the call count budget for the duration of the call even though no bearer traffic related to the given call actually transits the access link to the enclave at which the LSC is located.

5.3.4.13.6.1 IP-to-IP Call Type

5.3.4.13.6.1.1 Figure 5.3.4-21, IP-to-IP Call Forwarding on No Answer, depicts the sequence of AS-SIP messages involved in the forwarding of an unanswered call request intended for IP Party B at location 1 to a forwarded phone number (SIP URI) corresponding to an IP end instrument at location 2.

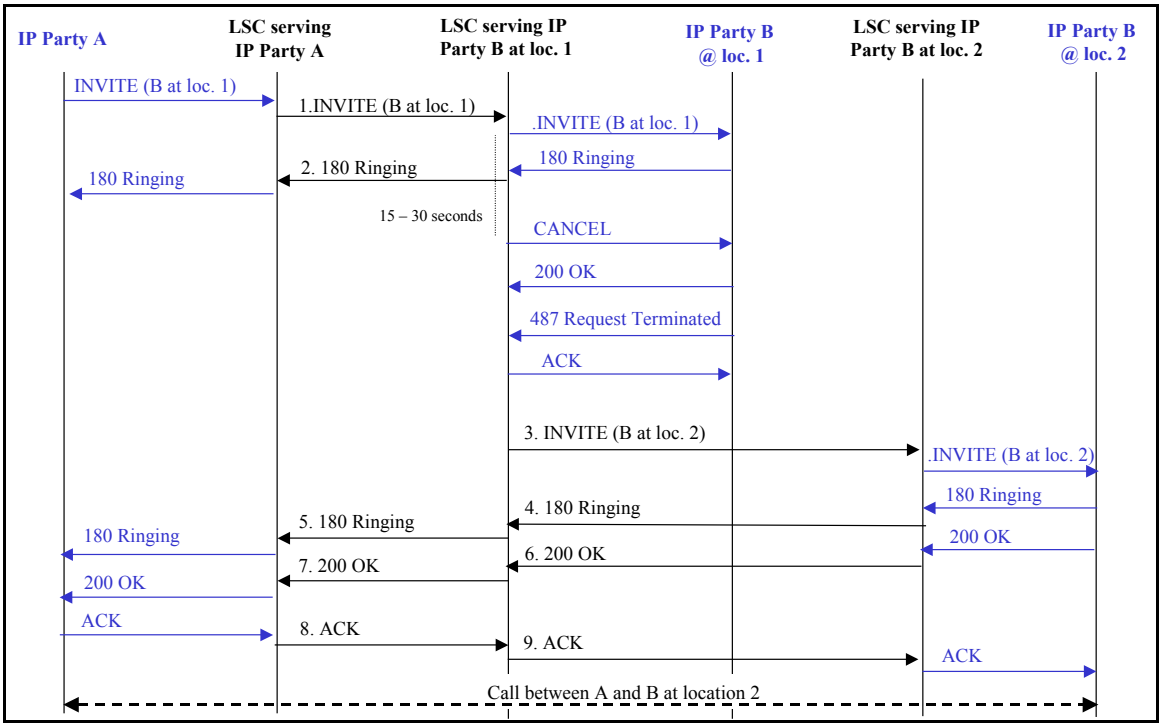


Figure 5.3.4-21. IP-to-IP Call Forwarding on No Answer

Due to real estate constraints, the Softswitches assigned to the LSC serving IP Party A, IP Party B at location 1, and IP Party B at location 2 have been omitted deliberately from the call flow diagram.

NOTE: The call flow diagram is based on Section 2.9 of draft-ietf-sipping-services-examples. The 100 Trying messages have been omitted.

NOTE : In order to clearly convey the call flow in this scenario, we have depicted SIP end instruments and indicated the SIP signaling between the LSC and SIP end instruments. In the case of H.323 and proprietary IP end points, comparable functionality must be provided in the signaling between the LSCs and their served IP end points

Call Forward (No Answer)

STEP	INSTRUCTION
1	IP Party A (a SIP end instrument) sends an INVITE to the LSC serving IP Party A The LSC serving IP Party A sends an INVITE to the LSC serving IP Party B at location 1. (The INVITE is ultimately intended for IP Party B at location 1.) User B has previously instructed the LSC serving IP Party B at location 1 that in the event of a no reply, the call is to be forwarded to another number (SIP URI) corresponding to an end instrument at location 2. The LSC will notify the IP end instrument of the pending call request, and if there is no answer within a predefined period, then the LSC serving IP Party B at location 1 will rewrite the Request URI and send it to the LSC serving IP Party B at location 2. The LSC serving IP Party B at location 1 sends the INVITE to IP Party B at location 1 (which is a SIP end instrument).
2	IP Party B at location 1 sends a 180 (Ringing) to the LSC serving IP Party B at location 1. The LSC serving IP Party B at location 1 forwards the 180 (Ringing) to the LSC serving IP Party A. The LSC serving IP Party A forwards the 180 (Ringing) to IP Party A.
3	When there is no answer within a configurable amount of time, the request times out. The LSC serving IP Party B at location 1 sends a CANCEL request to IP Party B at location 1. IP Party B at location 1 responds with a 200 (OK) to the CANCEL and a 487 (Request Terminated) to the INVITE. The LSC serving IP Party B at location 1 sends an ACK for the 487 (Request Terminated).* The LSC serving IP Party B at location 1 rewrites the Request URI and sends the INVITE to the LSC serving IP Party B at location 2. The LSC serving IP Party B at location 2 forwards the INVITE to IP Party B at location 2 (which is a SIP end instrument).
4, 5	IP Party B at location 2 sends a 180 (Ringing) to the LSC serving IP Party B at location 2. The LSC serving IP Party B at location 2 sends the 180 (Ringing) to the LSC serving IP Party B at location 1. The LSC serving IP Party B at location 1 sends the 180 (Ringing) to the LSC serving IP Party A. The LSC serving IP Party A sends the 180 (Ringing) to IP Party A.

STEP	INSTRUCTION
6, 7	IP Party B at location 2 goes off-hook and the SIP end instrument sends 200 (OK) to the LSC serving IP Party B at location 2. The LSC serving IP Party B at location 2 sends the INVITE to the LSC serving IP Party B at location 1. The LSC serving IP Party B at location 1 sends the 180 (Ringing) to the LSC serving IP Party A. The LSC serving IP Party A sends 200 (OK) to IP Party A.
8, 9	IP Party A sends an ACK to the LSC serving IP Party A The LSC serving IP Party A sends the ACK to the LSC serving IP Party B at location 1, which sends the ACK to the LSC serving IP Party B at location 2. The LSC serving IP Party B at location 2 sends the ACK to IP Party B at location 2.
*RFC 2543 compliant IP end instruments will not send a 487 (Request Terminated) to the INVITE.	

The forwarded call is now established between IP Party A and IP Party B at location 2.

5.3.4.13.7 Call Forward (Busy)

A user instructs that call requests to a particular phone number be routed to a different predefined phone number in the event the end instrument is busy with another call. In the following call flow diagrams, user B has instructed that when a call request is addressed to user B's phone at location 1 but the phone is currently busy with another call, then the new call request is to be forwarded to an end instrument at location 2.

Recalling Requirement 5.3.4.10.2.5.5, the new call request will be forwarded only if the existing call either has an equal or higher precedence level than the incoming call request. If the existing call has a lower precedence than the incoming call request, then the existing call will be preempted in favor of the new call request.

NOTE: It is important to note that when the LSC forwards an inbound call to a forwarded-to party the LSC remains in the call signaling path. When the forwarded-to party is located at an external enclave reached over the DISN WAN then the LSC allocates (2) call counts from the call count budget for the duration of the call even though no bearer traffic related to the given call actually transits the access link to the enclave at which the LSC is located.

5.3.4.13.7.1 IP-to-IP Call Type

5.3.4.13.7.1.1 Figure 5.3.4-22, IP-to-IP Call Forwarding Busy, depicts the sequence of AS-SIP messages involved in the forwarding of a call request intended for IP Party B at location 1. However, the end instrument for IP Party B at location 1 is currently busy with a call of equal or higher precedence than the incoming call request, so the call request is forwarded to another phone number (SIP URI) corresponding to an IP end instrument at location 2.

Due to real estate constraints, the Softswitches assigned to the LSC serving IP Party A, IP Party B at location 1, and IP Party B at location 2 have been omitted deliberately from the call flow diagram.

NOTE: The call flow diagram is based on Section 2.8 of draft-ietf-sipping-services-examples. The 100 Trying messages have been omitted.

NOTE: In order to clearly convey the call flow in this scenario, we have depicted SIP end instruments and indicated the SIP signaling between the LSC and SIP end instruments. In the case of H.323 and proprietary IP end points, comparable functionality must be provided in the signaling between the LSCs and their served IP end points

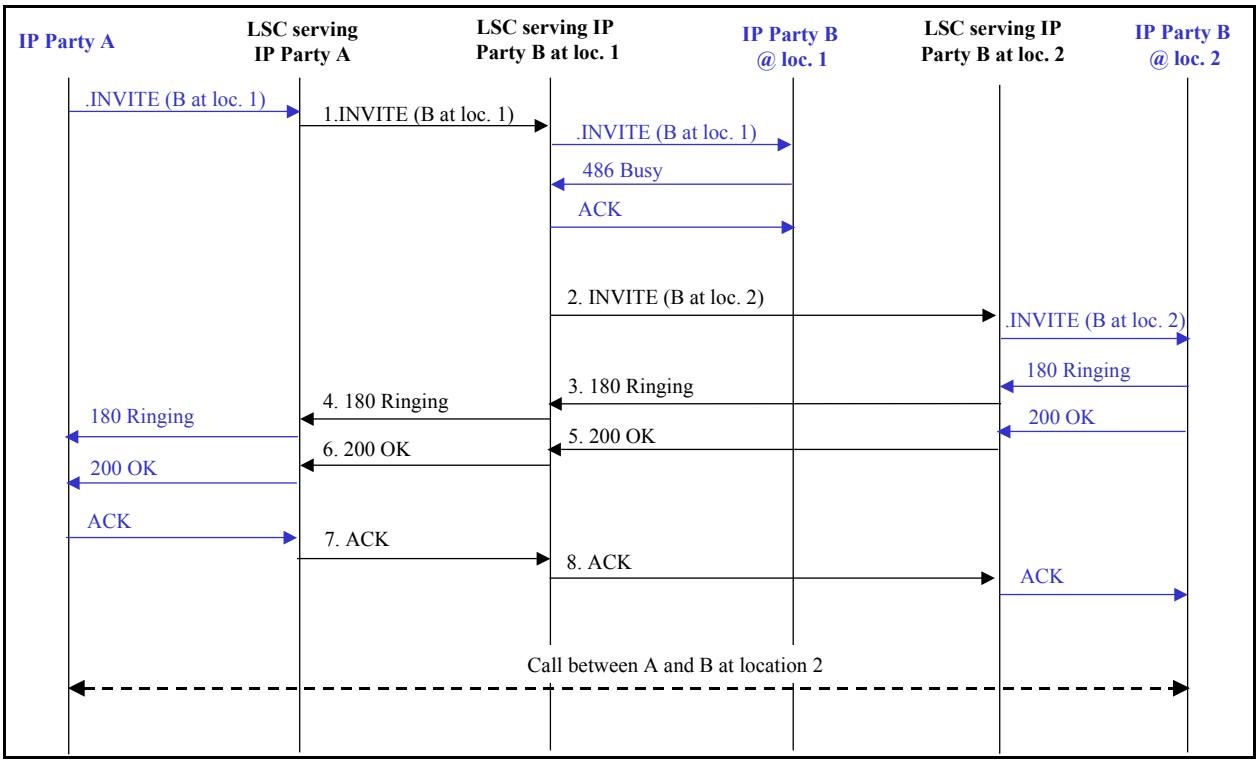


Figure 5.3.4-22. IP-to-IP Call Forwarding Busy

STEP	INSTRUCTION
1	IP Party A (a SIP end instrument) sends an INVITE to the LSC serving IP Party A The LSC serving IP Party A sends an INVITE to the LSC serving IP Party B at location 1. (The INVITE is ultimately intended for IP Party B at location 1.) User B has previously instructed the LSC serving IP Party B at location 1 that in the event the end instrument for IP Party B at location 1 is busy, the call is to be forwarded to another number (SIP URI) corresponding to an end instrument at location 2. The LSC serving IP Party B at location 1 sends the INVITE to IP Party B at location 1 (which is a SIP end instrument).
2	IP Party B at location 1 sends a 486 (Busy) to the LSC serving IP Party B at location 1. The LSC serving IP Party B at location 1 responds with an ACK to IP Party B at location 1. The LSC serving IP Party B at location 1 rewrites the Request URI and sends the INVITE to the LSC serving IP Party B at location 2. The LSC serving IP Party B at location 2 forwards the INVITE to IP Party B at location 2, which is a SIP end instrument.
3, 4	IP Party B at location 2 sends a 180 (Ringing) to the LSC serving IP Party B at location 2. The LSC serving IP Party B at location 2 sends the 180 (Ringing) to the LSC serving IP Party B at location 1. The LSC serving IP Party B at location 1 sends the 180 (Ringing) to the LSC serving IP Party A. The LSC serving IP Party A sends the 180 (Ringing) to IP party A.
5, 6	IP Party B at location 2 goes off-hook and sends a 200 (OK) to the LSC serving IP Party B at location 2. The LSC serving IP Party B at location 2 sends the INVITE to the LSC serving IP Party B at location 1. The LSC serving IP Party B at location 1 sends the 180 (Ringing) to the LSC serving IP Party A. The LSC serving IP Party A sends a 200 (OK) to IP Party A.
7, 8	IP Party A sends an ACK to the LSC serving IP Party A. The LSC serving IP Party A sends the ACK to the LSC serving IP Party B at location 1, which sends the ACK to the LSC serving IP Party B at location 2. The LSC serving IP Party B at location 2 sends the ACK to IP Party B at location 2.

The forwarded call is now established between IP Party A and IP Party B at location 2.

5.3.4.13.8 Call Transfer

There are three actors in a given transfer event, each playing one of the following roles:

- Transferee – the party being transferred to the Transfer Target
- Transferor – the party initiating the transfer
- Transfer Target – the new party being introduced into a call with the Transferee

The call transfer feature enables the call transferor, who has two calls (one with transferee and one with transfer target), to create either a direct signaling and bearer path between the transferee and the transfer target, or just a direct bearer path between the transferee and transfer target depending on the call flow used to implement the call transfer.

5.3.4.13.8.1 Call Transfer Modes

Call transfer can be operated in two different modes: unattended (blind) and attended (consultation transfer). Blind call transfer will forward the transferee to the new destination without talking to the transfer target. The alternative to this type of Call Transfer would be "Consultation Transfer," where the call transferor will have a chance to talk to the transfer target before making the transfer.

5.3.4.13.8.2 Unattended Transfer – Call Transferor: SIP

Two methods have been approved for conducting the unattended call transfer:

1. Method 1 removes the transferor LSC from the SIP signaling path and removes the EI from the signaling and bearer paths. (It is assumed that under normal circumstances the LSC is never in the bearer path.) The Transferor LSC employs the REFER request to provide the transferee with the contact information of the Transfer Target and to instruct the Transferee to initiate a session with the Transfer Target. The call flow is depicted in Figure 5.3.4-23, Unattended Call Transfer for IP EIs (REFER Method).

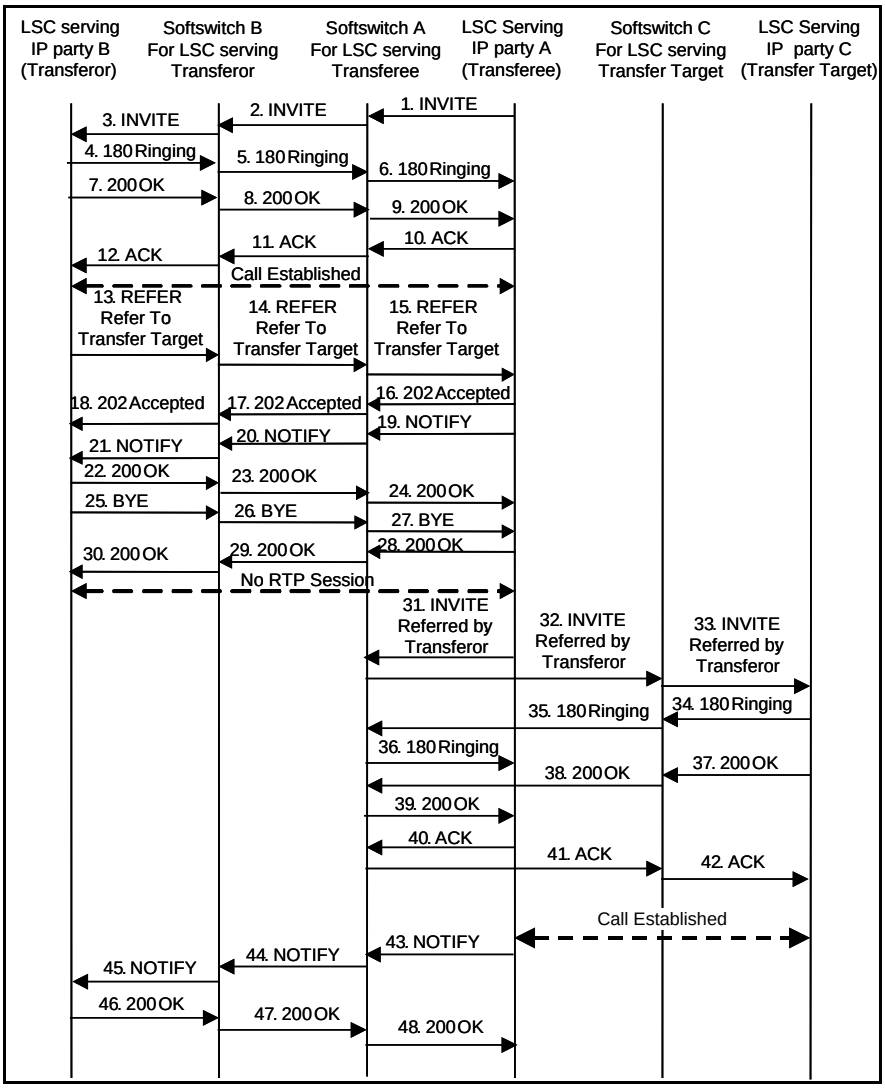


Figure 5.3.4-23. Unattended Call Transfer for IP EIs (REFER Method)

STEP	INSTRUCTION
1, 2, 3	Upon receiving an initial call request message from IP Party A (Transferee) (not depicted in the call flow diagram), the LSC serving IP Party A sends an INVITE to its assigned Softswitch (Softswitch A). Softswitch A forwards the INVITE to the Softswitch for the LSC serving IP Party B (Transferor) (Softswitch B). Softswitch B forwards the INVITE to the LSC serving IP Party B (Transferor). NOTE: Signaling between the EI serving IP Party A (Transferee) and the LSC serving IP Party A (Transferee) is not depicted. In addition, signaling between the LSC serving IP Party B (Transferor) and the EI serving IP Party B (Transferor) is not depicted.

STEP	INSTRUCTION
4, 5, 6	The LSC serving IP Party B (Transferor) sends a 180 (Ringing) to Softswitch B. Softswitch B forwards the 180 (Ringing) to Softswitch A, which forwards the 180 (Ringing) to the LSC serving IP Party A (Transferee). NOTE: Signaling between the Transferor's IP end instrument and the LSC serving Transferor is not depicted. In addition, signaling between the Transferee and the Transferee's IP end instrument is not depicted.
7, 8, 9	When IP Party B (Transferor) goes off hook (i.e., answers the call), the LSC serving IP Party B sends a 200 (OK) to Softswitch B. Softswitch B forwards the 200 (OK) to Softswitch A, which forwards the 200 (OK) to the LSC serving IP Party A (Transferee). NOTE: Signaling between the Transferor's IP end instrument and the LSC serving the Transferor is not depicted. In addition, signaling between the LSC serving the Transferee and the Transferee's IP end instrument is not depicted.
10, 11, 12	The LSC serving IP Party A (Transferee) sends an ACK to Softswitch A. Softswitch A forwards the ACK to Softswitch B, which forwards the ACK to the LSC serving IP Party B (Transferor). NOTE: Signaling between the EI serving IP Party A (Transferee) and the LSC serving IP Party A (Transferee) is not depicted. In addition, signaling between the LSC serving IP Party B (Transferor) and the EI serving IP Party B (Transferor) is not depicted.
13, 14, 15	The Transferor (IP Party B) wishes to transfer the call to a third party, the Transfer Target (IP Party C), and instructs the IP end instrument to initiate a request for a call transfer to the Transfer Target. In the case of a SIP end instrument, the message takes the form of a REFER request. In the case of an H.323 or proprietary IP end instrument, the LSC serving the Transferor MUST create the REFER request when the Transferor signals an intent to transfer the call. The LSC serving the Transferor sends the REFER request to Softswitch B. The REFER request includes a 'Refer-To' header with the SIP URI of the Transfer Target (IP Party C). The REFER request also MAY include the 'Referred-By' header that contains the SIP URI of the Transferor. Softswitch B forwards the REFER request to Softswitch A, which forwards the REFER request to the LSC serving IP Party A (Transferee). NOTE: Signaling between the Transferor's IP end instrument and the LSC serving the Transferor is not depicted. In addition, signaling between the LSC serving the Transferee and the Transferee's IP end instrument is not depicted.
16, 17, 18	The LSC serving the Transferee responds to the REFER request with a 202 (Accepted) that it sends to Softswitch A. Softswitch A forwards the 202 (Accepted) to Softswitch B. Softswitch B forwards the 202 (Accepted) to the LSC serving the Transferor.

STEP	INSTRUCTION
	NOTE: Signaling between the Transferee's IP end instrument and the LSC serving the Transferee is not depicted. In addition, signaling between the LSC serving the Transferor and the Transferor's IP end instrument is not depicted.
19, 20, 21	The LSC serving the Transferee creates (or forwards*) a NOTIFY with a body having the SIP response status line: SIP/2.0 100 Trying. The LSC serving the Transferee sends the NOTIFY to Softswitch B. Softswitch B forwards the NOTIFY to Softswitch A. Softswitch A forwards the NOTIFY to the LSC serving the Transferor. NOTE: Signaling between the Transferee's IP end instrument and the LSC serving the Transferee is not depicted. In addition, signaling between the LSC serving the Transferor and the Transferor's IP end instrument is not depicted. *If the Transferee uses a SIP end instrument
22, 23, 24	The LSC serving the Transferor sends a 200 (OK) response to the NOTIFY to Softswitch B. Softswitch B forwards the 200 (OK) to Softswitch A. Softswitch A forwards the 200 (OK) to the LSC serving the Transferee. NOTE: Signaling between the Transferor's IP end instrument and the LSC serving the Transferor is not depicted. In addition, signaling between the LSC serving the Transferee and the Transferee's IP end instrument is not depicted.
25, 26, 27	The LSC serving the Transferor now terminates the RTP session with the transferee. The LSC serving the transferor sends a BYE to Softswitch B. Softswitch B sends the BYE to Softswitch A. Softswitch A sends the BYE to the LSC serving the Transferee. NOTE: Signaling between the Transferor's IP end instrument and the LSC serving the Transferor is not depicted. In addition, signaling between the LSC serving the Transferee and the Transferee's IP end instrument is not depicted.
28, 29, 30	The LSC serving the Transferee responds to the BYE with a 200 (OK). The Transferee sends the BYE to Softswitch A. Softswitch A sends the 200 (OK) to Softswitch B. Softswitch B sends the 200 (OK) to the LSC serving the Transferor. NOTE: Signaling between the Transferee's IP end instrument and the LSC serving the Transferee is not depicted. In addition, signaling between the LSC serving the Transferor and the Transferor's IP end instrument is not depicted.
31, 32, 33	The LSC serving the Transferee creates (or forwards*) an INVITE using the SIP URI in the Refer-To header of the REFER request (received in step 15 from the Transferor) to generate the Request-URI of the INVITE. The INVITE MAY include a Referred-By header that contains the SIP URI of the Transferor.

STEP	INSTRUCTION
	The LSC serving the Transferee sends the INVITE to Softswitch A. Softswitch A sends the INVITE to Softswitch C (which is assigned to the LSC serving the Transfer Target (i.e., IP Party C)). Softswitch C sends the INVITE to the LSC serving the Transfer Target. NOTE: Signaling between the Transferee's IP end instrument and the LSC serving the Transferee is not depicted. In addition, signaling between the LSC serving the Transfer Target and the Transfer Target's IP end instrument is not depicted. *If the Transferee uses a SIP end instrument
34, 35, 36	The LSC serving the Transfer Target sends a 180 (Ringing) to Softswitch C. Softswitch C sends a 180 (Ringing) to Softswitch A. Softswitch A sends a 180 (Ringing) to the LSC serving the Transferee. NOTE: Signaling between the transfer Target's IP end instrument and the LSC serving the transfer target is not depicted. In addition, signaling between the LSC serving the transferee and the transferee's IP end instrument is not depicted.
37, 38, 39	The LSC serving the Transfer Target sends a 200 (OK) to Softswitch C. Softswitch C sends a 200 (OK) to Softswitch A. Softswitch A sends a 200 (OK) to the LSC serving the Transferee. NOTE: Signaling between the Transfer Target's IP end instrument and the LSC serving the Transfer Target is not depicted. In addition, signaling between the LSC serving the Transferee and the Transferee's IP end instrument is not depicted.
40, 41, 42	The LSC serving the Transferee sends an ACK to Softswitch A. Softswitch A sends the ACK to Softswitch C. Softswitch C sends the ACK to the LSC serving the Transfer Target. NOTE: Signaling between the Transferee's IP end instrument and the LSC serving the Transferee is not depicted. In addition, signaling between the LSC serving the Transfer Target and the Transfer Target's IP end instrument is not depicted.
43, 44, 45	The LSC serving the Transferee reports the success of the call transfer to the Transferor by creating (or forwarding*) a NOTIFY with a body having the SIP response status line: SIP/2.0 200 OK. The LSC serving the Transferee sends the NOTIFY to Softswitch A. Softswitch A forwards the NOTIFY to Softswitch B. Softswitch B forwards the NOTIFY to the LSC serving the Transferor. NOTE: Signaling between the Transferee's IP end instrument and the LSC serving the Transferee is not depicted. In addition, signaling between the LSC serving the Transferor and the Transferor's IP end instrument is not depicted.

STEP	INSTRUCTION
	*If the Transferee uses a SIP end instrument
46, 47, 48	The LSC serving the Transferor responds to the NOTIFY by creating a 200 (OK). The LSC serving the Transferor sends the 200 (OK) to Softswitch B. Softswitch B sends the 200 (OK) to Softswitch A. Softswitch A sends the 200 (OK) to the LSC serving the Transferee. NOTE: Signaling between the Transferor's IP end instrument and the LSC serving the Transferor is not depicted. In addition, signaling between the LSC serving the Transferee and the Transferee's IP end instrument is not depicted.

2. Method 2 does not remove the transferor LSC from the SIP signaling path. The transferor LSC employs re-INVITEs with the transferee and an INVITE with the transfer target in place of the use of the REFER request. The call flow is depicted in Figure 5.3.4-24, Unattended Call Transfer for IP End Instruments (INVITE Method).

Figure 5.3.4-24, Unattended Call Transfer for IP End Instruments (INVITE Method), presents an alternative SIP call flow for the unattended call transfer between a transferor, transferee, and transfer target that makes use of re-INVITEs and INVITEs (as opposed to the REFER request).

The basic sequence of events is as follows:

- The Transferee and the Transferor establish a session
- The Transferor places the session with the Transferee on hold (music on hold is optional)
- The Transferor initates the session establishment process with the Transfer Target (sends INVITE and receives 180 (Ringing)
- The Transferor updates the connected party information with the Transferee to reflect the identity of the Transfer Target
- The Transferor stops the music on hold if previously enabled and inserts ringback tone into bearer stream with Transferee
- The Transferor receives 200 from Transfer Target and stops playing ringback tone to Transferee

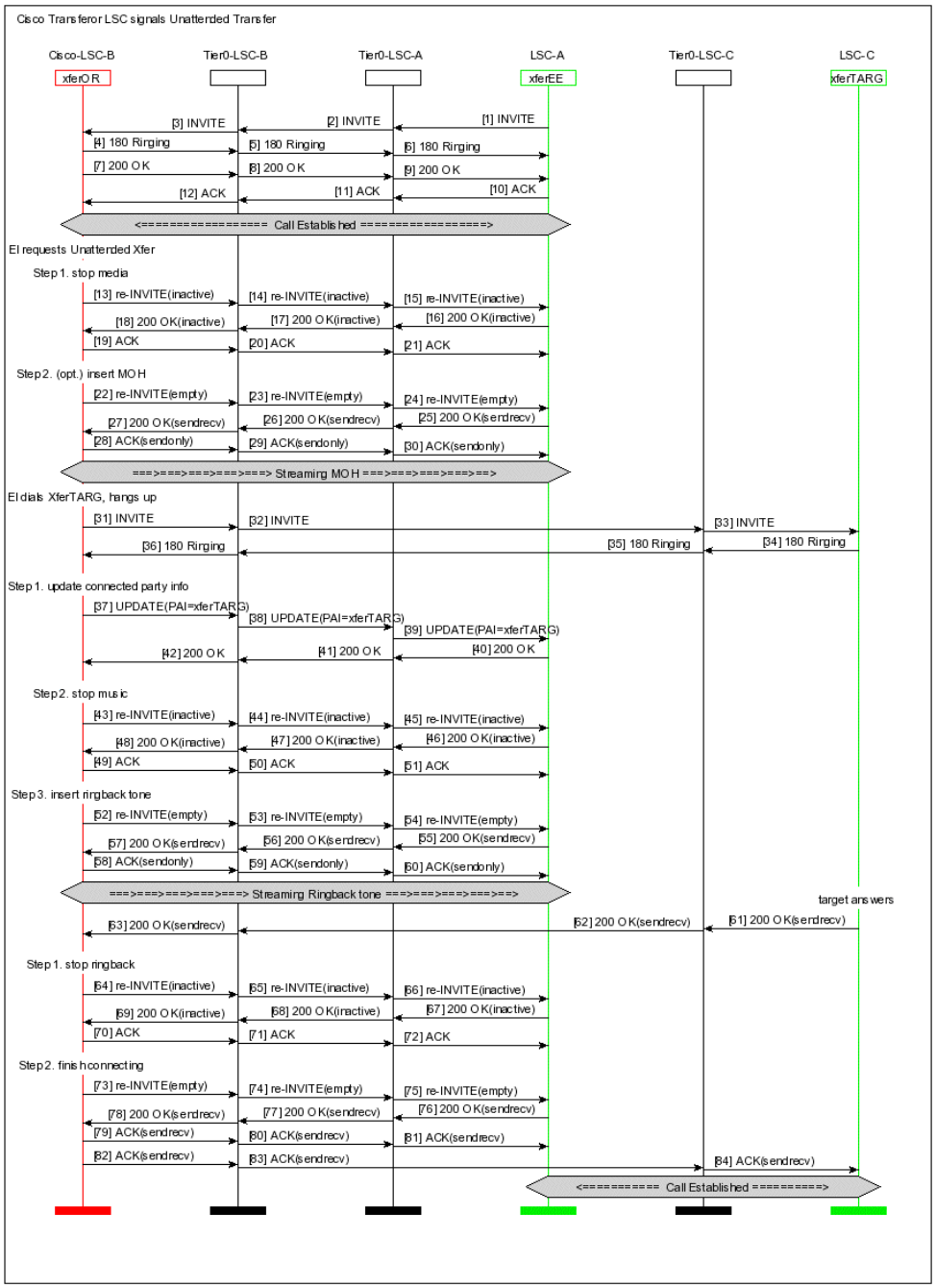


Figure 5.3.4-24. Unattended Call Transfer for IP End Instruments (INVITE Method)

- The Transferor employs a re-INVITE with Transferee to provide Transferee with the Transfer Target's IP address and udp port for the RTP bearer stream between Transferee and Transfer Target

- The Transferor completes session establishment with Transfer Target and provides Transfer Target with Transferee's IP address and udp port for the RTP stream between the Transfer Target and the Transferee

NOTE: The call flows between LSCs and the IP end instruments are not depicted.

Figure 5.3.4-25, Unattended Call Transfer for IP EIs (REFER Method), presents the SIP call flow for the unattended call transfer between a transferor, transferee, and transfer target that are all IP end instruments. The call flow is based on draft-ietf-sipping-service-examples sec. 2.4.

The basic sequence of events is as follows:

- The Transferee and the Transferor establish a session.

- The Transferor uses the REFER request to provide the Transferee with the contact information of the Transfer Target and to instruct the Transferee to initiate a session with the Transfer Target.

- The Transferee acknowledges the REFER request and terminates the session with the Transferor.

- The Transferee establishes a session with the Transfer Target.

- The Transferee notifies the Transferor of the successful establishment of the session between the Transferee and the Transfer Target.

NOTE: The call flows between LSCs and the IP end instruments are not depicted.

5.3.4.13.8.3 Attended Transfer Call Transferor: SIP

Two methods have been approved for conducting the attended call transfer: The first makes use of the REFER with Replaces method and the second makes use of INVITEs and re-INVITEs.

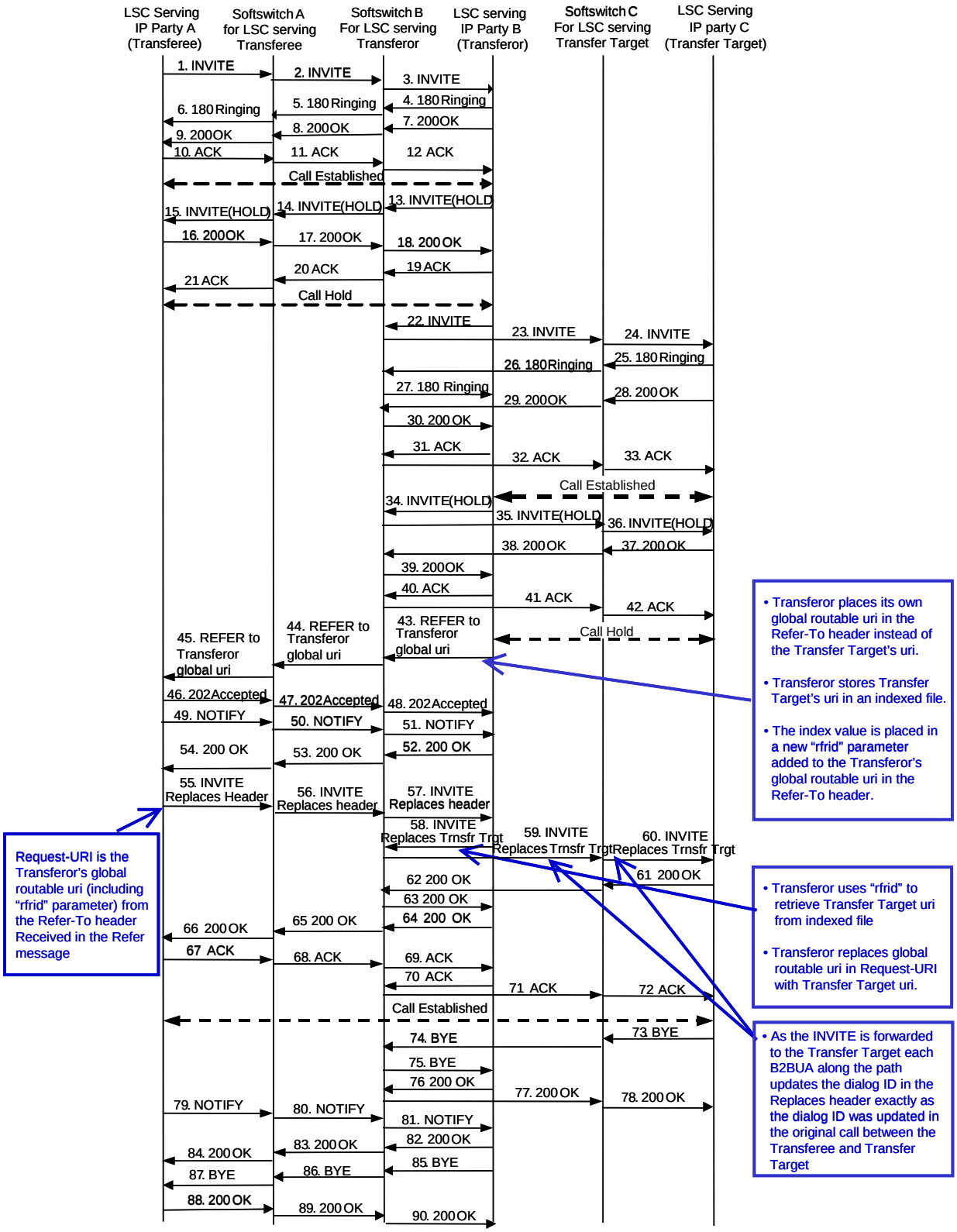


Figure 5.3.4-25. Attended Call Transfer for IP EIs (REFER Method)

Figure 5.3.4-25, Attended Call Transfer for IP EIs (REFER Method), presents the SIP call flow for the attended call transfer (using the REFER with Replaces method) between a transferor, transferee, and transfer target that are all IP end instruments. The call flow is loosely based upon ETSI TS 183 029 V2.5.0 Telecommunications and Internet converged Services and Protocols for Advanced Networking (TISPAN); PSTN/ISDN simulation services: Explicit Communication Transfer (ECT); Protocol specification. The basic sequence of events is as follows:

- The Transferee and the Transferor establish a session
- The Transferor places the session with the Transferee on hold
- The Transferor establishes a session with the Transfer Target

The Transferor places the session with the Transfer Target on hold The Transferor then proceeds with the creation of a REFER request intended for the Transferee. Normally, the URI of the Transfer Target would be used by the Transferor LSC to populate the Refer-To URI field. However, to enable the successful completion of the Attended Call Transfer using "REFER with Replaces," we need to keep the Transferor LSC in the signaling path of the REFER-triggered INVITE. As a result, the Transferor LSC inserts its own globally routable URI into the Refer-To header. The Transferor LSC places the Call-ID, to-tag, and from-tag information for the target dialog (from the perspective of the Transferor) in a single, fully escaped Replaces header field which is inserted into the Refer-to header (see the following example). The REFER is then forwarded downstream toward the Transferee.

NOTE: The Transferor LSC stores the actual Transfer Target URI in an indexed file and the index entry is placed in a new "rfrid" URI parameter that is inserted into the user-info field of the Refer-To URI as illustrated below:

Example:

Refer-
To:<sip:3121000000;rfrid=123456@dsn.mil;user=phone>;Replaces=592435881734450904%3B to-tag%3D9m2n3wq%3Bfrom-tag3D763231

- The Transferee accepts/acknowledges the REFER request.

- The Transferee attempts to establish a session by sending an INVITE request to the contact indentified in the Refer-To header. The INVITE request includes a single Replaces header field value (i.e., the un-escaped Replaces header field value from the Refer-to header within the body of the REFER which triggered the corresponding INVITE).

NOTE: The Transferor LSC is now permanently in the signaling path between the Transferee and Transfer Target until the transferred call between Transferee and Transfer Target is eventually terminated.

- Transferor LSC receives the INVITE. It uses the "rfrid" value to look up and retrieve the actual Transfer Target URI. The Transferor LSC replaces its globally routable URI in the Request-URI with the actual Transfer Target URI and forwards the INVITE toward the Transfer Target.

- As the INVITE request is forwarded from the Transferor LSC to the Transfer Target, the dialog ID value in the Replaces header is "updated" (mapped to the dialog ID value of a corresponding "call leg" as recognized by each of the signaling appliances along the signaling path) on each hop along the signaling path.

- After successfully establishing a session with the Transferee, the Transfer Target ends the session with the Transferor.

- The Transferee notifies the Transferor of the successful establishment of the session between the Transferee and the Transfer Target.

- The Transferor ends the session with the Transferee

NOTE: The call flows between LSCs and the IP end instruments are not depicted.

ASAC

It is important to note that the Figure 5.3.4-25, Attended Call Transfer for IP EIs (REFER Method) call flow requires the Transferor LSC to allocate two (2) call counts from the call count budget for the duration of the call even though no bearer traffic related to the given call actually transits the access link to the enclave at which the Transferor is located.

STEP	INSTRUCTION
1, 2, 3	Upon receiving an initial call request message from IP Party A (Transferee) (not depicted in the call flow diagram), the LSC serving IP Party A sends an INVITE to its assigned Softswitch (Softswitch A). Softswitch A forwards the INVITE to the Softswitch for the LSC serving IP Party B (Transferor) (Softswitch B). Softswitch B forwards the INVITE to the LSC serving IP Party B (Transferor). NOTE: Signaling between the EI serving IP Party A (Transferee) and the LSC serving IP Party A (Transferee) is not depicted. In addition, signaling between the LSC serving IP Party B (Transferor) and the EI serving IP Party B (Transferor) is not depicted.

STEP	INSTRUCTION
4, 5, 6	The LSC serving IP Party B (Transferor) sends a 180 (Ringing) to Softswitch B. Softswitch B forwards the 180 (Ringing) to Softswitch A, which forwards the 180 (Ringing) to the LSC serving IP Party A (Transferee). NOTE: Signaling between the EI serving IP Party B (Transferor) and the LSC serving IP Party B (Transferor) is not depicted. In addition, signaling between the LSC serving IP Party A (Transferee) and the EI serving IP Party A (Transferee) is not depicted.
7, 8, 9	When IP Party B (Transferor) goes off hook (i.e., answers the call), the LSC serving IP Party B sends a 200 (OK) to Softswitch B. Softswitch B forwards the 200 (OK) to Softswitch A, which forwards the 200 (OK) to the LSC serving IP Party A (Transferee). NOTE: Signaling between the EI serving IP Party B (Transferor) and the LSC serving IP Party B (Transferor) is not depicted. In addition, signaling between the LSC serving IP Party A (Transferee) and the EI serving IP Party A (Transferee) is not depicted.
10, 11, 12	The LSC serving IP Party A (Transferee) sends an ACK to Softswitch A. Softswitch A forwards the ACK to Softswitch B, which forwards the ACK to the LSC serving IP Party B (Transferor). NOTE: Signaling between the EI serving IP Party A (Transferee) and the LSC serving IP Party A is not depicted. In addition, signaling between the LSC serving IP Party B and the EI serving IP Party B (Transferor) is not depicted.
13, 14, 15	Transferor initiates call hold with Transferee. In response to a request on the part of the Transferor, the LSC serving the Transferor sends a mid-call INVITE to Softswitch B. The INVITE includes the attribute line “a=sendonly” or “a=inactive” if the stream had been a sendrecv media stream or “a=inactive” if the stream had been a recvonly stream. Softswitch B forwards the mid-call INVITE to Softswitch A, which forwards the mid-call INVITE to the LSC serving the Transferee. NOTE: The SIP UA MAY also support establishing a call hold by sending a mid-call INVITE that includes a session description that is the same as in the original request, but the “c” destination addresses for the media streams to be put on hold are set to zero: c=IN IP4 0.0.0.0. NOTE: Signaling between the Transferor’s end instrument and the LSC serving the Transferor is not depicted. In addition, signaling between the LSC serving the transferee and the end instrument serving the Transferee is not depicted.

STEP	INSTRUCTION
16, 17, 18	The LSC serving the Transferee sends a 200 (OK) to Softswitch A. Softswitch A sends the 200 (OK) to Softswitch B. Softswitch B sends the 200 (OK) to the LSC serving the Transferor. NOTE: Signaling between the Transferee's end instrument and the LSC serving the Transferee is not depicted. In addition, signaling between the LSC serving the transferor and the end instrument serving the Transferor is not depicted.
19, 20, 21	The LSC serving the Transferor sends an ACK to Softswitch B. Softswitch B sends an ACK to Softswitch A. Softswitch A sends the ACK to the LSC serving the Transferee. NOTE: Signaling between the Transferor's end instrument and the LSC serving the Transferor is not depicted. In addition,signaling between the LSC serving the transferee and the end instrument serving the Transferee is not depicted.
22, 23, 24	Upon receiving a call request message from the Transferor (not depicted in the call flow diagram), the LSC serving the Transferor sends an INVITE to Softswitch B. Softswitch B forwards the INVITE to the Softswitch C (which is responsible for the LSC serving the Transfer Target). Softswitch C forwards the INVITE to the LSC serving the Transfer Target (IP Party C). NOTE: Signaling between the IP end instrument serving the transferor and the LSC serving the transferor is not depicted. In addition,signaling between the LSC serving the Transfer Target and the IP end instrument serving the Transfer Target is not depicted.
25, 26, 27	The LSC serving the Transfer Target sends a 180 (Ringing) to Softswitch C. Softswitch C forwards the 180 (Ringing) to Softswitch B, which forwards the 180 (Ringing) to the LSC serving the Transferor. NOTE: Signaling between the IP end instrument serving the Transfer Target and the LSC serving the Transfer Target is not depicted. In addition,signaling between the LSC serving the Transferor and the IP end instrument serving the Transferor is not depicted.
28, 29, 30	When the Transfer Target goes off hook (i.e., answers the call), the LSC serving the Transfer Target sends a 200 (OK) to Softswitch C. Softswitch C forwards the 200 (OK) to Softswitch B, which forwards the 200 (OK) to the LSC serving the transferor. NOTE: Signaling between the EI serving IP Party C (Transfer Target) and the LSC serving the Transfer Target is not depicted. In addition, signaling between the LSC serving IP Party A (Transferor) and the EI serving IP Party A (Transferor) is not depicted.

STEP	INSTRUCTION
31, 32, 33	The LSC serving IP Party B (Transferor) sends an ACK to Softswitch B. Softswitch B forwards the ACK to Softswitch C, which forwards the ACK to the LSC serving IP Party C (Transfer Target). NOTE: Signaling between the EI serving IP Party B (Transferor) and the LSC serving IP Party B (Transferor) is not depicted. In addition, signaling between the LSC serving IP Party C (Transfer Target) and the EI serving IP Party C (Transfer Target) is not depicted.
34, 35, 36	Transferor initiates call hold with Transfer Target. In response to a request on the part of the Transferor, the LSC serving the Transferor sends a mid-call INVITE to Softswitch B. The INVITE includes the attribute line "a=sendonly" or "a=inactive" if the stream had been a sendrecv media stream or "a=inactive" if the stream had been a recvonly stream. Softswitch B forwards the mid-call INVITE to Softswitch C, which forwards the mid-call INVITE to the LSC serving the Transfer Target. NOTE: The SIP UA MAY also support establishing a call hold by sending a mid-call INVITE that includes a session description that is the same as in the original request, but the "c" destination addresses for the media streams to be put on hold are set to zero: c=IN IP4 0.0.0.0. NOTE: Signaling between the Transferor's end instrument and the LSC serving the Transferor is not depicted. In addition,signaling between the LSC serving the Transfer Target and the end instrument serving the Transfer Target is not depicted.
37, 38, 39	The LSC serving the Transfer Target sends a 200 (OK) to Softswitch C. Softswitch C sends the 200 (OK) to Softswitch B. Softswitch B sends the 200 (OK) to the LSC serving the Transferor. NOTE: Signaling between the Transfer Target's end instrument and the LSC serving the Transfer Target is not depicted. In addition,signaling between the LSC serving the transferor and the end instrument serving the Transferor is not depicted.
40, 41, 42	The LSC serving the Transferor sends an ACK to Softswitch B. Softswitch B sends an ACK to Softswitch C. Softswitch C sends the ACK to the LSC serving the Transfer Target. NOTE: Signaling between the Transferor's end instrument and the LSC serving the Transferor is not depicted. In addition,signaling between the LSC serving the transfer target and the end instrument serving the Transfer Target is not depicted.

STEP	INSTRUCTION
43, 44, 45	The Transferor (IP Party B) wishes to transfer the call with the Transferee (IP party A) to the Transfer Target (IP Party C) and instructs the IP end instrument to initiate a request for a call transfer to the Transfer Target. In the case of an attended call transfer and a SIP end instrument, the message takes the form of a REFER request whereby the Refer-To header has the format indicated in RFC 3515, page 3, example 3. To wit, the SIP URI of the Transfer Target is followed by ”?,” followed by ”Replaces=,” followed by the Call-ID of the established dialog between the Transferor and the Transfer target (where the “@” symbol is replaced by “%40”), followed by “%3Bto-tag=%3D” followed by the value of the to-tag of the dialog between the Transferor and the Transfer Target, followed by “%3Bfrom-tag=%3D,” followed by the value of the from-tag of the dialog between the Transferor and the Transfer Target. (For an example please see draft-ietf-sipping-service-examples sec. 2.5 Transfer attended message F15). Upon receiving the REFER, the Transferor LSC stores the Transfer Target’s uri in an indexed file. Transferor LSC places its own global routable uri in the Refer-To header Transferor LSC places the index value (used to access the Transfer Target URI in the indexed file) in a new “rfrid” parameter added to the Transferor LSC’s globally routable URI in the Refer-To header If the Call ID, To tag, or From tag used by the Transferor LSC in the established call to the Transfer Target is different from the values entered by the Transferor sip end instrument then the Transferor LSC places its values for Call ID, To tag, and From tag in the Replaces field of the Refer-To header. Transferor LSC sends the REFER to Softswitch B. Softswitch B forwards the REFER to Softswitch A. Softswitch A sends the REFER to the LSC serving IP party A (the Transferee LSC). NOTE: All AS-SIP signaling appliances in the signaling path from the Transferor LSC thru the Transferee LSC must preserve the entire URI including the the “rfrid” parameter located in the Refer-To header.
46, 47, 48	The LSC serving the Transferee responds to the REFER with a 202 (Accepted) that it sends to Softswitch A. Softswitch A forwards the 202 (Accepted) to Softswitch B. Softswitch B forwards the 202 (Accepted) to the LSC serving the Transferor. NOTE: Signaling between the Transferee’s IP end instrument and the LSC serving the Transferee is not depicted. In addition,signaling between the LSC serving the Transferor and the Transferor’s IP end instrument is not depicted.

STEP	INSTRUCTION
49, 50, 51	The LSC serving the Transferee creates (or forwards*) a NOTIFY with a body having the SIP response status line: SIP/2.0 100 Trying. The LSC serving the Transferee sends the NOTIFY to Softswitch A. Softswitch A forwards the NOTIFY to Softswitch B. Softswitch B forwards the NOTIFY to the LSC serving the Transferor. NOTE: Signaling between the Transferee's IP end instrument and the LSC serving the Transferee is not depicted. In addition,signaling between the LSC serving the Transferor and the Transferor's IP end instrument is not depicted. *If the Transferee uses a SIP end instrument
52, 53, 54	The LSC serving the Transferor sends a 200 (OK) to the NOTIFY to Softswitch B. Softswitch B forwards the 200 (OK) to Softswitch A, which forwards the 200 (OK) to the LSC serving the Transferee. NOTE: Signaling between the Transferor's IP end instrument and the LSC serving the Transferor is not depicted. In addition,signaling between the LSC serving the Transferee and the Transferee's IP end instrument is not depicted.
55, 56, 57	The LSC serving the Transferee creates (or forwards*) an INVITE addressed to the Transferor LSC's globally routable URI. The Request-URI field is the SIP URI from the Refer-To header of the REFER request (step 45) that consists of the globally routable URI of the Transferor LSC and the "rfrid" parameter. The INVITE also includes a Replaces header with a Call-ID, To-tag, and From-tag whose values are taken from the Refer-To header of the REFER request (step 45). LSC serving IP party A sends INVITE to Softswitch A which forwards the INVITE to Softswitch B which forwards the INVITE to LSC serving IP party B (i.e. Transferor LSC). NOTE: Signaling between the transferee's IP end instrument and the LSC serving the transferee is not depicted. *If the Transferee uses a SIP end instrument
58, 59, 60	Transferor LSC uses value in "rfrid" parameter to retrieve the Transfer Target URI. Transferor LSC replaces its global routable URI in the Request-URI with the Transfer Target URI. As the INVITE is forwarded from Transferor LSC to Transfer Target various of the AS-SIP signaling appliances implemented as B2BUAs will need to update the dialog ID in the Replaces header to match the dialog ID changes made across call legs to the established call between the Transferor and Transfer Target The Transferor LSC sends the INVITE to Softswitch B which sends the INVITE to Softswitch C which sends the INVITE to LSC serving IP party C. Note: Signaling between the LSC serving the transfer target and the transfer target's IP end instrument is not depicted.

STEP	INSTRUCTION
61, 62, 63, 64, 65, 66	The LSC serving the Transfer Target sends a 200 (OK) to Softswitch C. It forwards the 200 (OK) to Softswitch B, which forwards the 200 (OK) to the LSC serving the Transferor which forwards the 200 OK back to Softswitch B which forwards the 200 OK to Softswitch A which forwards the 200 OK to the LSC serving the Transferee. Note: Signaling between the transfer target's IP end instrument and the LSC serving the transfer target is not depicted. In addition, signaling between the LSC serving the transferee and the transferee's IP end instrument is not depicted.
67, 68, 69, 70, 71, 72	The LSC serving the transferee sends an ACK to Softswitch A. Softswitch A sends the ACK to Softswitch B. Softswitch B sends the ACK to the LSC serving the transferor. The LSC serving the transferor sends the ACK back to Softswithc B. Softswitch B sends the ACK to Softswitch C. Softswitch C sends the ACK to the LSC serving the transfer target. NOTE: Signaling between the transferee's IP end instrument and the LSC serving the transferee is not depicted. In addition, signaling between the LSC serving the transfer target and the transfer target's IP end instrument is not depicted.
73, 74, 75	Transfer Target terminates session with Transferor. The LSC serving the Transfer Target sends a BYE to Softswitch C. It sends the BYE to Softswitch A, which sends the BYE to the LSC serving the Transferor. NOTE: Signaling between the transfer target's IP end instrument and the LSC serving the transfer target is not depicted. In addition,signaling between the LSC serving the transferor and the transferor's IP end instrument is not depicted.
76, 77, 78	The LSC serving the Transferor sends a 200 (OK) to Softswitch A. It sends a 200 (OK) to Softswitch C, which sends a 200 (OK) to the LSC serving the Transfer Target. NOTE: Signaling between the transferor's IP end instrument and the LSC serving the transferor is not depicted. In addition,signaling between the LSC serving the transfer target and the transfer target's IP end instrument is not depicted.
79, 80, 81	The LSC serving the Transferee reports the success of the call transfer to the Transferor by creating (or forwarding*) a NOTIFY with a body having the SIP response status line: SIP/2.0 200 OK. The LSC serving the Transferee sends the NOTIFY to Softswitch A. It forwards the NOTIFY to Softswitch B, which forwards the NOTIFY to the LSC serving the Transferor. NOTE: Signaling between the transferee's IP end instrument and the LSC serving the transferee is not depicted. In addition,signaling between the LSC serving the transferor and the transferor's IP end instrument is not depicted. *If the Transferee uses a SIP end instrument

STEP	INSTRUCTION
82, 83, 84	The LSC serving the Transferor responds to the NOTIFY with a 200 (OK). The LSC serving the Transferor sends the 200 (OK) to Softswitch B. It sends the 200 (OK) to Softswitch A, which sends the 200 (OK) to the LSC serving the Transferee. NOTE: Signaling between the Transferor's IP end instrument and the LSC serving the Transferor is not depicted. In addition, signaling between the LSC serving the Transferee and the Transferee's IP end instrument is not depicted.
85, 86, 87	The LSC serving the Transferor sends a BYE to Softswitch B to initiate the session termination between the Transferor and the Transferee. Softswitch B sends the BYE to Softswitch A. It sends the BYE to the LSC serving the Transferee. NOTE: Signaling between the Transferor's IP end instrument and the LSC serving the Transferor is not depicted. In addition, signaling between the LSC serving the Transferee and the Transferee's IP end instrument is not depicted.
88, 89, 90	The LSC serving the Transferee responds to the BYE with a 200 (OK). The LSC serving the Transferee sends the 200 (OK) to Softswitch A. It sends the 200 (OK) to Softswitch B, which sends the 200 (OK) to the LSC serving the Transferor. NOTE: Signaling between the Transferee's end instrument and the LSC serving the Transferee is not depicted. In addition, signaling between the LSC serving the Transferor and the Transferor's IP end instrument is not depicted.

Figure 5.3.4-26, Attended Call Transfer for IP EI (INVITE and re-INVITE Method), presents an alternative SIP call flow for the attended call transfer between a transferor, transferee, and transfer target that makes use of an INVITE and re-INVITEs (as opposed to the REFER request and an INVITE with a Replaces header).

The basic sequence of events is as follows:

- The Transferee and the Transferor establish a session.
- The Transferor places the session with the Transferee on hold (music on hold is optional).
- The Transferor and the Transfer Target establish a session.
- The Transferor stops the music on hold with the Transferee if previously enabled and places the call on hold without media.

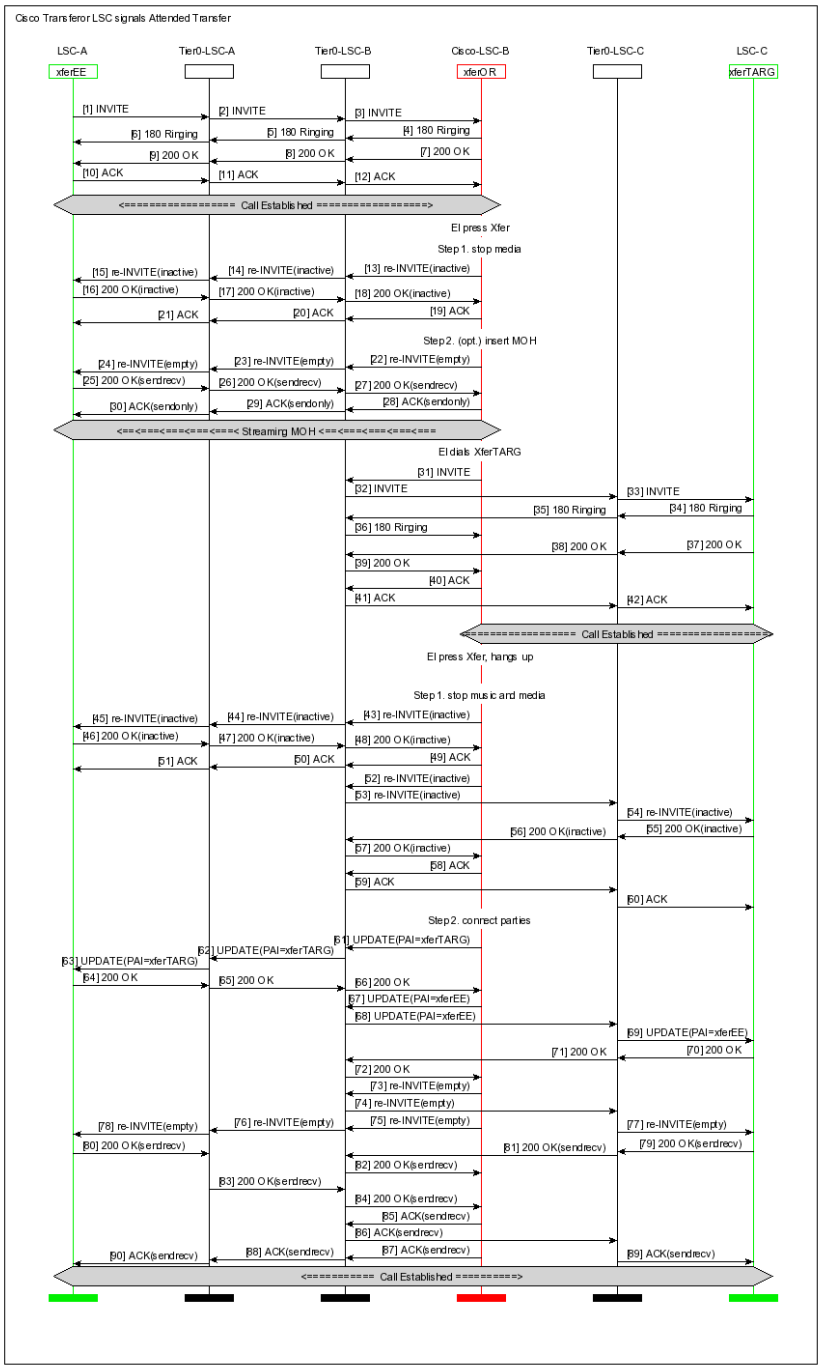


Figure 5.3.4-26. Attended Call Transfer for IP EI (INVITE and re-INVITE Method)

- The Transferor places the call with the Transfer Target on hold.
- The Transferor updates the connected party information with the Transferee to reflect the identity of the Transfer Target.
- The Transferor updates the connected party information with the Transfer Target to reflect the identity of the Transferee
- The Transferor initiates a re-INVITE with the Transferee to obtain an IP address and udp port to be provided to the Transfer Target and initiates a separate re-INVITE with the Transfer Target in order to obtain an IP address and udp port for the bearer stream to provide to the Transferee.
- The Transferor provides the Transferee with the IP address and udp port information obtained from the Transfer Target when the Transferor sends the sdp answer to the Transferee (ACK request 87, 88, 90).
- The Transferor provides the Transfer Target with the IP address and udp port information obtained from the Transferee when the Transferor sends the sdp answer to the Transfer Target (ACK request 85, 86, 89).

NOTE: The call flows between LSCs and the IP end instruments are not depicted.

ASAC

It is important to note that the Figure 5.3.4-26, Attended Call Transfer for IP EI (INVITE and re-INVITE Method) call flow requires the Transferor LSC to allocate two (2) call counts from the call count budget for the duration of the call even though no bearer traffic related to the given call actually transits the access link to the enclave at which the Transferor is located.

5.3.4.13.9 Modem on IP Networks

V.150.1 requirements TBD.

5.3.4.14 SIP Translation Requirements for Interworking AS-SIP Signaling Appliances

5.3.4.14.1 Introduction

The DISN Assured Services design has been evolving over time and the following Paragraphs detailing the requirements for interworking AS-SIP signaling and TDM signaling are crafted to

reflect that evolution. At the outset, the locus for AS-SIP -TDM signaling inter-working was the Softswitch[43]. It is now understood and the following Paragraphs reflect that the AS-SIP -TDM inter-working may occur at the Softswitch or at the LSC.

The detailed signal inter-working requirements in the following Paragraphs describe translation between AS-SIP and CCS7 ISUP. It is recognized that the TDM signaling to be inter-worked at the Softswitch may take the form of CCS7 ISUP and/or ISDN Q.931 and that TDM signaling at the LSC will in all likelihood take the form of ISDN Q.931 messages.[44] The most comprehensive standards document covering SIP-TDM signaling inter-working is ITU-T Recommendation Q.1912.5 "Interworking between Session Initiation Protocol (SIP) and Bearer Independent Call Control Protocol or ISDN User Part" which defines the requirements for SIP-ISUP translation and encapsulation. We have chosen to rely upon Q.1912.5 and to a lesser extent RFC 3398 "Integrated Services Digital Network (ISDN) User Part (ISUP) to Session Initiation Protocol (SIP) Mapping" as the base documents for defining signaling interoperability between SIP and TDM. As the inter-working between CCS7 ISUP and ISDN Q.931 is well understood and has been practiced in TDM switches for an extended period of time, the SIP-CCS7 translation requirements found in these appendices are also deemed to provide a sufficient basis for the interoperable inter-working of SIP with ISDN Q.931.

NOTE: This specification employs SIP translation for converting between ISUP signaling and AS-SIP signaling but does not employ SIP encapsulation of ISUP.

The signaling mediation requirements levied on the interworking AS-SIP signaling appliances are best organized and understood in the context of the role of the Originating TDM/IP signaling gateway and the Terminating IP/TDM signaling gateway in each of the three call signaling path types described below (i.e., TDM-to-TDM calls over IP backbone[45], TDM-to-IP calls, and IP-to-TDM calls).

5.3.4.14.1.1 TDM-to-TDM Calls Over IP Backbone

Figure 5.3.4-27 depicts the basic signaling elements in a TDM-to-TDM call flow bridging over an IP backbone wherein the Softswitch on the left assumes the role of an originating TDM/IP signaling gateway and the Softswitch on the right assumes the role of a terminating IP/TDM

[43]Identified in earlier versions as the Multifunction Softswitch or SIP-T(AS) signaling appliance.
[44] For completeness we note that the inter-working could also occur between AS-SIP and a Channel Associated Signaling trunk.
[45] For at least the 2008-2012 time frame Assured Services Requirements have adopted the principle that when a call request begins at an end instrument served by a TDM signaling appliance then said TDM signaling appliance will employ TDM call signaling on behalf of the call request and all subsequent signaling appliances that receive the forwarded call request MUST also employ TDM signaling until and unless the IP network offers the only available signaling path towards the intended destination. This rule will greatly reduce the incidence of TDM bridging call flows in the initial time frame.

signaling gateway. Each interworking gateway conducts translation between SIP and the corresponding TDM signaling. Refer to Table 5.3.4-11, Reference Case 1a – TDM-to-TDM Bridging over an IP Backbone, for Reference Case 1a.

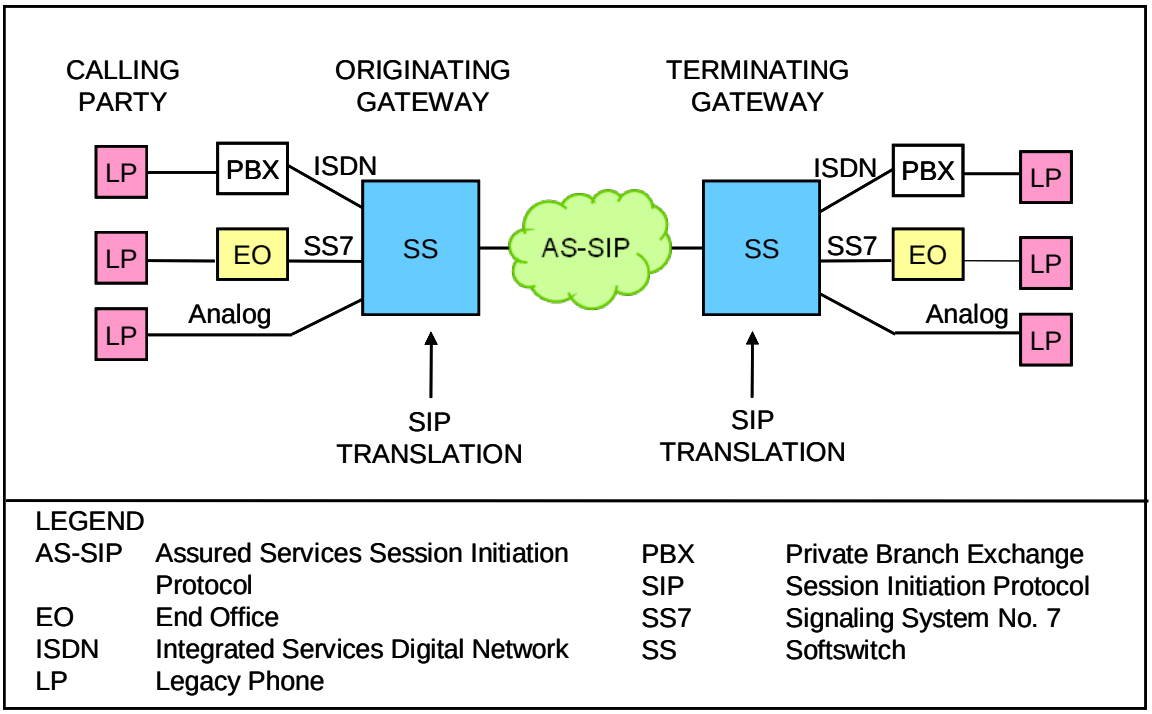


Figure 5.3.4-27. TDM-to-TDM Bridging over an IP Backbone

Table 5.3.4-11. Reference Case #1a – TDM-to-TDM Bridging over an IP Backbone

1A	Legacy phone	PBX	ISDN	Softswitch	AS-SIP	Softswitch	ISDN	PBX	Legacy phone
1B	Legacy phone	PBX	ISDN	Softswitch	AS-SIP	Softswitch	CCS7	EO	Legacy phone
1C	Legacy phone	PBX	ISDN	Softswitch	AS-SIP.	Softswitch	Analog		Legacy phone
1D	Legacy phone	EO	CCS7	Softswitch	AS-SIP	Softswitch	ISDN	PBX	Legacy phone
1E	Legacy phone	EO	CCS7	Softswitch	AS-SIP	Softswitch	CCS7	EO	Legacy phone
1F	Legacy phone	EO	CCS7	Softswitch	AS-SIP	Softswitch	Analog		Legacy phone
1G	Legacy phone		Analog	Softswitch	AS-SIP	Softswitch	ISDN	PBX	Legacy phone
1H	Legacy phone		Analog	Softswitch	AS-SIP	Softswitch	CCS7	EO	Legacy phone
1I	Legacy phone		Analog	Softswitch	AS-SIP	Softswitch	Analog		Legacy phone

Figure 5.3.4-28 depicts the basic signaling elements in a TDM-to-TDM call flow bridging from enclave to enclave wherein the LSC on the left assumes the role of an originating TDM/IP signaling gateway and the LSC on the right assumes the role of a terminating IP/TDM signaling gateway. In Figure 5.3.4-28, the TDM connectivity between the enclave and the core has been removed and the only connectivity from the enclave to the core consists of IP connectivity. Each

interworking gateway (LSC) conducts translation between SIP and the corresponding TDM signaling (e.g., ISDN Q.931). Refer to Table 5.3.4-12, Reference Case #1b – TDM-to-TDM Bridging from Enclave-to-Enclave, for Reference Case #1b.

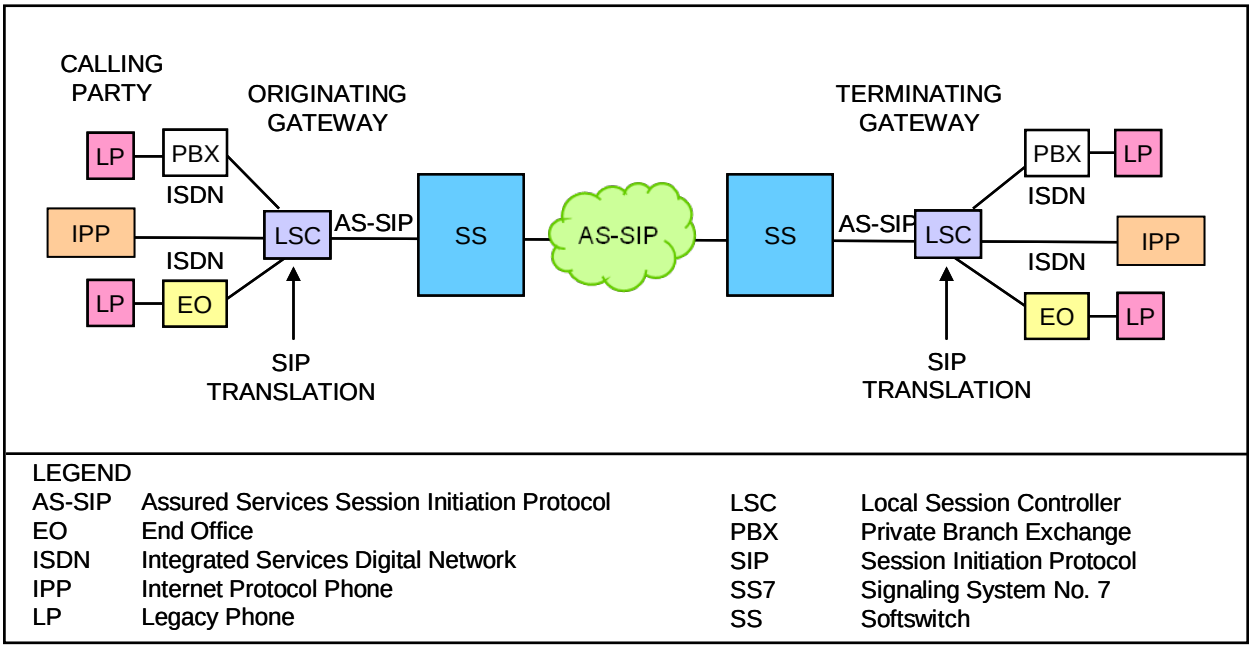


Figure 5.3.4-28. TDM-to-TDM Bridging from Enclave-to-Enclave

Table 5.3.4-12. Reference Case #1b – TDM-to-TDM Bridging from Enclave-to-Enclave

1J	Legacy phone	PBX	ISDN	LSC	AS-SIP	Softswitch	AS-SIP	Softswitch	AS-SIP	LSC	ISDN	PBX	Legacy phone
1K	Legacy phone	PBX	ISDN	LSC	AS-SIP	Softswitch	AS-SIP	Softswitch	AS-SIP	LSC	ISDN	EO	Legacy phone
1L	Legacy phone	EO	ISDN	LSC	AS-SIP	Softswitch	AS-SIP	Softswitch	AS-SIP	LSC	ISDN	PBX	Legacy phone
1M	Legacy phone	EO	ISDN	LSC	AS-SIP	Softswitch	AS-SIP	Softswitch	AS-SIP	LSC	ISDN	EO	Legacy phone

Figure 5.3.4-29 depicts the basic signaling elements in a TDM-to-TDM call flow bridging over an IP backbone wherein the Softswitch on the left assumes the role of an originating TDM/IP signaling gateway and the LSC on the right assumes the role of a terminating IP/TDM signaling gateway. Each interworking gateway conducts translation between SIP and the corresponding TDM signaling. Refer to Table 5.3.4-13 for Reference Case #1c.

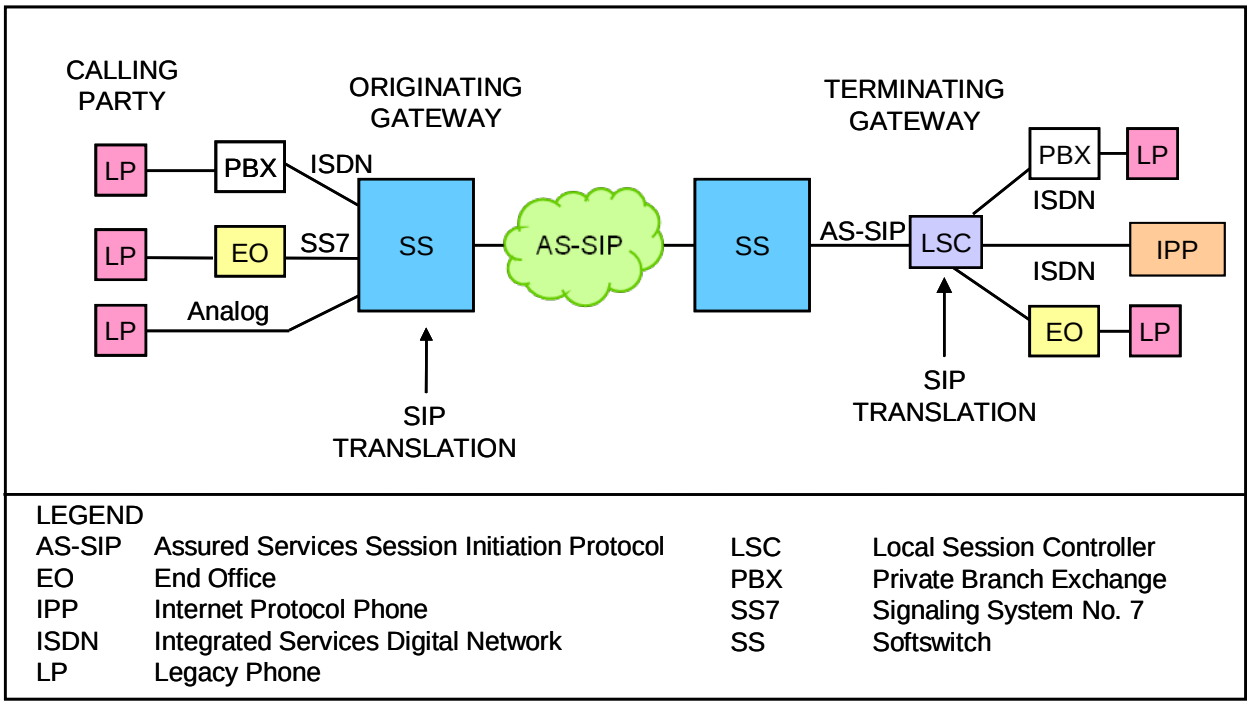


Figure 5.3.4-29. TDM-to-TDM Bridging from Softswitch-to-LSC

Table 5.3.4-13. Reference Case #1c – TDM-to-TDM Bridging from Softswitch-to-LSC

1N	Legacy phone	PBX	ISDN	Softswitch	AS-SIP	Softswitch	AS-SIP	LSC	ISDN	PBX	Legacy phone
1O	Legacy phone	PBX	ISDN	Softswitch	AS-SIP	Softswitch	AS-SIP	LSC	ISDN	EO	Legacy phone
1P	Legacy phone	EO	CCS7	Softswitch	AS-SIP	Softswitch	AS-SIP	LSC	ISDN	PBX	Legacy phone
1Q	Legacy phone	EO	CCS7	Softswitch	AS-SIP	Softswitch	AS-SIP	LSC	ISDN	EO	Legacy phone
1R	Legacy phone		Analog	Softswitch	AS-SIP	Softswitch	AS-SIP	LSC	ISDN	PBX	Legacy phone
1S	Legacy phone		Analog	Softswitch	AS-SIP	Softswitch	AS-SIP	LSC	ISDN	EO	Legacy phone

Figure 5.3.4-30 depicts the basic signaling elements in a TDM-to-TDM call flow bridging over an IP backbone wherein the LSC on the left assumes the role of an originating TDM/IP signaling gateway and the Softswitch on the right assumes the role of a terminating IP/TDM signaling gateway. Each inter-working gateway conducts translation between SIP and the corresponding TDM signaling. Refer to Table 5.3.4-14 for Reference Case #1d.

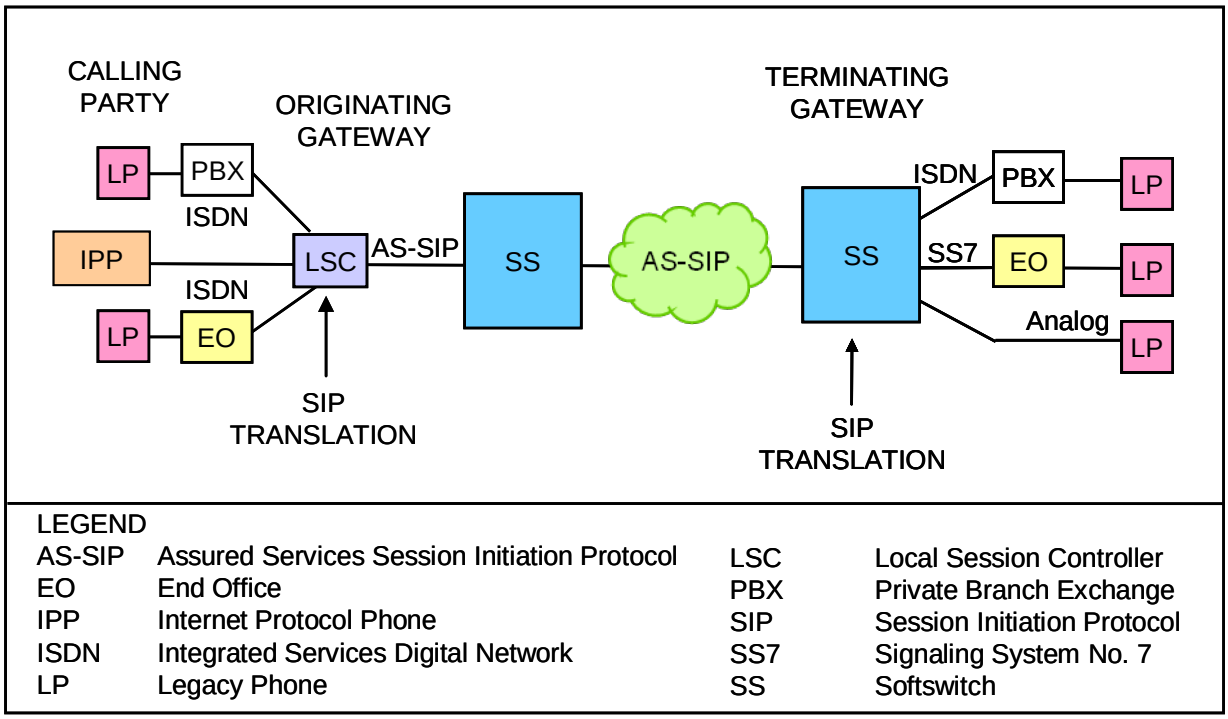


Figure 5.3.4-30. TDM-to-TDM Bridging from LSC-to-Softswitch

Table 5.3.4-14. Reference Case #1d – TDM-to-TDM Bridging from LSC-to-Softswitch

1T	Legacy phone	PBX	ISDN	LSC	AS-SIP	Softswitch	AS-SIP	Softswitch	ISDN	PBX	Legacy phone
1U	Legacy phone	PBX	ISDN	LSC	AS-SIP	Softswitch	AS-SIP	Softswitch	CCS7	EO	Legacy phone
1V	Legacy phone	PBX	ISDN	LSC	AS-SIP	Softswitch	AS-SIP.	Softswitch	Analog		Legacy phone
1W	Legacy phone	EO	ISDN	LSC	AS-SIP	Softswitch	AS-SIP	Softswitch	ISDN	PBX	Legacy phone
1X	Legacy phone	EO	ISDN	LSC	AS-SIP	Softswitch	AS-SIP.	Softswitch	CCS7	EO	Legacy phone
1Y	Legacy phone	EO	ISDN	LSC	AS-SIP	Softswitch	AS-SIP	Softswitch	Analog		Legacy phone

5.3.4.14.1.2 TDM-to-IP Calls Over an IP Backbone

Figure 5.3.4-31, TDM-to-IP Call over an IP Backbone, depicts the basic signaling elements in a TDM-to-IP call flow in which the Softswitch (shown to the left of the IP backbone) assumes the role of an originating TDM/IP signaling gateway. The originating TDM/IP signaling gateway will conduct translation between ISUP and SIP.

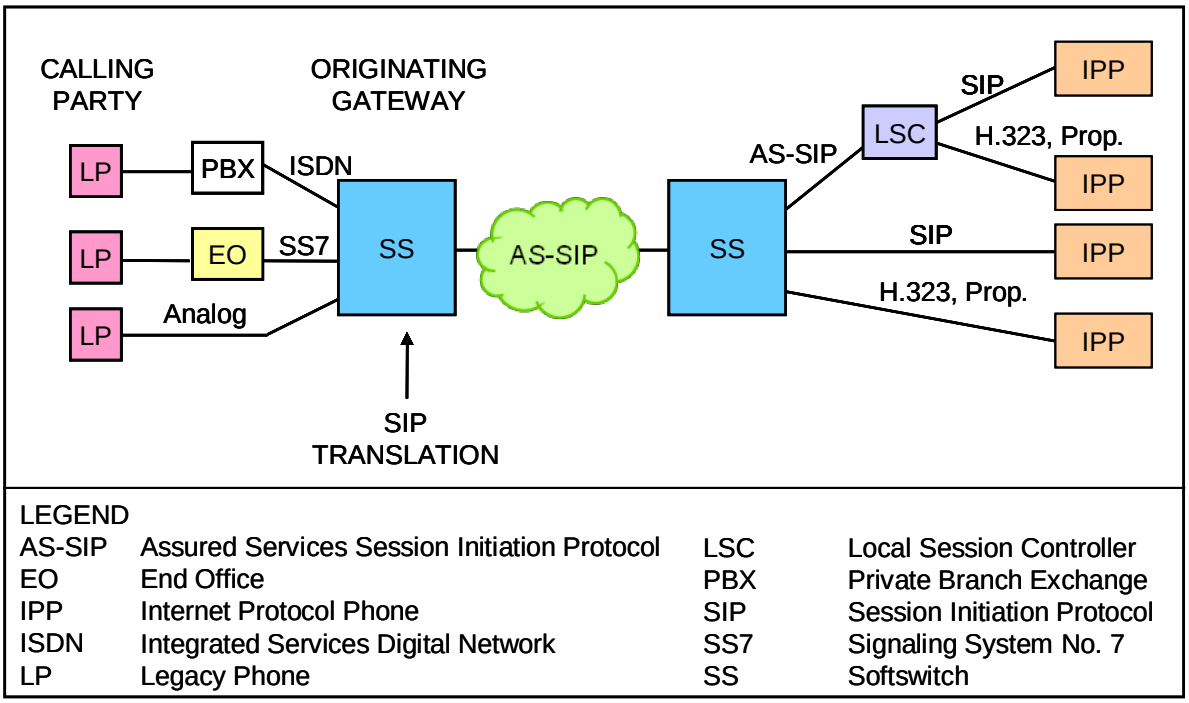


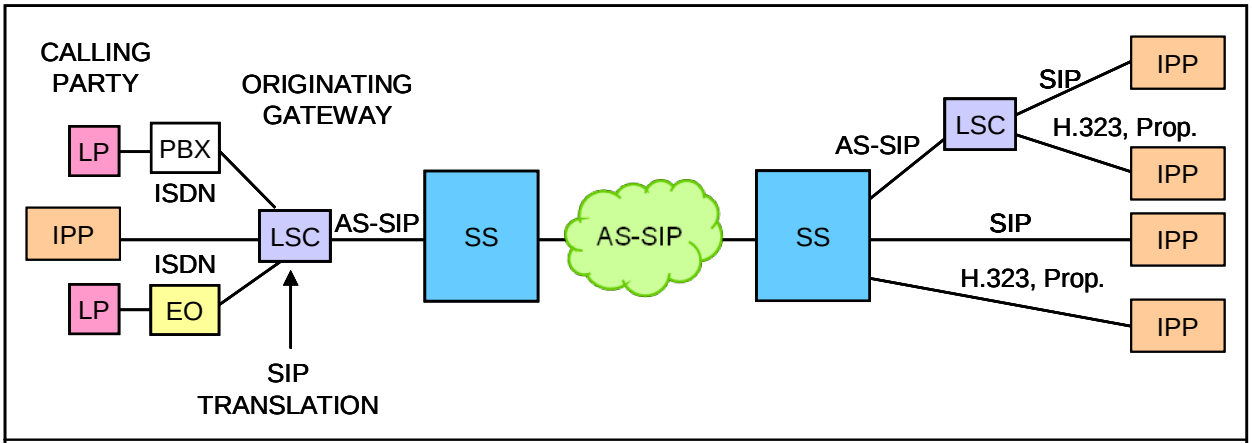
Figure 5.3.4-31. TDM-to-IP Call over an IP Backbone

The Softswitch to the right of the IP backbone forwards the AS-SIP message to an LSC or sends a SIP, H.323, or proprietary signaling message to a directly served IP end instrument. Refer to Table 5.3.4-15 for Reference Case #2a.

Figure 5.3.4-32, TDM-to-IP Call Translated at Originating Enclave, depicts the basic signaling elements in a TDM-to-IP call flow in which the LSC (shown to the left of the IP backbone) assumes the role of an originating TDM/IP signaling gateway. The originating TDM/IP signaling gateway will conduct translation between ISUP and SIP.

Table 5.3.4-15. Reference Case #2a – TDM-IP Call over an IP Backbone

2A	Legacy phone	PBX	ISDN	Softswitch	AS-SIP	Softswitch	AS-SIP	LSC	SIP	IP phone
2B	Legacy phone	PBX	ISDN	Softswitch	AS-SIP	Softswitch	AS-SIP	LSC	H323, Prop.	IP Phone
2C	Legacy phone	PBX	ISDN	Softswitch	AS-SIP	Softswitch	SIP			IP Phone
2D	Legacy phone	PBX	ISDN	Softswitch	AS-SIP	Softswitch	H.323, Prop.			IP Phone
2E	Legacy phone	EO	CCS7	Softswitch	AS-SIP	Softswitch	AS-SIP	LSC	SIP	IP phone
2F	Legacy phone	EO	CCS7	Softswitch	AS-SIP	Softswitch	AS-SIP	LSC	H323, Prop.	IP Phone
2G	Legacy phone	EO	CCS7	Softswitch	AS-SIP	Softswitch	SIP			IP Phone
2H	Legacy phone	EO	CCS7	Softswitch	AS-SIP	Softswitch	H.323, Prop.			IP Phone
2I.	Legacy phone		Analog	Softswitch	AS-SIP	Softswitch	AS-SIP	LSC	SIP	IP phone
2J.	Legacy phone		Analog	Softswitch	AS-SIP	Softswitch	AS-SIP	LSC	H323, Prop.	IP Phone
2K	Legacy phone		Analog	Softswitch	AS-SIP	Softswitch	SIP			IP Phone
2L	Legacy phone		Analog	Softswitch	AS-SIP	Softswitch	H.323, Prop.			IP Phone



LEGEND

AS-SIP	Assured Services Session Initiation Protocol	LSC	Local Session Controller
EO	End Office	PBX	Private Branch Exchange
IPP	Internet Protocol Phone	SIP	Session Initiation Protocol
ISDN	Integrated Services Digital Network	SS7	Signaling System No. 7
LP	Legacy Phone	SS	Softswitch

Figure 5.3.4-32. TDM-to-IP Call Translated at Originating Enclave

The Softswitch to the right of the IP backbone either sends a SIP, H.323, or proprietary signaling message to a directly served IP end instrument or forwards the AS-SIP message to the LSC which in turn sends a SIP, H.323, or proprietary signaling message to a directly served IP end instrument. Refer to Table 5.3.4-16 for Reference Case #2b.

Table 5.3.4-16. Reference Case #2b – TDM-IP Call Translated at Originating Enclave

2M	Legacy phone	PBX	ISDN	LSC	AS-SIP	Softswitch	AS-SIP	Softswitch	AS-SIP	LSC	SIP	IP phone
2N	Legacy phone	PBX	ISDN	LSC	AS-SIP	Softswitch	AS-SIP	Softswitch	AS-SIP	LSC	H.323, Prop.	IP phone
2O	Legacy phone	PBX	ISDN	LSC	AS-SIP	Softswitch	AS-SIP	Softswitch	SIP			IP phone
2P	Legacy phone	PBX	ISDN	LSC	AS-SIP	Softswitch	AS-SIP	Softswitch	H.323, Prop.			IP phone
2Q	Legacy phone	EO	ISDN	LSC	AS-SIP	Softswitch	AS-SIP	Softswitch	AS-SIP	LSC	SIP	IP phone
2R	Legacy phone	EO	ISDN	LSC	AS-SIP	Softswitch	AS-SIP	Softswitch	AS-SIP	LSC	H.323, Prop.	IP phone
2S	Legacy phone	EO	ISDN	LSC	AS-SIP	Softswitch	AS-SIP	Softswitch	SIP			IP phone
2T	Legacy phone	EO	ISDN	LSC	AS-SIP	Softswitch	AS-SIP	Softswitch	H.323, Prop.			IP phone

5.3.4.14.1.3 IP-to-TDM Calls Over an IP Backbone

Figure 5.3.4-33, IP-to-TDM Call over an IP Backbone, depicts the basic signaling elements in an IP-to-TDM call flow in which the Softswitch (shown to the right of the IP backbone) assumes the role of a terminating IP/TDM signaling gateway. The terminating IP/TDM signaling gateway will conduct translation between SIP and the corresponding TDM signaling.

The Softswitch to the left of the IP backbone operates as a SIP B2BUA or call stateful SIP proxy server when forwarding the SIP messages from a LSC or a SIP endpoint. Refer to Table 5.3.4-17 for Reference Case #3a.

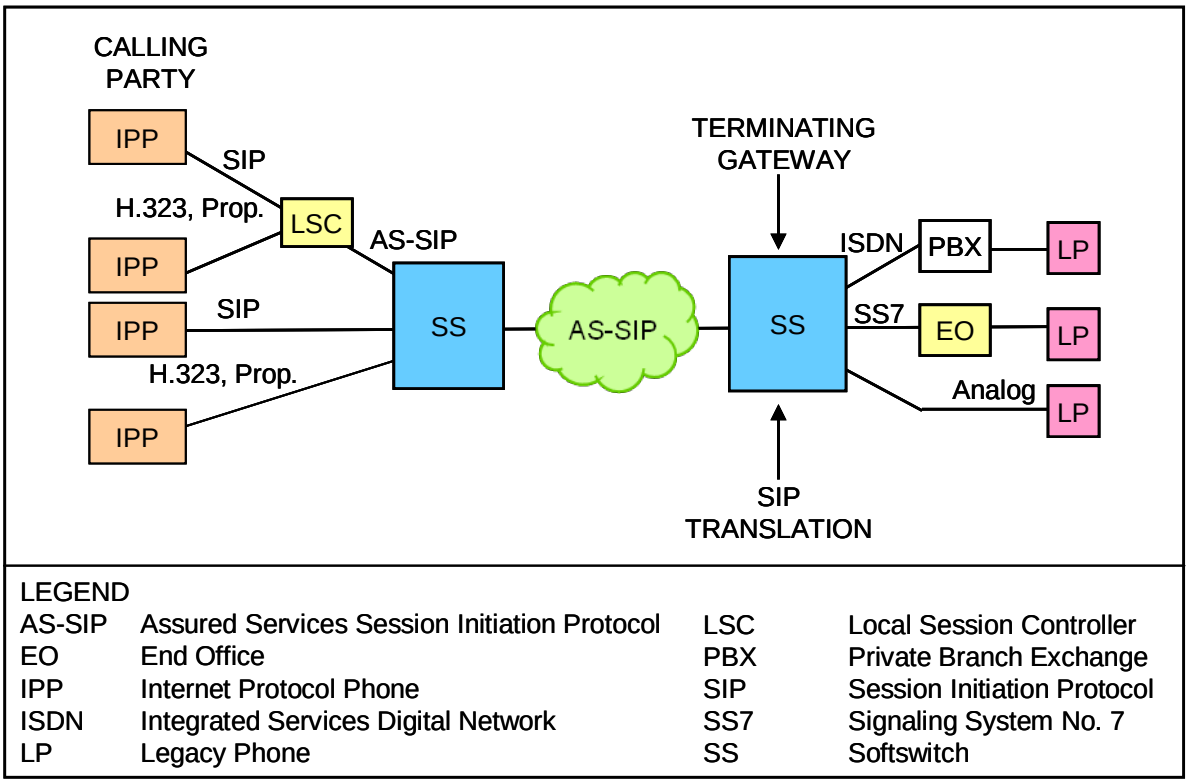


Figure 5.3.4-33. IP-to-TDM Call over an IP Backbone

Table 5.3.4-17. Reference Case #3a – IP-to-TDM Call over an IP Backbone

3A	IP phone	SIP	LSC	AS-SIP	Softswitch	AS-SIP	Softswitch	ISDN	PBX	Legacy phone
3B	IP phone	SIP	LSC	AS-SIP	Softswitch	AS-SIP	Softswitch	CCS7	EO	Legacy phone
3C	IP phone	SIP	LSC	AS-SIP	Softswitch	AS-SIP	Softswitch	Analog		Legacy phone
3D	IP phone	H.323/Prop.	LSC	AS-SIP	Softswitch	AS-SIP	Softswitch	ISDN	PBX	Legacy phone
3E	IP phone	H.323/Prop.	LSC	AS-SIP	Softswitch	AS-SIP	Softswitch	CCS7	EO	Legacy phone
3F	IP phone	H.323/Prop.	LSC	AS-SIP	Softswitch	AS-SIP	Softswitch	Analog		Legacy phone
3G	IP phone	SIP			Softswitch	AS-SIP	Softswitch	ISDN	PBX	Legacy phone
3H	IP phone	SIP			Softswitch	AS-SIP	Softswitch	CCS7	EO	Legacy phone
3I	IP phone	SIP			Softswitch	AS-SIP	Softswitch	Analog		Legacy phone
3J	IP phone	H.323/Prop.			Softswitch	AS-SIP	Softswitch	ISDN	PBX	Legacy phone
3K	IP phone	H.323/Prop.			Softswitch	AS-SIP	Softswitch	CCS7	EO	Legacy phone
3L	IP phone	H.323/Prop.			Softswitch	AS-SIP	Softswitch	Analog		Legacy phone

Figure 5.3.4-34 depicts the basic signaling elements in an IP-to-TDM call flow in which the LSC (shown to the right of the IP backbone) assumes the role of a terminating IP/TDM signaling gateway. The terminating IP/TDM signaling gateway will conduct translation between SIP and the corresponding TDM signaling.

The Softswitch to the left of the IP backbone operates as a SIP B2BUA or call stateful SIP proxy server when forwarding the SIP messages from a LSC or a SIP endpoint. Refer to Table 5.3.4-18 for Reference Case #3b.

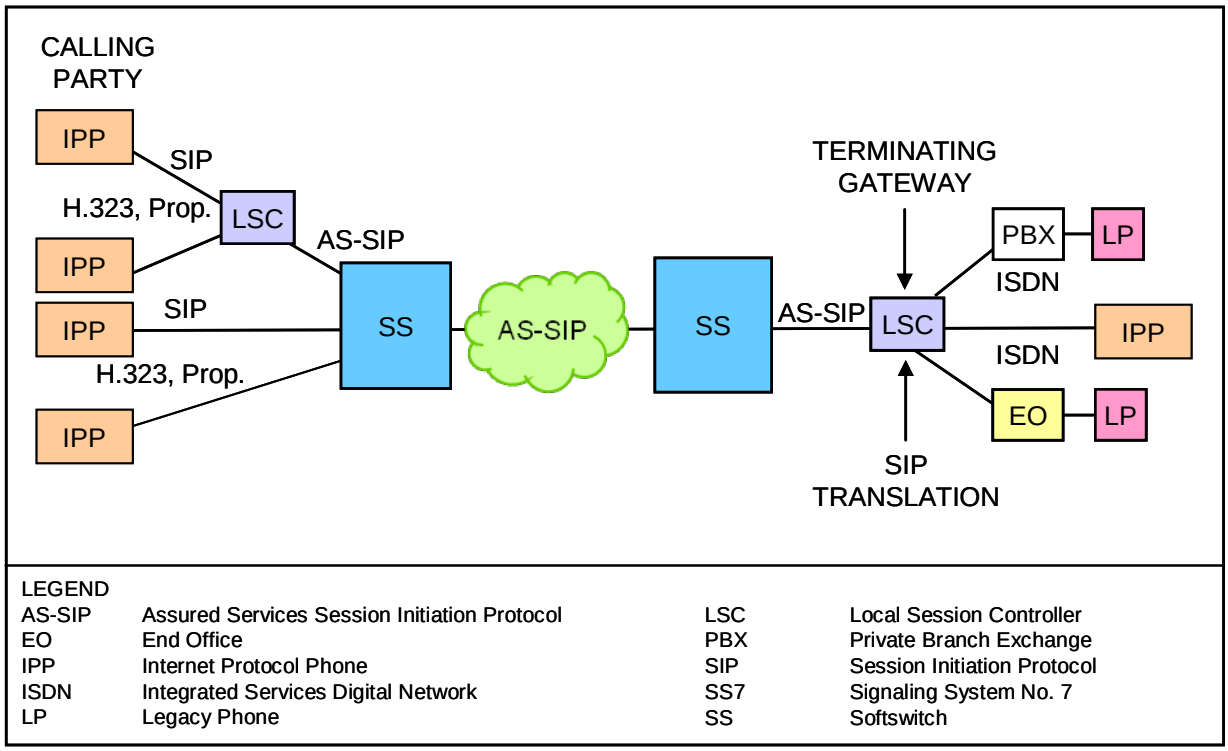


Figure 5.3.4-34. IP-to-TDM Call Translated at Destination Enclave

Table 5.3.4-18. Reference Case #3b – IP-to-TDM Call Translated at Destination Enclave

3M	IP phone	SIP	LSC	AS-SIP	Softswitch	AS-SIP	Softswitch	AS-SIP	LSC	ISDN	PBX	Legacy phone
3N	IP phone	SIP	LSC	AS-SIP	Softswitch	AS-SIP	Softswitch	AS-SIP	LSC	ISDN	EO	Legacy phone
3O	IP phone	H.323/Prop.	LSC	AS-SIP	Softswitch	AS-SIP	Softswitch	AS-SIP	LSC	ISDN	PBX	Legacy phone
3P	IP phone	H.323/Prop.	LSC	AS-SIP	Softswitch	AS-SIP	Softswitch	AS-SIP	LSC	ISDN	EO	Legacy phone
3Q	IP phone	SIP			Softswitch	AS-SIP	Softswitch	AS-SIP	LSC	ISDN	PBX	Legacy phone
3R	IP phone	SIP			Softswitch	AS-SIP	Softswitch	AS-SIP	LSC	ISDN	EO	Legacy phone
3S	IP phone	H.323/Prop.			Softswitch	AS-SIP	Softswitch	AS-SIP	LSC	ISDN	PBX	Legacy phone
3T	IP phone	H.323/Prop.			Softswitch	AS-SIP	Softswitch	AS-SIP	LSC	ISDN	EO	Legacy phone

5.3.4.14.2 Summary Description of the Three Call Types

5.3.4.14.2.1 TDM Bridging

Both end instruments are TDM but the call traverses an IP network.

Bearer: TDM to IP to TDM
Signaling: ISUP to AS-SIP to ISUP

Originating Gateway (O-IWU)

Receives IAM from CCS7 network, creates INVITE, maps between ISUP IAM parameters and SIP headers, and sends INVITE onto the IP network.

Receives AS-SIP messages, creates corresponding ISUP messages, translates SIP headers of AS-SIP messages to ISUP parameters, and sends the ISUP message onto the CCS7 network.

Terminating Gateway (I-IWU)

Receives INVITE, creates IAM, translates SIP headers of INVITE to IAM parameter fields, processes IAM in accordance with standard ISUP procedures, and sends the IAM onto the CCS7 network.

Receives ISUP messages from the CCS7 network (e.g., ACM, ANM, CPG, CON, REL, RLC) that are sent in the backward direction and associated with a previously received INVITE, creates the appropriate AS-SIP messages, maps the necessary info from the ISUP message to the SIP headers, and sends the AS-SIP message onto the IP network.

5.3.4.14.2.2 TDM-to-IP Call

Originator is a TDM end instrument and destination is an IP end instrument.

Bearer: TDM to IP, IP to TDM
Signaling: ISUP to AS-SIP

Originating Gateway (O-IWU)

Receives IAM from CCS7 network, creates INVITE, maps between ISUP IAM parameters and SIP headers, and sends INVITE onto the IP network.

Receives AS-SIP requests and responses including 1XX, 200 OK, 202 Accepted, 3XX, 4XX, 5XX, 6XX, BYE, etc, maps the AS-SIP request/response to an ISUP message, and sends the ISUP message onto the CCS7 network.

5.3.4.14.2.3 IP-to-TDM Call

The Originator is an IP end instrument and the destination is a TDM end instrument.

Bearer: IP to TDM, TDM to IP
Signaling: AS-SIP to ISUP

Terminating Gateway (I-IWU)

Receives INVITE, maps INVITE header fields to IAM parameters, and sends IAM onto CCS7 network.

Receives ISUP messages from the CCS7 network (e.g., ACM, ANM, CPG, CON, REL, RLC), maps ISUP messages and fields to AS-SIP messages and header fields, and sends AS-SIP messages onto IP network.

5.3.4.14.3 SIP URI and Mapping of Telephony Number into SIP URI

5.3.4.14.3.1 **[FY2008]** Any telephone number translated by an interworking AS-SIP signaling appliance from ISUP [or Q.931] parameters to fields in SIP headers MUST be represented as a SIP URI per UCR 2008, Section 5.3.4.7.6, SIP URI and Mapping of Telephony Number into SIP URI.

5.3.4.14.3.2 **[FY2008]** When an interworking AS-SIP signaling appliance receives a TDM call request to be translated into an AS-SIP INVITE in which the dialed number is from the DSN worldwide numbering plan then the AS-SIP signaling appliance MUST ensure that the userinfo part of the SIP URI in the Request-URI field of the INVITE is the complete 10-digit DSN number.

5.3.4.14.3.2.1 **[FY2008]** In the event the dialed number in the ISUP (or Q.931) parameter is a DSN number having fewer than the full 10-digits then the inter-working AS-SIP signaling appliance MUST prepend the three (3) area code digits (KXX) of the AS-SIP signaling appliance's local area code to create the full 10-digit DSN number.

5.3.4.14.3.2.2 The SIP URI MUST have a "user=phone" field appended to the URI.

5.3.4.14.3.2.3 The 10-digit DSN number MAY be followed by a phone-context descriptor consisting of a domain name (per RFC 3966).

5.3.4.14.3.3 When an interworking AS-SIP signaling appliance receives a TDM call request to be translated into an AS-SIP INVITE in which a telephone number translated by the interworking AS-SIP signaling appliance is a PSTN number, then, whenever possible, the userinfo part of the SIP URI MUST be represented in global E.164 notation and MUST have a "user=phone" field appended to the URI.

5.3.4.14.3.3.1 When the numbering plan indicator of the Called Party Number has the value signifying ISDN Numbering Plan (Recommendation E.164) and the number is not an emergency number or directory assistance number or other service code then:

5.3.4.14.3.3.1.1 If the nature of address indicator is set to National significant number then the originating gateway prepends the country code and generates an E.164 number that is placed after the "+" sign in the userinfo part of the SIP URI.

5.3.4.14.3.3.1.2 If the nature of address indicator is set to Subscriber (i.e. local) number then the originating gateway prepends the country code, area code, city code (if necessary) required to generate an E.164 number that is placed after the "+" sign in the userinfo part of the SIP URI.

NOTE: If for some reason there is insufficient information to generate the E.164 number then the SIP URI will reject the call request. The cause code value for the Release message is 28 Incomplete Address.

5.3.4.14.4 General Requirements for Interworking AS-SIP Signaling Appliances

(Q.1912.5, Section 5.4.3.3, modified to reflect translation but not encapsulation.)

5.3.4.14.4.1 (ITU ISUP only) (Applies to TDM Bridging call type and TDM-IP call type) When an interworking AS-SIP signaling appliance receives an ISUP message having the optional Forward Call Indicators parameter with the IAM segmentation indicator set to "Additional information being sent by unsolicited information message" or the optional Backward Call Indicators parameter with the IAM segmentation indicator set to "Additional information has been received and added to IAM" then the interworking AS-SIP signaling appliance MUST wait for the segmentation message and translate the ISUP message to the appropriate AS-SIP message.

5.3.4.14.5 ISUP Versions

This specification describes the translation and processing applicable to the interoperation of AS-SIP and the ITU-T Q.761-4 (1992) version of ISUP.

This specification also covers the translation and processing applicable to the interoperation of AS-SIP and ANSI ISUP (including ANSI T1.113-2000, Telecordia GR-317, GR-317-CORE, *Switching System Generic Requirements for Call Control Using the Integrated Services Digital Network User Part (ISDNUP)*, GR-394-CORE, *Switching System Generic Requirements for Interexchange Carrier Interconnection (ICI) Using the Integrated Services Digital Network User Part (ISDNUP)*). Differences between the function of the ANSI ISUP and the ITU-T ISUP will be identified in this specification.

5.3.4.14.5.1 Encapsulation of ISUP Messages in AS-SIP Requests/Responses

All ISUP encapsulation has been removed from the appendices.

5.3.4.14.5.2 De-Encapsulation of ISUP Messages from AS-SIP Requests/Responses

All ISUP de-encapsulation has been removed from the appendices.

5.3.4.14.5.3 ISUP Messages that are Never Encapsulated

ISUP messages are never encapsulated.

5.3.4.14.5.4 Tones

5.3.4.14.5.4.1 Media paths controlled by the interworking AS-SIP signaling appliance MUST support the transmission and receipt of DTMF-related named events as set forth in RFC 2833.

5.3.4.14.5.4.2 Media paths controlled by the interworking AS-SIP signaling appliance MAY support the transmission and receipt of standard subscriber line tone events set forth in RFC 2833.

5.3.4.14.5.4.3 When a DTMF digit is transmitted over a media path whose signaling is controlled by an interworking AS-SIP signaling appliance (e.g., Softswitch or LSC controlling a Media Gateway), then:

5.3.4.14.5.4.3.1 If the audio codec is G.711, it is STRONGLY RECOMMENDED that the DTMF-related named events of RFC 2833, Section 3.10 be used.

5.3.4.14.5.4.3.2 If the audio codec is not G.711 then the DTMF-related named events of RFC 2833, Section 3.10 MUST be used.

NOTE: IP end instruments that exchange bearer traffic with a Media Gateway controlled by an interworking AS-SIP signaling appliance will either need to support the transmission and receipt of DTMF-related named events as set forth in RFC 2833 or will require an intermediary device in the bearer plane to perform a conversion between the DTMF tones and the RFC 2833, Section 3.10 DTMF-related named events.

5.3.4.14.6 Translation Requirements for an Interworking AS-SIP Signaling Appliance Operating as an Originating Gateway

5.3.4.14.6.1 General Requirements (Originating Gateway)

5.3.4.14.6.1.1 Originating gateways facing ISUP networks in which overlap dialing is used will implement timers to insure that all digits have been collected before an INVITE is transmitted to the IP network. [RFC 3398]

5.3.4.14.6.1.2 Originating gateways MUST wait until a complete ISUP message is received before sending any corresponding INVITE. [RFC 3398]

5.3.4.14.6.2 TDM Bridging Call Flow and TDM-IP Call Flow Requirements (Originating Gateway)

Originating gateway sends AS-SIP INVITE.

5.3.4.14.6.2.1 As specified in the General Requirements section, all the digits MUST be collected (i.e., a complete address) before the originating gateway is permitted to create the INVITE (i.e., en bloc addressing). [Q.1912.5, Section 7.1]

5.3.4.14.6.2.2 When the originating gateway receives an IAM and the originating gateway is NOT employing precondition signaling for the AS-SIP call request:

5.3.4.14.6.2.2.1 If the continuity check indicator in the Nature of Connection Indicators parameter in the IAM had been set to "continuity check not required" the originating gateway creates an AS-SIP INVITE, promptly sends the INVITE onto the IP network, sets the SIP T1 timer, and sets the ISUP T11 timer.

5.3.4.14.6.2.2.2 If the continuity check indicator in the Nature of Connection Indicators parameter in the IAM had been set to "continuity check required on this circuit" or "continuity check performed on previous circuit" the originating gateway delays sending the INVITE until it receives a Continuity message with the Continuity Indicators parameter set to "*continuity check successful*" (which MUST be received prior to expiration of the ISUP T8 timer). If the ISUP T8 timer expires prior to receiving the Continuity message then the originating gateway does NOT send the INVITE.

5.3.4.14.6.2.3 When the originating gateway receives an IAM and the originating gateway is employing precondition signaling for the AS-SIP call request:

5.3.4.14.6.2.3.1 Originating gateway creates an AS-SIP INVITE with precondition fields in the SDP offer, sends the AS-SIP INVITE onto the IP network, sets the SIP T1 timer, and sets the ISUP T11 timer.

5.3.4.14.6.2.3.2 If the continuity check indicator in the Nature of Connection Indicators parameter in the IAM had been set to "continuity check not required" then when the requested preconditions have been met in the IP network the originating gateway sends the SDP offer or answer confirming that the precondition has been met.

5.3.4.14.6.2.3.3 If the continuity check indicator in the Nature of Connection Indicators parameter in the IAM had been set to "continuity check required on this circuit" or "continuity check performed on previous circuit" then the originating gateway only sends the SDP offer or answer confirming that the precondition has been met when the requested preconditions have been met in the IP network, and a COT message is received with the continuity indicators parameter set to "continuity check successful" prior to the expiration of the ISUP T8 timer.

5.3.4.14.6.2.3.4 If the COT message is received with the Continuity Indicators parameter set to "continuity check failed" or if the ISUP timer T8 expires before receiving the COT message AND the originating gateway has not received a final response to the INVITE then the originating gateway MUST send a CANCEL onto the IP network and a REL with cause value 47 (resource unavailable, unspecified) to the CCS7 network.

5.3.4.14.6.2.3.5 If the COT message is received with the Continuity Indicators parameter set to "continuity check failed" or if the ISUP timer T8 expires before receiving the COT message AND the originating gateway has received a final response to the INVITE then the originating gateway MUST send a BYE with cause value 47 (resource unavailable, unspecified) onto the IP network and a REL with cause value 47 (resource unavailable, unspecified) to the CCS7 network.

Originating Gateway Maps ISUP IAM Parameters to AS-SIP INVITE Headers

<u>Request-URI Field</u> [RFC 3398, Section 8.2.1.1]

5.3.4.14.6.2.4 The Request–URI field MUST be a SIP URI.

5.3.4.14.6.2.5 The Request-URI MUST include the "user=phone" URI parameter.

5.3.4.14.6.2.6 **[Conditional]** If the Forward Call Indicator (FCI) "number translated" bit [i.e., the 'M' bit] is set to 1 indicating that a LNP dip has occurred:

If a Generic Digits parameter is present (a Generic Address Parameter (GAP) in ANSI ISUP):

The Generic Digits (or GAP) value in the form of a SIP URI MUST be placed in the Request-URI field.

An "npdi=yes" field MUST be appended to the SIP URI.

The contents of the Called Party Number (CPN) MUST be copied into an "rn=" field, which is appended to the SIP URI.

If a Generic Digits parameter (or GAP) is NOT present and both the LRN (Location Routing Number) and the dialed number are in the CPN parameter then the dialed number in the form of a SIP URI MUST be placed in the Request-URI field, the "npdi=yes" field MUST be appended, and the LRN copied into a "rn=" field and appended to the Request-URI.

5.3.4.14.6.2.7 If the Forward Call Indicator (FCI) "number translated" bit indicates that a LNP dip has NOT occurred:

The Called Party Number (CPN) in the form of a SIP URI MUST be placed in the Request-URI field.

5.3.4.14.6.2.8 If either the CIP (ANSI) or TNS (ITU-T) parameter is present and has a value then a "cic=" field with the value from the CIP or TNS SHOULD be appended to the SIP URI. The "cic=" parameter MUST be prefixed with the country code of the called party number. For example: CIC "5062" for a US called party number is "+1-5062."

<u>To Header Field</u> [RFC 3398, Section 8.2.1.1]

5.3.4.14.6.2.9 If the Original Called Number (OCN) parameter is present in the IAM then, the telephone number in the OCN parameter, in the form of a SIP URI, SHOULD be placed in the To header field.

5.3.4.14.6.2.10 If the OCN parameter is NOT present then the value of the To header field is the same as the value of the Request-URI field.

<u>From Header Field</u> [Q.1912.5, Section 7.1.3]

5.3.4.14.6.2.11 (ANSI ISUP) If the calling party number field (CIN) is not present in the IAM then the From header field MUST be populated with a SIP URI which consists of a user portion with the value unavailable and the hostname of the originating gateway (e.g., sip:unavailable@DoDgw.com).

5.3.4.14.6.2.12 (ITU-T ISUP) If the calling party number field (CIN) is not present in the IAM and the IAM does not have a Generic Number parameter (ITU ISUP only) then the From header field MUST be populated with a SIP URI which consists of a user portion with the value unavailable and the hostname of the originating gateway (e.g., sip:unavailable@DoDgw.com).

5.3.4.14.6.2.13 (ITU-T ISUP) If the calling party number field (CIN) is not present in the IAM and the IAM has a Generic Number parameter (ITU ISUP only) whose "presentation indicator" field is NOT set to "presentation allowed" then the From header field MUST be populated with a

SIP URI which consists of a user portion with the value unavailable and the hostname of the originating gateway (e.g., sip:unavailable@DoDgw.com).

5.3.4.14.6.2.14 (ITU-T ISUP) If the calling party number field (CIN) is not present in the IAM and the IAM has a Generic Number parameter (ITU ISUP only) whose "presentation indicator" field is set to "presentation allowed" then the From header field MUST be populated with a SIP URI derived from the Generic Number.

5.3.4.14.6.2.15 When the calling party number (CIN) parameter is present and the "presentation indicator" field is set to "presentation allowed":

The From header field MUST be populated either with a SIP URI derived from the calling party number.

The originating gateway MUST include a P-Asserted-Identity header derived from the calling party number in the form of a SIP URI. [RFC 3325] In the case of a DSN number, the PAssertedID-value MUST contain the SIP URI of the calling party whereby the userinfo part includes the full 10-digit DSN number.

5.3.4.14.6.2.16 When the calling party number parameter is present and the "presentation indicator" field is set to "presentation restricted":

The From header field SHOULD be populated with a SIP URI with a display name and username of "Anonymous" (e.g., From: Anonymous <sip:anonymous@anonymous.invalid>).

The originating gateway MAY include a Privacy header field with priv-value = "id." [RFC 3323, RFC 3325, Q.1912.5]

The originating gateway MUST include a P-Asserted-Identity header derived from the calling party number in the form of a SIP URI. [RFC 3325] In the case of a DSN number, the PAssertedID-value MUST contain the SIP URI of the calling party whereby the userinfo part includes the full 10-digit DSN number.

5.3.4.14.6.2.17 When the calling party number parameter is present and the "presentation indicator" field is set to "address unavailable" then the From header field SHOULD be populated with a SIP URI which consists of the hostname of the originating gateway without a user portion. [RFC 3398]

<u>SDP Information</u> [Q.1912.5, Section 7.1.1]

5.3.4.14.6.2.18 Table 5.3.4-19, 26/Q.1912, describes the mapping between the relevant fields in the TMR/USI (Transmission Medium Requirement /User Service Information) parameters and the SDP media description lines when transcoding is not available at the originating gateway. This table is copied on the next page for the reader's convenience.

NOTE: The Transmission Medium Requirement is a mandatory parameter in the ITU-T ISUP IAM but is not present in the ANSI ISUP IAM. There is an optional User Service Information parameter in ITU ISUP and a similar but not identical mandatory User Service Information parameter in the ANSI ISUP IAM).

5.3.4.14.6.2.19 If the originating gateway supports G.711 encoding and transcoding between A-Law and mu-Law:

5.3.4.14.6.2.19.1 If the call is from an A-Law TDM network the originating gateway MUST send an SDP offer with both A-Law (PCMA) and mu-Law (PCMU) in the media description and PCMA takes precedence over PCMU.

5.3.4.14.6.2.19.2 If the call is from a mu-Law TDM network the originating gateway MUST send an SDP offer with mu-Law (PCMU) and optionally A-Law (PCMA) included in the media description and PCMU takes precedence over PCMA.

Originating Gateway Maps ISUP Messages to AS-SIP Messages

[Q.1912.5, Section 7.7.1]

5.3.4.14.6.2.29 If the originating gateway receives a REL from the CCS7 network prior to sending an INVITE to the IP network then the INVITE is NOT sent.

5.3.4.14.6.2.30 If the originating gateway receives a REL from the CCS7 network after sending an INVITE to the IP network but prior to receiving a response then the originating gateway holds the REL until an AS-SIP response is received and,

5.3.4.14.6.2.30.1 If the AS-SIP response does NOT establish a confirmed dialog (2xx) or early dialog (101-199) then the originating gateway sends a CANCEL. A Reason header field containing the (Q.850) Cause Value of the REL SHOULD be included in the CANCEL Request.

NOTE: If the originating gateway receives a 200 OK INVITE after sending the CANCEL, the originating gateway MUST respond with an ACK and then send a BYE request.

Table 5.3.4-19. 26/Q.1912

TMR PARAMETER	USI PARAMETER		HLC IE IN ATP	m= line			b= line	a= line
TMR codes	Information Transport Capability	User Information Layer 1 Protocol Indicator	High Layer Characteristics Identification	<media>	<transport>	<fmt-list>	<modifier>: <bandwidth-value>	rtpmap:<dynamic-PT> <encoding name>/<clock rate>(/encoding parameters>
"speech"	"Speech"	"G.711 mu-Law"	Ignore	Audio	RTP/AVP	0 (and possibly 8)[1]	AS:64	rtpmap:0 PCMU/8000 (and possibly rtpmap:8 PCMA/8000) [1]
"speech"	"Speech"	"G.711 mu-Law"	Ignore	Audio	RTP/AVP	Dynamic PT (and possibly a second Dynamic PT) [1]	AS:64	rtpmap:<dynamic-PT> PCMU/8000 (and possibly rtpmap:<dynamic-PT> PCMA/8000) [1]
"speech"	"Speech"	"G.711 A-Law"	Ignore	Audio	RTP/AVP	8	AS:64	rtpmap:8 PCMA/8000
"speech"	"Speech"	"G.711 A-Law"	Ignore	Audio	RTP/AVP	Dynamic PT	AS:64	rtpmap:<dynamic-PT> PCMA/8000
"3.1 KHz audio"	USI Absent		Ignore	Audio	RTP/AVP	0 and/or 8[1]	AS:64	rtpmap:0 PCMU/8000 and/or rtpmap:8 PCMA/8000[1]
"3.1 KHz audio"	"3.1 KHz audio"	"G.711 mu-Law"	Note 3	Audio	RTP/AVP	0 (and possibly 8) [1]	AS:64	rtpmap:0 PCMU/8000 (and possibly rtpmap:8 PCMA/8000) [1]
"3.1 KHz audio"	"3.1 KHz audio"	"G.711 A-Law"	Note 3	Audio	RTP/AVP	8	AS:64	rtpmap:8 PCMA/8000
"3.1 KHz audio"	"3.1 KHz audio"		"Facsimile Group 2/3"	Image	udptl	t38	AS:64	Based on T.38.
"3.1 KHz audio"	"3.1 KHz audio"		"Facsimile Group 2/3"	Image	tcptl	t38	AS:64	Based on T.38.

TMR PARAMETER	USI PARAMETER		HLC IE IN ATP	m= line			b= line	a= line
"64 kbit/s unrestricted"	"Unrestricted digital inf. W/tone/ann."	N/A	Ignore	Audio	RTP/AVP	9	AS:64	rtpmap:9 G722/8000
"64 kbit/s unrestricted"	"Unrestricted digital information"	N/A	Ignore	Audio	RTP/AVP	Dynamic PT	AS:64	rtpmap:<dynamic-PT> CLEARMODE/8000[2]
"2 x 64 kbit/s unrestricted"	"Unrestricted digital information"	N/A	Ignore	FFS	FFS	FFS	FFS	FFS
"384 kbit/s unrestricted"	"Unrestricted digital information"	N/A	Ignore	FFS	FFS	FFS	FFS	FFS
"1536 kbit/s unrestricted"	"Unrestricted digital information"	N/A	Ignore	FFS	FFS	FFS	FFS	FFS
"1920 kbit/s unrestricted"	"Unrestricted digital information"	N/A	Ignore	FFS	FFS	FFS	FFS	FFS
"N x 64 kbit/s unrestricted" N from 3 to 29	"Unrestricted digital information"	N/A	Ignore	FFS	FFS	FFS	FFS	FFS

[1]Both PCMA and PCMU required under the conditions stated in Q.1912.5, Section 7.1.1.
[2]Since CLEARMODE has not yet been standardized, its use is for further study.
[3]HLC normally absent in this case. It is possible for HLC to be present with the value "Telephony," although clause 6.3.1/Q.939 indicates that this would normally be accompanied by a value of "Speech" for the Information Transfer Capability element.

5.3.4.14.6.2.30.2 If the AS-SIP response does establish either an early dialog or confirmed dialog then the originating gateway sends a BYE request mapping the Cause Indicators parameter to the SIP Reason header.

5.3.4.14.6.2.31 If the originating gateway receives REL from CCS7 network after having received an AS-SIP response that established a confirmed dialog or early dialog then the originating gateway MUST send a BYE request mapping the Cause Indicators parameter to the SIP Reason header.

NOTE: The Protocol field of the Reason header field will be assigned the value "Q.850," the Protocol-cause field will be assigned the cause value from the REL, and the reason-text field will be based on the provisioning of the originating gateway.

[Q.1912.5, Section 7.7.4]

5.3.4.14.6.2.32 When the originating gateway receives a RSC (Reset Circuit message) from the ISUP network:

If the originating gateway receives RSC from the CCS7 network prior to sending an INVITE to the IP network then the INVITE is NOT sent.

5.3.4.14.6.2.33 If the originating gateway receives RSC from the CCS7 network after sending an INVITE to the IP network but prior to receiving a response:

5.3.4.14.6.2.33.1 If the AS-SIP response does NOT establish a confirmed dialog (2xx) or early dialog (101-199) then the originating gateway sends a CANCEL. A Reason header field containing the (Q.850) Cause Value of the REL that is being sent to the ISUP network SHOULD be included in the CANCEL Request.

5.3.4.14.6.2.33.2 If the AS-SIP response does establish either an early dialog or confirmed dialog then the originating gateway sends a BYE request mapping the Cause Indicators parameter to the SIP Reason header.

5.3.4.14.6.2.34 If the originating gateway receives RSC from the CCS7 network after having received an AS-SIP response that established a confirmed dialog or early dialog then the originating gateway MUST send a BYE request mapping the Cause Indicators parameter to the SIP Reason header.

[Q.1912.5, Section 7.7.4]

5.3.4.14.6.2.35 When the originating gateway receives a GRS (Circuit Group Reset message) from the ISUP network:

If the originating gateway receives GRS from the CCS7 network prior to sending an INVITE to the IP network then the INVITE is NOT sent.

5.3.4.14.6.2.36 If the originating gateway receives GRS from the CCS7 network after sending an INVITE to the IP network but prior to receiving a response:

5.3.4.14.6.2.36.1 If the AS-SIP response does NOT establish a confirmed dialog (2xx) or early dialog (101-199) then the originating gateway sends a CANCEL. A Reason header field containing the (Q.850) Cause Value of the REL that is being sent to the ISUP network SHOULD be included in the CANCEL Request.

5.3.4.14.6.2.36.2 If the AS-SIP response does establish either an early dialog or confirmed dialog then the originating gateway sends a BYE request mapping the Cause Indicators parameter to the SIP Reason header.

5.3.4.14.6.2.37 If the originating gateway receives GRS from the CCS7 network after having received a response that established a confirmed dialog or early dialog then the originating gateway MUST send a BYE request mapping the Cause Indicators parameter to the SIP Reason header.

NOTE: One SIP message MUST be sent for each call affected by the GRS.

[Q.1912.5, Section 7.7.4]

5.3.4.14.6.2.38 When the originating gateway receives a CGB (Circuit Group Blocking message) with the Circuit Group Supervision Message Type indicator set to “hardware failure oriented” from the ISUP network:

If the originating gateway receives CGB from the CCS7 network prior to sending an INVITE to the IP network then the INVITE is NOT sent.

5.3.4.14.6.2.39 If the originating gateway receives a CGB (Circuit Group Blocking message) with the Circuit Group Supervision Message Type indicator set to “hardware failure oriented” from the ISUP network after sending an INVITE to the IP network but prior to receiving a response:

5.3.4.14.6.2.39.1 If the AS-SIP response does NOT establish a confirmed dialog (2xx) or early dialog (101-199) then the originating gateway sends a CANCEL. A Reason header field

containing the (Q.850) Cause Value of the REL that is being sent to the ISUP network SHOULD be included in the CANCEL Request.

5.3.4.14.6.2.39.2 If the AS-SIP response does establish either an early dialog or confirmed dialog then the originating gateway sends a BYE request mapping the Cause Indicators parameter to the SIP Reason header.

5.3.4.14.6.2.40 If the originating gateway receives a CGB (Circuit Group Blocking message) with the Circuit Group Supervision Message Type indicator set to "hardware failure oriented" from the ISUP network after having received an AS-SIP response that established a confirmed dialog or early dialog then the originating gateway MUST send a BYE request mapping the Cause Indicators parameter to the SIP Reason header.

NOTE: One SIP message MUST be sent for each call affected by the CGB.

Autonomous Release by Originating Gateway

[Q1912.5, Section 7.7.3]

5.3.4.14.6.2.41 Table 5.3.4-20, 37/Q.1912.5, details the events that trigger an autonomous release by the originating gateway resulting in the transmission of a CANCEL or BYE to the IP network and a REL to the CCS7 network.

Table 5.3.4-20. 37/Q.1912.5

REL ← CAUSE INDICATORS PARAMETER	TRIGGER EVENT	→ SIP
As determined by ISUP procedure.	COT received with the Continuity Indicators parameter set to "continuity check failed" (ISUP only) or the ISUP timer T8 expires.	Send CANCEL or BYE according to the rule described in section titled OG Mapping of ISUP REL Message to SIP Message.
REL with cause value 47 (resource unavailable, unspecified).	Internal resource reservation unsuccessful	As determined by SIP procedure
As determined by ISUP procedure.	ISUP procedures result in generation of autonomous REL on ISUP side.	CANCEL or BYE according to the rule described in section titled OG Mapping of ISUP REL Message to SIP Message.
Depending on the SIP release reason.	SIP procedures result in a decision to release the call.	As determined by SIP procedure.

5.3.4.14.6.2.42 A Reason header field containing the (Q.850) Cause Value of the REL SHOULD be included in the BYE request or CANCEL request.

Originating Gateway Maps AS-SIP Messages to ISUP Messages

180 Ringing [Q.1912.5, Section 7.3.1]

5.3.4.14.6.3.3 When an originating gateway receives a Ringing response:

The originating gateway MUST stop the ISUP T11 timer.

The originating gateway will use its standard ISUP procedures to determine whether to send an ACM or CPG over the ISUP network.

In the case of the ACM the called party's status indicator of the Backward Call Indicators (BCI) is set to "subscriber free" (bit DC 01).

In the case of the ACM for a call that originates in a SIP mobile network the Interworking indicator of the BCI is set to "interworking encountered" (bit I 1).

In the case of the ACM for a call that originates in a SIP mobile network the ISUP indicator of the BCI is set to "ISUP not used all the way" (bit K 0).

In the case of the ACM for a call that originates in a SIP mobile network the ISDN access indicator of the BCI is set to "terminating access non-ISDN" (bit M 0).

In the case of the CPG the Event indicator of the Event information parameter is set to "alerting" (GFEDCBA 000001).

The originating gateway transmits a ringing tone on the TDM bearer circuit to the caller.

<u>183 Session Progress</u> [Q.1912.5, Section 7.3.2]

5.3.4.14.6.3.4 If 183 Session progress is received then the originating gateway MUST NOT send an ISUP message onward over the ISUP network.

<u>200 OK INVITE</u> [Q,1912.5, Section 7.5]

5.3.4.14.6.3.5 When an originating gateway receives a 200 OK INVITE:

The originating gateway MUST stop the ISUP timer T11.

(ITU ISUP) The originating gateway will use its standard ISUP procedures to determine whether to send an ANM or CON over the ISUP network.

NOTE: The CON is an ITU ISUP message (not used in ANSI ISUP) indicating that sufficient information has been received and that the called subscriber has answered. It serves as both an ACM and an ANM.

(ANSI ISUP) The originating gateway will send an ANM over the ISUP network.

The originating gateway will terminate the ringing tone to the calling party.

(ITU ISUP) If the originating gateway creates a CON message then the called party's status indicator of the Backward Call indicators is set to "no indication" (bit DC 00) and if the call originates in a SIP mobile network then the Interworking indicator of the BCI is set to "interworking encountered" (bit I 1), the ISUP indicator of the BCI is set to "ISUP not used all the way" (bit K 0), and the ISDN access indicator of the BCI is set to "terminating access non-ISDN" (bit M 0).

<u>BYE</u> [Q.1912.5, Section 7.7.2]

5.3.4.14.6.3.6 When the originating gateway receives a BYE:

The originating gateway creates a REL to send over the ISUP network.

If the BYE includes a Reason header field with Q.850 cause value then the Q.850 cause value MAY be mapped to the cause value of the cause indication parameter of the REL and the location field of the cause indication parameter is assigned "network beyond interworking point."

If the cause value is not available from the Reason header field then Cause value No. 16 ("normal clearing") is placed in the Cause Indicators parameter of the REL.

<u>4XX, 5XX, 6XX</u> [Q.1912.5, Section 7.7.6]

5.3.4.14.6.3.7 When the originating gateway receives a 4XX, 5XX, 6XX response to the INVITE then:

If a Reason header field with Q.850 cause value is present then the Q.850 cause value SHOULD be mapped to the cause value of the cause indication parameter of the REL and the location field of the cause indication parameter is assigned "network beyond interworking point."

Otherwise the 4XX, 5XX, 6XX response code is mapped to the REL ISUP cause value in accordance with Table 5.3.4-21, 40/Q.1912.5, which is copied below for the reader's convenience.

Table 5.3.4-21. 40/Q.1912.5

←REL (CAUSE VALUE)	←4XX/5XX/6XX SIP MESSAGE	REMARKS
127 Interworking	400 Bad Request	
127 Interworking	401 Unauthorized	Note 1
127 Interworking	402 Payment Required	
127 Interworking	403 Forbidden	
1 Unallocated number	404 Not Found	
127 Interworking	405 Method Not Allowed	
127 Interworking	406 Not Acceptable	
127 Interworking	407 Proxy authentication Required	Note 1
127 Interworking	408 Request Timeout	
22 Number changed (without diagnostic)	410 Gone	
127 Interworking	413 Request Entity Too Long	Note 1
127 Interworking	414 Request-uri Too Long	Note 1
127 Interworking	415 Unsupported Media Type	Note 1
127 Interworking	416 Unsupported URI Scheme	Note 1
127 Interworking	420 Bad Extension	Note 1
127 Interworking	421 Extension Required	Note 1
127 Interworking	423 Interval Too Brief	
20 Subscriber absent	480 Temporarily Unavailable	
127 Interworking	481 Call/Transaction Does Not Exist	
127 Interworking	482 Loop Detected	
127 Interworking	483 Too Many Hops	
28 Invalid Number format	484 Address Incomplete	Note 1
127 Interworking	485 Ambiguous	
17 User busy	486 Busy Here	
127 Interworking or no mapping (Note 3)	487 Request Terminated	Note 2
127 Interworking	488 Not Acceptable Here	
No mapping	491 Request Pending	Note 2
127 Interworking	493 Undecipherable	
127 Interworking	500 Server Internal Error	
127 Interworking	501 Not Implemented	
127 Interworking	502 Bad Gateway	
127 Interworking	503 Service Unavailable	Note 1
127 Interworking	504 Server Timeout	
127 Interworking	505 Version Not Supported	Note 1
127 Interworking	513 Message Too Large	Note 1
127 Interworking	580 Precondition Failure	Note 1
17 User busy	600 Busy Everywhere	
21 Call rejected	603 Decline	

←REL (CAUSE VALUE)	←4XX/5XX/6XX SIP MESSAGE	REMARKS
1 Unallocated number	604 Does Not Exist Anywhere	
127 Interworking	606 Not Acceptable	
Note 1 – this response may be handled entirely on the SIP side; if so, it is not interworked. Note 2 – this response does not terminate a SIP dialog, but only a specific transaction within it. Note 3 – No mapping if the O-IWU previously issued a CANCEL request for the INVITE.		

5.3.4.14.7 Translation Requirements for Interworking AS-SIP Signaling Appliance Operating as a Terminating Gateway

5.3.4.14.7.1 General Requirements

5.3.4.14.7.1.1 The terminating gateway MUST include a To tag in the first backward non-100 provisional response, in order to establish an early dialog. [Q.1912.5, Section 6]

5.3.4.14.7.2 TDM Bridging and IP-TDM Call Flow Requirements (Terminating Gateway)

Terminating Gateway Receives AS-SIP INVITE

5.3.4.14.7.2.1 When the terminating gateway receives an INVITE from the IP network, the terminating gateway MUST ensure that a complete telephone number has been received in the INVITE before an IAM is transmitted to the ISUP network.

[Q1912.5, Sections 6.1.1 and 6.1.2]

5.3.4.14.7.2.2 When the terminating gateway receives an INVITE with a complete telephone number for purposes of routing to the ISUP network, and the INVITE does not include an SDP offer:

5.3.4.14.7.2.2.1 In compliance with AS-SIP GSS Requirement 8.1.1.14 the INVITE MUST indicate support for reliable provisional responses (e.g., INVITE has Require header field or Support header field with option tag 100rel) in which case:

5.3.4.14.7.2.2.1.1 If the call is to be routed over an A-Law TDM network, the terminating gateway MUST send a 183 Session progress response having a SDP offer with A-Law (PCMA) and mu-Law (PCMU) in the media description (assuming terminating gateway supports G.711 encoding) with A-Law (PCMA) having precedence over mu-Law (PCMU).

5.3.4.14.7.2.2.1.2 If the call is to be routed over a mu-Law TDM network, the terminating gateway MUST send a 183 Session progress response having a SDP offer with mu-Law (PCMU)

in the media description and MAY optionally include A-Law (PCMA) and mu-Law (PCMU) will take precedence over A-Law (PCMA) if present (assuming terminating gateway supports G.711 encoding and transcoding between A-Law and mu-Law).

5.3.4.14.7.2.2.1.3 If SIP preconditions are not being used for this call request, the terminating gateway MUST send the IAM when it receives the SDP answer with media description.

5.3.4.14.7.2.2.1.4 If SIP precondition signaling is being used AND the subsequent ISUP network supports continuity checking, the terminating gateway will immediately send out the IAM and set the continuity check indicator in the Nature of Connections Indicator parameter to "continuity check performed on previous circuit" or "continuity check required on this circuit" (if COT check to be performed on outgoing circuit).

5.3.4.14.7.2.2.1.5 If SIP precondition signaling is being used AND the subsequent ISUP network does not support continuity checking, the terminating gateway will defer sending the IAM until all preconditions are met.

5.3.4.14.7.2.2.2 If, in violation of Requirement 5.3.4.7.1.1.14, the INVITE does not include a Supported header with the option tag '100rel', the terminating gateway MUST immediately send out the IAM over the ISUP network.[1]

5.3.4.14.7.2.3 When the terminating gateway receives an INVITE with a complete telephone number for purposes of routing to the ISUP network, and the INVITE includes an SDP offer:

5.3.4.14.7.2.3.1 If the terminating gateway operates as an international gateway and employs G.711 encoding:

5.3.4.14.7.2.3.1.1 If the call is going onto an A-Law TDM network, the terminating gateway MUST delete the mu-Law media description if present from the SDP answer in the first non-failure provisional response it sends back in response to receipt of the INVITE.

5.3.4.14.7.2.3.1.2 If the call is going onto n mu-Law TDM network and both A-Law and mu-Law were present in the offer then the terminating gateway MUST delete the A-Law from the media description from the SDP answer in the first non-failure provisional response it sends back in response to receipt of the INVITE.

5.3.4.14.7.2.3.2 If SIP preconditions are not being used then the terminating gateway MUST immediately send the IAM onto the ISUP network.

[1] The first non-failure provisional response sent by the terminating gateway MUST include an sdp offer.

5.3.4.14.7.2.3.3 If SIP precondition signaling is being used AND the subsequent ISUP network supports continuity checking, the terminating gateway will immediately send out the IAM and set the continuity check indicator in the Nature of Connections Indicator parameter to "continuity check performed on previous circuit" or "continuity check required on this circuit" (if COT check to be performed on outgoing circuit).

5.3.4.14.7.2.3.4 If SIP precondition signaling is being used, AND the subsequent ISUP network does not support continuity checking, the terminating gateway will defer sending the IAM until all preconditions are met.

5.3.4.14.7.2.3.4.5 The first non-failure provisional response sent by the terminating gateway MUST include an sdp answer.

Terminating Gateway Maps AS-SIP INVITE Headers to ISUP IAM Parameters

Called Party Number [RFC 3398, Section 7.2.1.1]

5.3.4.14.7.2.4 When the terminating gateway receives an AS-SIP INVITE:

5.3.4.14.7.2.4.1 If there is no "npdi=yes" field within the Request-URI, then the telephone number in the userinfo part of the SIP URI MUST be converted to ISUP format and placed in the Called Party Number (CPN) parameter.

5.3.4.14.7.2.4.2 **[Conditional]** If there is a "npdi=yes" field within the Request-URI field, but no "rn=" field, then the telephone number of the userinfo part of the SIP URI of the Request-URI field MUST be converted to ISUP format and placed in the CPN parameter.

5.3.4.14.7.2.4.3 **[Conditional]** If there is a "npdi=yes" field within the Request-URI and a "rn=" field then the telephone number in the "rn=" field MUST be converted to ISUP format and placed in the CPN parameter. The telephone number in the Request-URI field MUST be converted to ISUP format and placed in the Generic Digits (GAP) parameter.

5.3.4.14.7.2.5 If the primary telephone number in the Request-URI and that of the To header are at variance, then the To header SHOULD be used to populate an OCN parameter. Otherwise the To header field SHOULD be ignored. [RFC 3398]

5.3.4.14.7.2.6 If the "cic=" parameter is present in the Request-URI, then if local policy supports transmission of the Carrier Identification Code in the IAM then terminating gateway policy determines whether the CIC is carried in the CIP or TNS parameter.

5.3.4.14.7.2.7 The information contained in the INVITE Request-URI field, specifically the telephone number in the userinfo part of the SIP URI, MUST be converted to ISUP format and placed in the Called Party Number parameter.

5.3.4.14.7.2.8 If the number in the Request-URI field being converted to ISUP format is a global E.164 number, the NoA indicator is set to "International number" and the Numbering plan indicator is set to "ISDN numbering plan (Recommendation E.164)."

5.3.4.14.7.2.9 If the number in the Request-URI field being converted to ISUP format belongs to the DSN worldwide numbering plan then NoA indicator is set to "Subscriber number" and Numbering plan indicator is set to "Private numbering plan."

5.3.4.14.7.2.10 If the number in the Request-URI field being converted to ISUP format is a national number then NoA indicator is set to "National significant number" and the numbering plan indicator is set to "ISDN numbering plan (Recommendation E.164)".

NOTE: This case SHOULD NOT occur because AS-SIP signaling appliances that receive a call request from a served IP end instrument intended for the PSTN MUST convert nationally significant numbers to international E.164 numbers.

<u>Calling Party's Category</u> [Q.1912.5, Section 6.1.3.2]

5.3.4.14.7.2.11 The calling party's category is set to "calling party's category unknown" (bit 0000 0000).

<u>Nature of Connection Indicators</u> [Q.1912.5, Section 6.1.3.3]

5.3.4.14.7.2.12 The satellite indicator SHOULD be set to "One satellite circuit in the connection" (bit BA 01).

5.3.4.14.7.2.13 The continuity check indicator SHOULD be set to "Continuity check not required" (bit DC 00) if there is no pending precondition request.

5.3.4.14.7.2.14 The continuity check indicator SHOULD be set to "Continuity check performed on a previous circuit" (bit DC 10) if there is a pending precondition request.

5.3.4.14.7.2.15 The echo control device indicator SHOULD be set to "outgoing echo control device included" (bit E 1) if the INVITE is from a mobile network.

<u>Forward Call Indicators</u> [Q.1912.5, Section 6.1.3.4]

5.3.4.14.7.2.16 The interworking indicator SHOULD be set to “Interworking encountered” (bit D 1).

5.3.4.14.7.2.17 The ISUP indicator SHOULD be set to “ISUP not used all the way” (bit F 0).

5.3.4.14.7.2.18 The ISUP preference indicator SHOULD be set to “ISUP not required all the way” (bit HG 01) unless the INVITE is from a mobile network in which case the ISUP preference indicator will be set in accordance with local policy.

5.3.4.14.7.2.19 The ISDN access indicator SHOULD be set to “Originating access non-ISDN” (bit I 0).

<u>USI/TMR (User Service Information / Transmission Medium Requirement)</u> [Q.1912.5, Section 6.1.3.5]

5.3.4.14.7.2.20a (ITU ISUP only) If the call originates from a mobile IP network, the TMR parameter MUST be set to 3.1 kHz audio, the optional USI parameter is NOT sent, and transcoding is applied when required.

5.3.4.14.7.2.21 (ANSI ISUP only) If the call originates from a mobile IP network, the Information transfer capability of the USI parameter MUST be set to 3.1 kHz Audio.

5.3.4.14.7.2.22 (ITU ISUP) If the call does not originate from a mobile network and the SDP is received by the terminating gateway before the IAM is sent and if transcoding between A-Law and mu-Law is not supported by the terminating gateway, the values for the mandatory TMR parameter and the optional USI parameter will be derived from the SDP as detailed below in Table A-4, 6/Q1912.5, which is copied on the next page for the reader’s convenience.

5.3.4.14.7.2.23 (ITU ISUP) If the call does not originate from a mobile network and the SDP is received by the terminating gateway after the IAM is sent, the bearer service values defined by the mandatory TMR parameter and the optional USI parameter will be set in accordance with local policy.

5.3.4.14.7.2.24 (ITU ISUP) If the call does not originate from a mobile network and if transcoding between A-Law and mu-Law is supported by the terminating gateway, the bearer service values defined by the mandatory TMR parameter and the optional USI parameter will be set in accordance with local policy.

5.3.4.14.7.2.25 (ANSI ISUP) If the call does not originate from a mobile network and the SDP is received by the terminating gateway before the IAM is sent and if transcoding between A-Law and mu-Law is not supported by the terminating gateway, the values for the mandatory USI

parameter will be derived from the SDP as detailed below in Table 5.3.4-22, 6/Q.1912.5, which is copied on the next page for the reader's convenience.

5.3.4.14.7.2.26 (ANSI ISUP) If the call does not originate from a mobile network and the SDP is received by the terminating gateway after the IAM is sent, the bearer service values defined by the mandatory TMR parameter and the optional USI parameter will be set in accordance with local policy.

5.3.4.14.7.2.27 (ANSI ISUP) If the call does not originate from a mobile network and if transcoding between A-Law and mu-Law is supported by the terminating gateway, the bearer service values defined by the mandatory TMR parameter and the optional USI parameter will be set in accordance with local policy.

5.3.4.14.7.2.28 (ITU ISUP) If the terminating gateway is an international gateway and the audio coding is G.711, and the incoming call is treated as an ISDN originated call, the User Information Layer 1 Protocol indicator of the optional USI parameter MUST be set in accordance with the encoding law (i.e., A-Law or mu-Law) of the succeeding CCS7 network.

5.3.4.14.7.2.29 (ANSI ISUP) If the terminating gateway is an international gateway and the audio coding is G.711, and the incoming call is treated as an ISDN originated call, the User Information Layer 1 Protocol indicator of the mandatory USI parameter MUST be set in accordance with the encoding law (i.e., A-Law or mu-Law) of the succeeding CCS7 network.

Calling Party Number [Q.1912.5, Section 6.1.3.6]

5.3.4.14.7.2.30 When the terminating gateway receives the AS-SIP INVITE:

5.3.4.14.7.2.30.1 If the From header field does not have a SIP URI with a telephone number for the user part of the URI, AND if there is no P-Asserted-Identity header[2] or a P-Asserted-Identity header that does not have a SIP URI with a telephone number for the user part of the URI, the terminating gateway SHOULD omit the Calling Party Number parameter from the IAM.

[2] The presence of a P-Asserted-Identity header is mandated by AS-SIP GSS Requirement 5.3.4.7.1.1.23.

Table 5.3.4-22. 6/Q.1912.5

	M= LINE		B= LINE	A= LINE	TMR PARAMETER	USI PARAMETER[3]		HLC PARAMETER
<media>	<transport>	<fmt-list>	<modifier>: <bandwidth-value>	rtpmap:<dynamic-PT> <encoding name>/<clock rate>(/encoding parameters>	TMR codes	Information Transport Capability	User Information Layer 1 Protocol Indicator	High Layer Characteristics Identification
			NOTE – <bandwidth value> for <modifier> of AS is evaluated to be B kbit/s.					
audio	RTP/AVP	0	N/A or up to 64 kbit/s	N/A	"3.1KHz audio"	"3.1KHz audio"	"G.711[1] mu-Law"	Note 3
audio	RTP/AVP	Dynamic PT	N/A or up to 64 kbit/s	rtpmap:<dynamic-PT> PCMU/8000	"3.1KHz audio"	"3.1KHz audio"	"G.711[1] mu-Law"	Note 3
audio	RTP/AVP	8	N/A or up to 64 kbit/s	N/A	"3.1KHz audio"	"3.1KHz audio"	"G.711[1] A-Law"	Note 3
audio	RTP/AVP	Dynamic PT	N/A or up to 64 kbit/s	rtpmap:<dynamic-PT> PCMA/8000	"3.1KHz audio"	"3.1KHz audio"	"G.711[1] A-Law"	Note 3
audio	RTP/AVP	9	AS:64 kbit/s	rtpmap:9 G722/8000	"64 kbit/s unrestricted"	"Unrestricted digital inf. w/tones/ann"		
audio	RTP/AVP	Dynamic PT	AS:64 kbit/s	rtpmap:<dynamic-PT> CLEARMODE/8000[2]	"64 kbit/s unrestricted"	"Unrestricted digital information"		
image	udptl	t38	N/A or up to 64 kbit/s	Based on T.38	"3.1 KHz audio"	"3.1KHz audio"		*"Facsímile Group 2/3"*
image	tcptl	t38	N/A or up to 64 kbit/s	Based on T.38	"3.1 KHz audio"	"3.1KHz audio"		*"Facsímile Group 2/3"*

NOTES
1. In this table, the codec G.711 is used only as an example. Anoher codec is possible.
2. CLEARMODE has not yet been standardized; and its usage is FFS.
3. HLC normally absent in this case. It is possible for HLC to be present with the value "Telephony," although clause 6.3.1/Q.939 indicates that this would normally be accompanied by a value of "Speech" for the Information Transfer Capability element.

5.3.4.14.7.2.30.2 If the From header field does not have a SIP URI with a telephone number for the user part of the URI AND if there is a P-Asserted-Identity header with a SIP URI with a telephone number for the user part of the URI, AND there is either no Privacy header field or a Privacy header field whose priv-value is "none" then the terminating gateway MUST place the telephone number from the P-Asserted-Identity header field into the calling party number field, and:

- In the case of a number from the DSN worldwide numbering plan set NoA indicator to "Subscriber number" and Numbering plan indicator to "Private numbering plan", set screening indicator to "Network provided," and set presentation indicator to "Presentation allowed."

- In the case of a PSTN number set NoA indicator to "unique international number" or to "national (significant) number" as appropriate, set screening indicator to "Network provided," and set presentation indicator to "Presentation allowed."

5.3.4.14.7.2.30.3 If the From header field does not have a SIP URI with a telephone number for the user part of the URI AND if there is a P-Asserted-Identity header with a SIP URI with a telephone number for the user part of the URI, AND there is a Privacy header whose priv-value is "header," or "user," or "id":

5.3.4.14.7.2.30.3.1 If the terminating gateway will be forwarding the IAM to an untrusted network then the terminating gateway MUST NOT add a Calling Party Number parameter to the IAM, or

5.3.4.14.7.2.30.3.2 If the terminating gateway will be forwarding the IAM to a trusted network the terminating gateway MUST place the telephone number from the P-Asserted-Identity header into the calling party number field, and:

- In the case of a number from the DSN worldwide numbering plan set NoA indicator to "Subscriber number" and Numbering plan indicator to "Private numbering plan", set screening indicator to "Network provided," and set presentation indicator to "Presentation allowed."

- In the case of a PSTN number set NoA indicator to "unique international number" or to "national (significant) number" as appropriate, set screening indicator to "Network provided," and set presentation indicator to "Presentation allowed."

5.3.4.14.7.2.30.4 If the From header field has a SIP URI with a telephone number for the user part of the URI AND if there is no P-Asserted-Identity header[1] or a P-Asserted-Identity header that does not have a SIP URI with a telephone number for the user part of the URI AND there is either no Privacy header field or a Privacy header field whose priv-value is "none":

5.3.4.14.7.2.30.4.1 The terminating Gateway MUST place the telephone number in the From header field into the calling party number field, and:

- In the case of a number from the DSN worldwide numbering plan set NoA indicator to "Subscriber number" and Numbering plan indicator to "Private numbering plan", set screening indicator to "User provided," and set presentation indicator to "Presentation allowed."

- In the case of a PSTN number set NoA indicator to "unique international number" or to "national (significant) number" as appropriate, set screening indicator to "User provided," and set presentation indicator to "Presentation allowed."

  AND

5.3.4.14.7.2.30.4.2 (ITU ISUP only) In the case of a PSTN number the terminating gateway SHOULD place the telephone number in the From header field into the Generic Number field, set Number qualifier indicator to "additional calling party number," set NoA indicator to "unique international number" or to "national (significant) number" as appropriate, set Number incomplete indicator to "complete," set Numbering plan indicator to "ISDN (telephony) numbering plan (Recommendation E.164)," set screening indicator to "User provided, not verified," set presentation indicator to "Presentation allowed."

5.3.4.14.7.2.30.5 If the From header field has a SIP URI with a telephone number for the user part of the URI AND if there is no P-Asserted-Identity header field[2] or a P-Asserted-Identity header field that does not have a SIP URI with a telephone number for the user part of the URI AND there is a Privacy header field whose priv-value is "header" or "user" or "id" then:

5.3.4.14.7.2.30.5.1 The terminating gateway MUST place the telephone number in the From header field into the calling party number field, and:

- In the case of a number from the DSN worldwide numbering plan set NoA indicator to "Subscriber number" and Numbering plan indicator to "Private

[1] The presence of a P-Asserted-Identity header is mandated by AS-SIP GSS requirement 5.3.4.7.1.1.23
[2] The presence of a P-Asserted-Identity header is mandated by AS-SIP GSS requirement 5.3.4.7.1.1.23.

numbering plan", set screening indicator to "User provided," and set presentation indicator to "Presentation restricted."

- In the case of a PSTN number set NoA indicator to "unique international number" or to "national (significant) number" as appropriate, set screening indicator to "User provided," and set presentation indicator to "Presentation restricted."

  AND

5.3.4.14.7.2.30.5.2 (ITU ISUP only) In the case of a PSTN number the terminating gateway SHOULD place the telephone number in the From header field into the Generic Number field, set number qualifier indicator to "additional calling party number," set NoA indicator to "unique international number" or to "national (significant) number" as appropriate, set Number incomplete indicator to "complete," set Numbering plan indicator to "ISDN (telephony) numbering plan (Recommendation E.164)," set screening indicator to "User provided, not verified," set presentation indicator to "Presentation restricted."

5.3.4.14.7.2.30.6 If the From header field has a SIP URI with a telephone number for the user part of the URI AND if there is a P-Asserted-Identity header field with a SIP URI with a telephone number for the user part of the URI, AND there is either no Privacy header field or a Privacy header field whose priv-value is "none":

5.3.4.14.7.2.30.6.1 The terminating gateway MUST place the telephone number from the P-Asserted-Identity header field into the calling party number field, and:

- In the case of a number from the DSN worldwide numbering plan set NoA indicator to "Subscriber number" and Numbering plan indicator to "Private numbering plan", set screening indicator to "Network provided," and set presentation indicator to "Presentation allowed."

- In the case of a PSTN number set NoA indicator to "unique international number" or to "national (significant) number" as appropriate, set screening indicator to "Network provided," and set presentation indicator to "Presentation allowed."

  AND

5.3.4.14.7.2.30.6.2 (ITU ISUP only) In the case of a PSTN number the terminating gateway SHOULD place the telephone number in the From header field into the Generic Number field, set Number qualifier indicator to "additional calling party number," set NoA indicator to "unique

international number" or to "national (significant) number" as appropriate, set Number incomplete indicator to "complete," set Numbering plan indicator to "ISDN (telephony) numbering plan (Recommendation E.164)," set screening indicator to "User provided, not verified," set presentation indicator to "Presentation allowed."

5.3.4.14.7.2.30.7 If the From header field has a SIP URI with a telephone number for the user part of the URI AND if there is a P-Asserted-Identity header field with a SIP URI with a telephone number for the user part of the URI, AND there is a Privacy header field whose priv-value is "header" or ""user" or "id":

5.3.4.14.7.2.30.7.1 If the terminating gateway will be forwarding the IAM to an untrusted network, the terminating gateway MUST omit the Calling Party Number parameter from the IAM and in the case of a PSTN number (ITU ISUP only) MAY derive the telephone number for the Generic Number from the From header field and set Number qualifier indicator to "additional calling party number," set NoA indicator to "unique international number" or to "national (significant) number" as appropriate, set Number incomplete indicator to "complete," set Numbering plan indicator to "ISDN (telephony) numbering plan (Recommendation E.164)," set screening indicator to "User provided, not verified," set presentation indicator to "Presentation restricted."

5.3.4.14.7.2.30.7.2 If the terminating gateway will be forwarding the IAM to a trusted network, the terminating gateway MUST place the telephone number from the P-Asserted-Identity header field into the calling party number field, and:

- In the case of a number from the DSN worldwide numbering plan set NoA indicator to "Subscriber number" and Numbering plan indicator to "Private numbering plan", set screening indicator to "Network provided," and set presentation indicator to "Presentation restricted."

- In the case of a PSTN number set NoA indicator to "unique international number" or to "national (significant) number" as appropriate, set screening indicator to "Network provided," and set presentation indicator to "Presentation restricted."

  AND

(ITU ISUP only) In the case of a PSTN number MAY derive the telephone number for the Generic Number from the From header field and set Number qualifier indicator to "additional calling party number," set NoA indicator to "unique international number" or to "national (significant) number" as appropriate, set Number incomplete indicator to "complete," set Numbering plan indicator to "ISDN (telephony) numbering plan (Recommendation E.164)," set

screening indicator to "User provided, not verified," set presentation indicator to "Presentation restricted."

Terminating Gateway Maps ISUP Messages to AS-SIP Messages

[Q.1912.5, Section 6.4] (ITU ISUP only)

5.3.4.14.7.2.31 When the terminating gateway receives a CON, the terminating gateway MUST send a 200 (OK) INVITE response.

[Q.1912.5, Section 6.5]

5.3.4.14.7.2.32 When the terminating gateway receives an ACM and the called party's status indicator of the ACM Backward Call Indicators parameter is set to "subscriber free," (bit 01) the terminating gateway MUST send a 180 Ringing response.

5.3.4.14.7.2.33 When the terminating gateway receives an ACM with cause parameters it is NOT inter-worked.

[Q.1912.5, Section 6.6]

5.3.4.14.7.2.34 When the terminating gateway receives a CPG and the bits of the event indicator of the CPG Event Information parameter indicate "alerting," the terminating gateway MUST send a 180 Ringing response.

5.3.4.14.7.2.35 When the terminating gateway receives a CPG and the bits of the event indicator of the CPG Event Information parameter indicate either "progress" or "in-band information or an appropriate pattern is now available," the terminating gateway generally does not inter-work the CPG. An exception to this rule is that the CPG is inter-worked when the Generic Notification Indicator is set to 'remote hold' or 'remote retrieval' in support of the call hold supplementary service as depicted in Figure 5.3.4-45, TDM-to-IP Call Hold; TDM Party Places Call On Hold, and Figure 5.3.4-48, IP-to-TDM Call Hold; IP Party Places Call On Hold.

5.3.4.14.7.2.36 When the terminating gateway receives an ANM, the terminating gateway MUST send a 200 OK. [Q.1912.5, Section 6.7]

5.3.4.14.7.2.38 When the terminating gateway receives a REL subsequent to receiving an ANM or CON (ITU ISUP only): [Q.1912.5, Section 6.11.2]

5.3.4.14.7.2.38.1 The terminating gateway MUST send a RLC onto the CCS7 network.

5.3.4.14.7.2.38.2 The terminating gateway MUST send a BYE and SHOULD include a Reason header field whose protocol field is assigned the value "Q.850," the protocol-cause field is assigned the cause value from the REL, and the Reason-Text field is based on the provisioning of the terminating gateway.

5.3.4.14.7.2.39 When the terminating gateway receives a REL prior to receiving an ANM or CON (ITU ISUP only): [Q.1912.5, Section 6.11.2]

5.3.4.14.7.2.39.1 The terminating gateway MUST Send a RLC onto the CCS7 network.

5.3.4.14.7.2.39.2 The terminating gateway MUST send the appropriate response as described in Table 5.3.4-23, 21/Q.1912.5, and copied for the reader's convenience. [Q1912.5, Section 6.11.2]

Table 5.3.4-23. 21/Q.1912.5

←SIP MESSAGE	← REL CAUSE INDICATORS PARAMETER
404 Not Found	Cause Value No. 1 ("*unallocated (unassigned) number*")
500 Server Internal Error	Cause Value No. 2 ("*no route to network*")
500 Server Internal Error	Cause Value No. 3 ("*no route to destination*")
500 Server Internal Error	Cause Value No. 4 ("*Send special information tone*")
404 Not Found	Cause Value No. 5 ("*Misdialed trunk prefix*")
500 Server Internal Error	Cause Value No. 8 ("*Preemption*")
500 Server internal Error	Cause Value No. 9 ("*Preemption-circuit reserved for reuse*")
486 Busy Here	Cause Value No. 17 ("*user busy*")
480 Temporarily unavailable	Cause Value No. 18 ("*no user responding*")
480 Temporarily unavailable	Cause Value No. 19 ("*no answer from the user*")
480 Temporarily unavailable	Cause Value No. 20 ("*subscriber absent*")
480 Temporarily unavailable	Cause Value No. 21 ("*call rejected*")
410 Gone	Cause Value No. 22 ("*number changed*")
No mapping	Cause Value No. 23 ("*redirection to new destination*")
480 Temporarily unavailable	Cause Value No. 25 ("*Exchange routing error*")
502 Bad Gateway	Cause Value No. 27 ("*destination out of order*")
484 Address Incomplete	Cause Value No. 28 ("*invalid number format (address incomplete*")
500 Server Internal Error	Cause Value No. 29 ("*facility rejected*")
480 Temporarily unavailable	Cause Value No. 31 ("*normal unspecified*") (Class default)
486 Busy here if Diagnostics Indicator includes the (CCBS indicator = "*CCBS possible"*) else 480 Temporarily unavailable	Cause Value in the Class 010 (resource unavailable, Cause Value No. 34)

←SIP MESSAGE	← REL CAUSE INDICATORS PARAMETER
500 Server Internal Error	Cause Value in the Class 010 (resource unavailable, Cause Value No. 38-47) (47 is class default)
500 Server Internal Error	Cause Value No. 50 ("*requested facility not subscribed*")
500 Server Internal Error (SIP-I only)	Cause Value No. 55 ("*incoming calls barred within CUG*")
500 Server Internal Error	Cause Value No. 57 ("*bearer capability not authorized*")
500 Server Internal Error	Cause Value No. 58 ("*bearer capability not presently*")
500 Server Internal Error	Cause Value No. 63 ("*service option not available, unspecified*") (Class default)
500 Server Internal Error	Cause Value in the Class 100 (service or option not implemented Cause Value No. 65 - 79) (79 is class default)
500 Server Internal Error (SIP-I only)	Cause Value No. 87 ("*user not member of CUG*")
500 Server Internal Error	Cause Value No. 88 ("*incompatible destination*")
500 Server Internal Error (SIP-I only)	Cause Value No. 90 ("*Non-existent CUG*")
404 Not Found	Cause Value No. 91 ("*invalid transit network selection*")
500 Server Internal Error	Cause Value No. 95 ("*invalid message*") (Class default)
500 Server Internal Error	Cause Value No. 97 ("*Message type non-existent or not implemented*")
500 Server Internal Error	Cause Value No. 99 ("*information element/parameter non-existent or not implemented*")
480 Temporarily unavailable	Cause Value No. 102 ("*recovery on timer expiry*")
500 Server Internal Error	Cause Value No. 103 ("*Parameter non-existent or not implemented, pass on*")
500 Server Internal Error	Cause Value No. 110 ("*Message with unrecognized Parameter, discarded*")
500 Server Internal Error	Cause Value No. 111 ("*protocol error, unspecified*") (Class default)
480 Temporarily unavailable	Cause Value No. 127 ("*interworking unspecified*") (Class default)
NOTES 1. The 500 response will include a Reason header whose reason-params has the value preemption ;cause=4 ;text="Non-IP Preemption". 2. The 500 response will include a Reason header whose reason-params has the value preemption ;cause=4 ;text="Non-IP Preemption"	

[Q.1912.5, Section 6.11.4]

5.3.4.14.7.2.40 When the terminating gateway receives a RSC (Reset Circuit message) from the ISUP network:

5.3.4.14.7.2.40.1 If the terminating gateway has already received an ACK for a previously sent 200 OK INVITE then the terminating gateway MUST send a BYE.

5.3.4.14.7.2.40.2 If the terminating gateway has sent a 200 OK INVITE but has not received an ACK then the terminating gateway MUST wait for the ACK before sending the BYE.

5.3.4.14.7.2.40.3 In all other cases, the terminating gateway MUST send a 500 (Server Internal Error) message response.

[Q.1912.5, Section 6.11.4]

5.3.4.14.7.2.41 When the terminating gateway receives a GRS (Circuit Group Reset message) from the ISUP network:

5.3.4.14.7.2.41.1 If the terminating gateway has already received an ACK for a previously sent 200 OK INVITE, the terminating gateway MUST send a BYE.

5.3.4.14.7.2.41.2 If the terminating gateway has sent a 200 OK INVITE but has not received an ACK, the terminating gateway MUST wait for the ACK before sending the BYE.

5.3.4.14.7.2.41.3 In all other cases, the terminating gateway MUST send a 500 (Server Internal Error) message response.

NOTE: One AS-SIP message MUST be sent for each call affected by the GRS.

[Q.1912.5, Section 6.11.4]

5.3.4.14.7.2.42 When the terminating gateway receives a CGB (Circuit Group Blocking message) with the Circuit Group Supervision Message Type indicator set to “hardware failure oriented” from the ISUP network:

5.3.4.14.7.2.42.1 If the terminating gateway has already received an ACK for a previously sent 200 OK INVITE, the terminating gateway MUST send a BYE.

5.3.4.14.7.2.42.2 If the terminating gateway has sent a 200 OK INVITE but has not received an ACK, the terminating gateway MUST wait for the ACK before sending the BYE.

5.3.4.14.7.2.42.3 In all other cases, the terminating gateway MUST send a 500 (Server Internal Error) message response.

NOTE: One AS-SIP message MUST be sent for each call affected by the CGB.

Terminating Gateway Maps AS-SIP Messages to ISUP Messages

BYE [Q.1912.5, Section 6.11.1]

5.3.4.14.7.2.43 When the terminating gateway receives a BYE Request then the terminating gateway MUST send a REL onto the ISUP network.

5.3.4.14.7.2.44 If the BYE has a Reason header field with a Q.850 cause value, the terminating gateway MAY map the Q.850 cause value from the Reason header field to the Cause Value field of the REL Cause Indication parameter, and set the Location field to "network beyond interworking point".

5.3.4.14.7.2.45 If the BYE does not have a Reason header field with a Q.850 cause value then the terminating gateway MUST place Cause Value No. 16 (normal clearing) in the REL.

CANCEL [Q.1912.5, Section 6.11.1]

5.3.4.14.7.2.46 When the terminating gateway receives a CANCEL request, the terminating gateway MUST send a REL to the ISUP network.

5.3.4.14.7.2.47 If the CANCEL has a Reason header field with a Q.850 cause value then the terminating gateway MAY map the Q.850 cause value from the Reason header field to the Cause Value field of the REL Cause Indication parameter, and set the Location field to "network beyond interworking point."

5.3.4.14.7.2.48 If the CANCEL does not have a Reason header field with a Q.850 cause value then the terminating gateway MUST place Cause Value No. 31 (normal unspecified) in the REL.

ISUP Messages that are Encapsulated by Terminating Gateway for Transparent Transport

No ISUP messages are encapsulated in AS-SIP messages for transport over the IP network.

5.3.4.14.7.3 Autonomous Release of Call by Terminating Gateway

[Q1912.5, Section 6.11.3]

5.3.4.14.7.3.1 Table 5.3.4-24, 22/Q.1912.5, details the events that trigger an autonomous release by the terminating gateway resulting in the transmission of a BYE, 4xx, or 5xx to the IP network and a REL to the CCS7 network.

Table 5.3.4-24. 22/Q.1912.5

← SIP	TRIGGER EVENT	REL → CAUSE INDICATORS PARAMETER
484 Address Incomplete	Determination that insufficient digits received. Applicable to overlap dialing which is prohibited in this specification. When UAS receives a request with a Request-URI that is incomplete then UAS sends back 484 response.	Not applicable.
480 Temporarily Unavailable	Congestion at the IWU	Not applicable.
BYE	ISUP procedures result in release after answer.	According to ISUP procedures.
500 Server Internal Error	Call release due to the ISUP compatibility procedure (Note 1)	According to ISUP procedures.
484 Address Incomplete	Call release due to expiry of T7 within the ISUP procedures	According to ISUP procedures.
480 Temporarily Unavailable	Call release due to expiry of T9 within the ISUP procedures	According to ISUP procedures.
480 Temporarily Unavailable	Other ISUP procedures result in release before answer.	According to ISUP procedures.
NOTE If the I-IWU receives unrecognized ISUP or BICC signalling information and determines that the call needs to be released based on the coding of the compatibility indicators, then see clause 2.9.5.2/Q.764 and clause 13.4.3/Q.1902.4.		

5.3.4.14.7.3.2 A Reason header field containing the (Q.850) Cause Value of the REL message MAY be included in the BYE request.

5.3.4.15 Relevant Timers for the Terminating Gateway and the Originating Gateway

5.3.4.15.1 ISUP Timers

ISUP T7 Timer

5.3.4.15.1.4 When the terminating gateway receives an initial INVITE, the terminating gateway sets an ISUP T7 timer, maps the INVITE header fields to an IAM message, and sends the IAM onto the CCS7 network.

5.3.4.15.1.5 If an ACM is received from the ISUP network prior to expiration of the T7 timer then the terminating gateway cancels the T7 timer, and,

5.3.4.15.1.5.1 If the Called Party's Status of Backward Call indicator parameter is "no indication" (bit 00) (i.e., early ACM), the terminating gateway creates a 183 Session progress response, maps the ACM parameter fields to the SIP response header fields, and sends the response onto the IP network.

5.3.4.15.1.5.2 If the Called Party's Status of Backward Call indicator parameter is "Subscriber free" (bit 01), the terminating gateway creates a 180 Ringing response, maps the ACM parameter fields to the SIP response header fields, and sends the response onto the IP network.

5.3.4.15.1.6 If the ISUP T7 timer at the terminating gateway expires prior to receipt of an ACM from the ISUP network, the terminating gateway MUST send a REL with cause code 102 "protocol error, recovery on timer expiry" to the ISUP network, and send a 504 response "gateway timeout" onto the IP network.

ISUP T11 Timer

5.3.4.15.1.7 When the originating gateway receives an IAM from the ISUP network, the originating gateway sets the ISUP T11 timer, sets the SIP timer T1 (if the underlying transport protocol is unreliable (e.g., UDP)), creates an AS-SIP INVITE, and sends the INVITE onto the IP network.

5.3.4.15.1.11 If the originating gateway receives a 180 Ringing response, the originating gateway MUST cancel the ISUP T11 timer, set the ISUP T9 timer, create an ACM (setting the called party's status indicator of the Backward Call Indicators will have been set to "subscriber free" (bit 01), send the ACM onto the ISUP network, and transmit a ringing tone over the TDM bearer circuit to the caller.
5.3.4.15.1.12 If the originating gateway receives a 183 Session progress response, the originating gateway MUST take no action on the ISUP side.
5.3.4.15.1.13 If the originating gateway does not receive a 180 Ringing prior to expiration of the ISUP T11 timer, the originating gateway MUST set timer T9, send an ACM with the Called Party's Status of the Backward Call indicator parameter set to "no indication" (bit 00) onto the ISUP network, and transmit a ringing tone over the TDM bearer circuit to the caller.

ISUP T9 Timer (NOT used by all ISUP Networks)

5.3.4.15.1.17 Upon receipt of an ACM from the ISUP network, the terminating gateway sets an ISUP T9 timer and sends a 18x response onto the IP network.

5.3.4.15.1.17.1 If the ACM is an early ACM (i.e., the Called Party's Status of Backward Call indicator parameter is "no indication" (bit 00), the SIP response is 183 Session progress.

5.3.4.15.1.17.2 If the ACM has the Called Party's Status of Backward Call indicator parameter is "Subscriber free" (bit 01), then the SIP response is 180 Ringing.

5.3.4.15.1.18 If an ANM is received from the ISUP network prior to expiration of the ISUP T9 timer, the terminating gateway cancels the T9 timer, creates a 200 OK INVITE, and sends the 200 OK INVITE onto the IP network.

5.3.4.15.1.19 If an ANM is NOT received from the ISUP network prior to expiration of the ISUP T9 timer, the terminating gateway SHOULD send a "480 Temporarily Unavailable" response onto the IP network and an REL message with cause value 19 (no answer from the user) to the ISUP network.

5.3.4.15.2 SIP Timers

5.3.4.15.2.1 When the originating gateway sends an AS-SIP INVITE over an unreliable transport layer protocol (i.e., UDP), the originating gateway MUST set SIP timer A with a default value of T1 equals 500ms [RFC 3261, Sections 17.1.1.1 and 17.1.1.2). If the timer expires prior to the originating gateway receiving a response to the INVITE, the originating gateway retransmits the INVITE. The originating gateway will repeat this process (with the T1 timer duration doubling each time) if it does not receive a response until 7 transmissions of the INVITE and 7 expirations of the timer at which time the originating gateway MUST send a CANCEL onto the IP network and send a REL over the ISUP network

5.3.4.15.2.2 When the originating gateway sends an AS-SIP INVITE over a reliable transport layer then the originating gateway MUST NOT set SIP timer A.

5.3.4.15.2.3 When the terminating gateway receives an ANM from the ISUP network (ITU ISUP, ANSI ISUP) or a CON (ITU ISUP only) and sends a 200 OK INVITE, the terminating gateway MUST set SIP timer T1. If the timer expires prior to the terminating gateway receiving an ACK to the 200 OK, the terminating gateway retransmits the 200 OK INVITE. The terminating gateway will repeat this process (with the T1 timer duration doubling each time) if it does not receive an ACK until 7 transmissions of the INVITE and 7 expirations of the T1 timer at which time the terminating gateway MUST send a BYE onto the IP network and send a REL over the ISUP network.

5.3.4.16 SIP Requirements for Interworking AS-SIP Signaling Appliances

5.3.4.16.1 General Requirements

Interworking AS-SIP signaling appliances MUST comply with UCR 2008 Section 5.3.4.7.1, AS-SIP Signaling Appliances, as well as the additional general requirements enumerated below.

5.3.4.16.1.1 When an interworking AS-SIP signaling appliance receives a request that contains a Require header field with one or more option-tags that it does not understand then the interworking AS-SIP signaling appliance MUST return a 420 (Bad Extension) response. The response MUST include an Unsupported header field listing those option-tags the element did not understand. [RFC 3261, Section 8.2.2.3]

5.3.4.16.1.2 All outbound INVITEs generated by an interworking AS-SIP signaling appliance MUST include a Supported header with the option tag '100rel'.

5.3.4.16.2 Methods

5.3.4.16.2.1 INVITE

5.3.4.16.2.1.1 Interworking AS-SIP signaling appliances MUST support generating and receiving SIP INVITE Requests.

5.3.4.16.2.1.2 Interworking AS-SIP signaling appliances MUST comply with the requirements applicable to INVITE Client Transactions (see RFC 3261, Sections 17.1.1.1, 17.1.1.2, 17.1.1.3, 17.1.3, and 17.1.4) and INVITE Server Transactions (see RFC 3261, Sections 17.2.1, 17.2.3, and 17.2.4).

5.3.4.16.2.1.3 Interworking AS-SIP signaling appliances MUST comply with the requirements of RFC 3261 Section 13.2.1, Creating the Initial INVITE, Section 13.2.2, Processing the INVITE Responses, and Section 13.3.1, Processing of the INVITE.

5.3.4.16.2.1.4 Interworking AS-SIP signaling appliances MUST support generating and receiving SIP re-INVITES per RFC 3261, Section 14.

5.3.4.16.2.2 CANCEL

5.3.4.16.2.2.1 Interworking AS-SIP signaling appliances MUST support generating and receiving SIP CANCEL Requests and comply with RFC 3261, Section 9.

5.3.4.16.2.3 REGISTER

Not applicable

5.3.4.16.2.4 OPTIONS

5.3.4.16.2.4.1 Interworking AS-SIP signaling appliances MUST support generating and receiving SIP OPTIONS Requests and MUST comply with the requirements for SIP OPTIONS

set forth in RFC 3261, Section 11, Querying for Capabilities, which includes 11.1, Construction of OPTIONS Request, and 11.2, Processing of OPTIONS Request.

5.3.4.16.2.5 BYE

5.3.4.16.2.5.1 Interworking AS-SIP signaling appliances MUST support generating and receiving SIP BYE Requests and MUST comply with the requirements of RFC 3261, Section 15, Terminating a Session.

5.3.4.16.2.6 ACK

5.3.4.16.2.6.1 Interworking AS-SIP signaling appliances MUST support generating and receiving SIP ACK Requests as defined in RFC 3261.

5.3.4.16.2.7 INFO

INFO Method requirements have been removed.

5.3.4.16.2.8 PRACK

5.3.4.16.2.8.1 Interworking AS-SIP signaling appliances MUST support generating and receiving the SIP PRACK method as defined in RFC 3262.

5.3.4.16.2.8.2 Interworking AS-SIP signaling appliances MUST support use of the option tag '100rel' with the Require header and Supported header, and MUST support the use of header fields Rack, Rseq as defined in RFC 3262.

5.3.4.16.2.9 UPDATE

5.3.4.16.2.9.1 Interworking AS-SIP signaling appliances MUST support generating and receiving the SIP UPDATE method as defined in RFC3311.

5.3.4.16.2.10 REFER

5.3.4.16.2.10.1 Interworking AS-SIP signaling appliances MUST support generating and receiving the SIP REFER method, the Refer-To header, and the refer event package as defined in RFC 3515.

5.3.4.16.2.10.2 Interworking AS-SIP signaling appliances MAY support generating and receiving/processing the Referred-By header. [RFC 3892]

5.3.4.16.2.11 SUBSCRIBE

5.3.4.16.2.11.1 At this time the AS-SIP GSS has not mandated the use of any event packages in conjunction with the SUBSCRIBE request. A requirement to support specified event packages may be added in the future.

5.3.4.16.2.12 NOTIFY

5.3.4.16.2.12.1 Interworking AS-SIP signaling appliances MUST support the NOTIFY Method for event notification defined in RFC 3265. In particular, this specification employs the NOTIFY request in the call transfer supplementary service.

5.3.4.16.3 Header Fields

5.3.4.16.3.1 Interworking AS-SIP signaling appliances MUST, in adherence with the enumerated RFCs, be capable of generating, receiving, and processing the following SIP headers (see RFC 3261, Section 20, RFC 3262, RFC 3265, RFC 3325, RFC 3326, RFC 3515, RFC 3891, RFC 4028, and RFC 4412 as modified herein):

Accept
Alert-Info
Allow
Allow-Events
Call-ID
Contact
Content-Disposition
Content-Length
Content-Type
Cseq
Date
Event
Expires
From
Max-Forwards
Min-Expires
Min-SE
P-Asserted-Identity
RAck
Reason
Record-Route
Refer-To

Replaces
Require
Resource-Priority
Retry-After
RSeq
Session-Expires
Subscription-State
Supported
To
Unsupported
Via
Warning

5.3.4.16.3.2 Interworking AS-SIP signaling appliances MAY be capable of receiving/processing the following SIP header:

Referred-By [RFC 3892]

5.3.4.16.3.3 The From header MUST include a tag field as specified in RFC 3261, Section 19.3.

5.3.4.16.3.4 The To header of a request that is part of a dialog MUST include a tag field as specified in RFC 3261, Section 19.3.

5.3.4.16.3.5 Interworking AS-SIP signaling appliances MUST support the use of option tags for the Require, Supported, and Unsupported headers. Option-tags currently used in this specification are 'replaces', '100rel', 'resource-priority', 'precondition', and 'timer'.

Route Header

5.3.4.16.3.6 In the event the interworking AS-SIP signaling appliance is an LSC then:

5.3.4.16.3.6.1 **[FY2008-FY2010] [Objective]** When the interworking LSC sends a SIP Request message to its local EBC intended for its Softswitch, then it is an objective requirement for the FY2008-FY2010 time frame that the interworking LSC add a route set comprised of two (2) Route headers where the first Route header is the SIP URI for the EBC at the enclave, and the second Route header is the SIP URI for the EBC serving the Softswitch. This is not a threshold requirement until FY2010.

5.3.4.16.3.6.1.1 **[FY2008-FY2010] [Conditional]** If the interworking LSC adds a route set comprised of two (2) Route headers, then the default format of the SIP URI for the Route header

will consist of an alphanumeric identifier for the userinfo part and an IP address for the host name.

Example:

Route: <sip:ebcenc1@192.168.7.125;lr>
Route: <sip:ebcsdn3@195.117.2.1;lr>

5.3.4.16.3.6.2 **[FY2010+]** When an interworking LSC sends a SIP Request message to its local EBC intended for its Softswitch, then, as a default configuration, the interworking LSC MUST add a route set comprised of two (2) Route headers where the first Route header is the SIP URI for the EBC at the enclave, and the second Route header is the SIP URI for the EBC serving the Softswitch.

5.3.4.16.3.7 In the event the interworking AS-SIP signaling appliance is a Softswitch then:

5.3.4.16.3.7.1 **[FY2008]** When an interworking Softswitch forwards a SIP request to a peer Softswitch, then the interworking Softswitch MUST add a route set comprised of two (2) Route headers where the first Route header is the SIP URI for the EBC that serves the interworking Softswitch, and the second Route header is the SIP URI for the EBC serving the peer Softswitch.

5.3.4.16.3.7.1.1 **[FY2008]** The default format of the SIP URI for the Route header will consist of an alphanumeric identifier for the userinfo part and an IP address for the host name.

Example:

Route: <sip:ebcsdn3@192.168.100.100;lr>
Route: <sip:ebcsdn7@196.1.2.111;lr>

5.3.4.16.3.7.2 **[FY2008]** When an interworking Softswitch forwards a SIP request to a subtended LSC, then the interworking Softswitch MUST add a route set comprised of two (2) Route headers where the first Route header is the SIP URI for the EBC that serves the interworking Softswitch, and the second Route header is the SIP URI for the EBC serving the subtended LSC.

5.3.4.16.3.7.2.1 **[FY2008]** The default format of the SIP URI for the Route header will consist of an alphanumeric identifier for the userinfo part and an IP address for the host name.

Example:

Route: <sip:ebcsdn7@192.168.88.50;lr>
Route: <sip:ebcenc25@188.2.44.3;lr>

Interworking AS-SIP Signaling Appliance and VIA Header Requirements

5.3.4.16.3.8 When an interworking AS-SIP signaling appliance generates an outbound AS-SIP request, the interworking AS-SIP signaling appliance MUST add its own VIA header to the AS-SIP request.

5.3.4.16.3.9 When an interworking AS-SIP signaling appliance receives a SIP response to be translated into TDM signaling, then the interworking AS-SIP signaling appliance operates as the UAC for SIP purposes.

5.3.4.16.3.10 When an interworking AS-SIP signaling appliance receives an inbound SIP request to be translated into TDM signaling, then the AS-SIP signaling appliance operates as the UAS for SIP purposes.

5.3.4.16.3.11 When an interworking AS-SIP signaling appliance generates a SIP response on behalf of a signaling message received from the TDM network, then prior to forwarding the SIP response the interworking AS-SIP signaling appliance MUST include the VIA headers received in the corresponding SIP request.

CCA-ID Parameter

5.3.4.16.3.12 When an interworking AS-SIP signaling appliance operating as an originating gateway receives an IAM from the TDM network and sends an INVITE to another AS-SIP signaling appliance (Softswitch or LSC), then the interworking AS-SIP signaling appliance MUST add a CCA-ID parameter to the SIP URI of the Contact header populated with its unique identifier before forwarding the INVITE onward to the next AS-SIP signaling appliance.

5.3.4.16.4 Response Codes

5.3.4.16.4.1 Interworking AS-SIP signaling appliances MUST support sending, receiving, and processing the provisional (1xx) response codes: 100 (Trying), 180 (Ringing), and 183 (Session Progress). [RFC 3261, Section 21.1, Provisional 1xx]

5.3.4.16.4.2 Interworking AS-SIP signaling appliances MUST support the successful (2xx) response codes: 200 (OK) [RFC 3261, Section 21.2, 200 OK] and 202 (Accepted) [RFC 3515].

5.3.4.16.4.3 Interworking AS-SIP signaling appliances MAY be capable of operating as redirect servers and MAY support the following redirection (3xx) response codes: 300 (Multiple Choices), 301 (Moved Permanently), 302 (Moved Temporarily), and 305 (Use Proxy). [RFC 3261, Section 21.3, Redirection 3xxx]

5.3.4.16.4.4 Interworking AS-SIP signaling appliances MUST support the request failure (4xx) response codes: 400 (Bad Request), 401 (Unauthorized), 403 (Forbidden), 404 (Not Found), 405 (Method Not Allowed), 406 (Not Acceptable), 407 (Proxy Authentication Required), 408 (Request Timeout), 410 (Gone), 413 (Request Entity Too Large), 414 (Request-URI Too Long), 415 (Unsupported Media Type), 416 (Unsupported URI Scheme), 417 (Unknown Resource-Priority), 420 (Bad Extension), 421 (Extension Required), 422 (Session Interval Too Small), 423 (Interval Too Brief), 480 (Temporarily Unavailable), 481 (Call/Transaction Does Not Exist), 482 (Loop Detected), 483 (Too Many Hops), 484 (Address Incomplete), 485 (Ambiguous), 486 (Busy Here), 487 (Request Terminated), 488 (Not Acceptable Here), and 491 (Request Pending). [RFC 3261, Section 21.4, Request Failure 4xx]

5.3.4.16.4.5 Interworking AS-SIP signaling appliances upon properly receiving a CANCEL for an INVITE MUST first send a 200 (OK) to the CANCEL, and then follow up with a 487 (Request Terminated) to the INVITE.

5.3.4.16.4.6 Interworking AS-SIP signaling appliances MUST support the server failure (5xx) response codes: 500 (Server Internal Error), 501 (Not Implemented), 502 (Bad Gateway), 503 (Service Unavailable), 504 (Server Timeout), 505 (Version Not Supported), 513 (Message Too Large) [RFC 3261, Section 21.5, Server Failure 5xx], and 580 (Precondition Failure) [RFC 3312].

5.3.4.16.4.7 Interworking AS-SIP signaling appliances MUST support the global failures (6xx) response codes: 600 (Busy Everywhere), 603 (Decline), 604 (Does Not Exist Anywhere), and 606 (Not Acceptable). [RFC 3261, Section 21.6, Global Failures 6xx]

5.3.4.16.5 SIP Preconditions

See UCR 2008, Section 5.3.4.7.5, SIP Preconditions – SBU Network Only, and UCR 2008, Section 5.3.4.7.5b, SIP Preconditions –Classified Network Only.

5.3.4.16.6 64kbps Transparent Calls (Clear Channel)

Interworking AS-SIP signaling appliances MUST comply with the requirements in UCR 2008, Section 5.3.4.7.7, 64kbps Transparent Calls (Clear Channel).

5.3.4.16.7 Transport of Route Code Information over AS-SIP

Interworking AS-SIP signaling appliances directly serving IP end instruments MUST comply with the requirements in UCR 2008, Section 5.3.4.7.8, Transport of Route Code Information over AS-SIP. In addition, interworking AS-SIP signaling appliances directly serving IP end instruments MUST meet the requirements enumerated below.

5.3.4.16.7.1 When an interworking AS-SIP signaling appliance receives an INVITE whose Request URI includes the tgrp parameter and trunk-context parameter and the INVITE is to be interworked into an ISUP IAM then the interworking AS-SIP signaling appliance MUST conduct the following translation:

- If tgrp=hotline, then the Information Transfer Capability of the User Service Information parameter is set to Speech (“00000”).
- If tgrp=ccdata, then the Information Transfer Capability of the User Service Information parameter is set to Unrestricted Digital Information (“00000”).
- If tgrp=nosat ← N/A not defined.
- If tgrp=hotline-ccdata, then the Information Transfer Capability of the User Service Information parameter is set to Unrestricted Digital Information (“00000”).

5.3.4.16.7.2 When an interworking AS-SIP signaling appliance receives an INVITE whose Request URI includes the tgrp parameter and trunk-context parameter and the INVITE is to be interworked into an ISDN Q.931 SETUP message, then the translation to be performed by the interworking AS-SIP signaling appliance is summarized in Table 5.3.4-25.

Table 5.3.4-25. SIP tgrp to ISDN Q.931 Mapping

SIP TGRP=VALUE	Q.931 IE / BEARER CAPABILITY
No label	Voice Bearer Cap (BC)
tgrp=ccdata	56/64k circuit-mode data
tgrp=nosat	N/A – not defined
tgrp=hotline	Off hook indicator of voice, speech BC
tgrp=hotline-ccdata	Off hook indicator of data, 56/64k cmd BC

5.3.4.17 Keep-Alive Timer Requirements for interworking AS-SIP Signaling Appliances

5.3.4.17.1 Keep-Alive Timer Requirements for Interworking AS-SIP Signaling Appliances

Interworking AS-SIP signaling appliances MUST comply with the Section 9, SIP Session Keep-Alive Timer, of the AS-SIP GSS as well as the additional E1 requirements enumerated below.

5.3.4.17.1.1 When an interworking AS-SIP signaling appliance receives an outbound request from the PSTN (i.e., the interworking AS-SIP signaling appliance is operating as an originating gateway) and the destination is NOT an IP end instrument directly served by the interworking AS-SIP signaling appliance then the interworking AS-SIP signaling appliance MUST operate in accordance with the UAC behavior set forth in RFC 4028, Sections 7.1, Generating an Initial Session Refresh Request; 7.2, Processing a 2xx Response; 7.3, Processing a 422 Response; 7.4, Generating Subsequent Session Refresh Requests; and 10, Performing Refreshes (when responsible for performing the refresh).

5.3.4.17.1.2 When an interworking AS-SIP signaling appliance receives an outbound request from the PSTN (i.e., the interworking AS-SIP signaling appliance is operating as an originating gateway) and the destination is an IP end instrument directly served by the interworking AS-SIP signaling appliance then this document does NOT require the use of the keep-alive mechanism.

5.3.4.17.1.3 When an interworking AS-SIP signaling appliance acting as a terminating gateway receives a call request from another AS-SIP signaling appliance then the interworking AS-SIP signaling appliance MUST operate in accordance with the UAS behavior set forth in RFC 4028, Section 9, and RFC 4028, Section 10, Performing Refreshes (when responsible for performing the refresh).

5.3.4.17.1.4 When an interworking AS-SIP signaling appliance receives an outbound request from a directly served IP end instrument and is the terminating gateway for the call request then this document does NOT require the use of the keep-alive mechanism.

5.3.4.18 Precedence and Preemption Extensions for Interworking AS-SIP Signaling Appliances

5.3.4.18.1 Precedence Level Communicated over SIP Signaling

See UCR 2008, Section 5.3.4.10.2, Precedence Level Communicated over SIP Signaling, for descriptions.

5.3.4.18.1.1 "Resource-Priority" Header Field

Interworking AS-SIP signaling appliances MUST comply with the requirements in UCR 2008, Section 5.3.4.10.2.1, Resource-Priority Header Field.

5.3.4.18.1.2 Namespace

Interworking AS-SIP signaling appliances MUST comply with the requirements in UCR 2008, Section 5.3.4.10.2.1.1, Namespace.

5.3.4.18.1.3 r-priority

Interworking AS-SIP signaling appliances MUST comply with the requirements in UCR 2008 Section 5.3.4.10.2.1.2, r-priority.

5.3.4.18.2 Requirements for Interworking AS-SIP Signaling Appliances

Interworking AS-SIP signaling appliances directly serving IP end instruments MUST comply with Section 5.3.4.10.2.2, Requirements for AS-SIP Signaling Appliances Serving IP End Instruments, of the AS-SIP GSS. All interworking AS-SIP signaling appliances MUST also comply with the requirements enumerated below.

Call Request Received from CCS7 Network

5.3.4.18.2.1 **[FY2008-FY2012]** Whenever an interworking AS-SIP signaling appliance receives an ISUP message that requires translation into an INVITE, UPDATE, or REFER request then:

5.3.4.18.2.1.1 **[FY2008-FY2012]** If the ISUP message contains a Multilevel Precedence and Preemption (MLPP) information element, the interworking AS-SIP signaling appliance MUST:

- Translate the four (4) network identity digits of the MLPP information element into the value for the corresponding network domain subfield in accordance with a translation table configured in the interworking AS-SIP signaling appliance. (For FY2008-2012, a DSN interworking AS-SIP signaling appliance will always enter "dsn" into the network domain subfield.)

  – If the four (4) network identity digits of the MLPP information element are the binary coded decimal 0000 (i.e., the MLPP equivalent of the "dsn" network domain ID), then the value to be placed into the r-priority field is determined from the MLPP precedence level bits using Table 5.3.4-26. In the event the precedence level bits do not

have an authorized value, then the r-priority field is given the value "0."

Table 5.3.4-26. Table of Correspondence between MLPP Bits in ISUP Message and Character Representation of Single Decimal Value for "r-priority" Field in Resource Priority Header

PRECEDENCE LEVEL	MLPP PRECEDENCE LEVEL BITS	"RESOURCE-PRIORITY" R-PRIORITY VALUE
ROUTINE	0100	"0"
PRIORITY	0011	'2'
IMMEDIATE	0010	'4'
FLASH	0001	'6'
FLASH-OVERRIDE	0000	'8'

– **[FY2008-2012]** If the four (4) network identity digits of the MLPP information element are some number other than the binary coded decimal 0000, then the r-priority field is assigned the value "0."

- Convert the hexadecimal value of the 3-octet MLPP service domain into a text string consisting of six (6) characters, which is placed into the precedence-domain subfield.

Implementation Note: In the FY2008-FY2012 time frame if the hexadecimal value in the 3-octet MLPP service domain is a value other then 0x000000 then it is acceptable for the inter-working AS-SIP signaling appliance to convert the MLPP service domain to a precedence domain subfield having the text string "000000".

NOTE: **[FY2012+]** It is anticipated that additional network domains will be defined and corresponding Network Identity digits will be defined for the new network domains. The new network domains will have associated r-priority values defined for them and corresponding values for the MLPP precedence level bits will be defined. In addition, precedence domains other than "000000" may be added and will be directly convertible into the 3-octet MLPP service domain.

5.3.4.18.2.1.2 **[FY2008+]** If the ISUP message does not contain a MLPP information element, an interworking AS-SIP signaling appliance MUST assign "dsn" to the network domain subfield, assign "0" to the r-priority field, and assign "000000" to the precedence-domain subfield.

5.3.4.18.2.1.3 Call Request Intended for the CCS7 Network

[FY2008-2012] When an interworking AS-SIP signaling appliance receives an INVITE, UPDATE, or REFER message from an AS-SIP signaling appliance intended for an end instrument on the TDM network, then the interworking AS-SIP signaling appliance MUST:

- Set the network identity digits of the MLPP information element to the binary coded decimal value "0000."
- Translate the value of the r-priority field of the Resource Priority Header to the equivalent MLPP precedence level bits (see Table 5.3.4-26).
- Set the service domain to $000000000000000000000000_{binary}$ (i.e., 0x000000).

5.3.4.18.2.1.4 **[FY2008-2012]** When an interworking AS-SIP signaling appliance receives a call signaling message from a directly served IP end instrument intended for a TDM end instrument (for which the AS-SIP signaling appliance is also the interworking gateway) and the corresponding ISUP message is an IAM, then the interworking AS-SIP signaling appliance MUST:[3]

- Set the network identity digits of the MLPP information element to the binary coded decimal value "0000."
- Translate the precedence value of the call request to the equivalent MLPP precedence level bits. For example, in the case of an AS-SIP EI, use Table 5.3.4-26 to translate between r-priority value and MLPP precedence level bits.
- Set the service domain to $000000000000000000000000_{binary}$ (i.e., 0x000000).

5.3.4.18.3 Option Tag 'resource-priority'

Interworking AS-SIP signaling appliances MUST comply with the requirements in UCR 2008, Section 5.3.4.10.2.3, Option Tag 'resource-priority'.

5.3.4.18.3.1 Interworking AS-SIP signaling appliances MUST support the option tag 'resource-priority' for use with the Require header.

[3]In the case of a precedence call request from a directly served IP EI, the interworking AS-SIP signaling appliance must authenticate and authorize the caller.

5.3.4.18.3.2 The interworking AS-SIP signaling appliance MUST receive and accept a Require header field with the option tag 'resource-priority' in the INVITE, UPDATE, and REFER messages. Interworking AS-SIP signaling appliances MUST NOT reject the message with a 420 (Bad Extension) but rather MUST accept the request and translate it into the appropriate TDM signaling message as required.

5.3.4.18.4 Error Conditions

Improper Network-Domain, Priority Value, or Precedence-Domain

FY2008-2012

5.3.4.18.4.1 **[FY2008-FY2012]** When the interworking AS-SIP signaling appliance receives a SIP request with a Resource Priority header intended for a destination on the TDM network and the SIP request either does not have a Require header or has a Require header but not the option tag 'resource-priority', then:

5.3.4.18.4.1.1 **[FY2008-FY2012]** If the interworking AS-SIP signaling appliance does not recognize the value of the network domain subfield of the namespace, then the network domain subfield is treated as if it were set to "dsn" and the r-priority value is treated as if it were set to "0." If the precedence-domain subfield is either syntactically flawed or does not consist of the text string "000000," then it is still treated as if it had the value "000000." NOTE: In the conversion to the Precedence Level Information Element, the Network Identity digits are "0000," the MLPP precedence level bits are "0100" (routine), and the service domain is 0x000000.

5.3.4.18.4.1.2 **[FY2008-FY2012]** If the interworking AS-SIP signaling appliance recognizes the value of the network domain subfield of the namespace but the r-priority field does not have an authorized value for the given network domain then the r-priority value is treated as if it were set to the lowest priority level. If the precedence-domain subfield is either syntactically flawed or does not consist of the text string "000000," then it is still treated as if it had the value "000000."

5.3.4.18.4.1.3 **[FY2008-FY2012]** If the interworking AS-SIP signaling appliance receives a namespace with a recognized network domain and an authorized r-priority value whose precedence-domain subfield has a text string that is either syntactically invalid or does not consist of the text string "000000," then the precedence-domain subfield is treated as if it were set to the text string "000000."

5.3.4.18.4.2 **[FY2008-FY2012]** When the interworking AS-SIP signaling appliance receives a SIP request with a Resource Priority header intended for a destination on the TDM network and the SIP request has a Require header field with an option tag 'resource-priority', then:

5.3.4.18.4.2.1 **[FY2008-FY2012]** If the interworking AS-SIP signaling appliance does not recognize the value of the network domain subfield of the namespace then the interworking AS-SIP signaling appliance MUST reject the request with a 417 (Unknown Resource-Priority) response code.

5.3.4.18.4.2.2 **[FY2008-FY2012]** If the interworking AS-SIP signaling appliance recognizes the value of the network domain subfield but the value of the r-priority field is not valid for the given network domain then the r-priority value is treated as if it were set to the lowest priority level. If the precedence-domain subfield has a text string that is syntactically invalid or does not consist of the text string "000000," then the precedence-domain subfield is treated as if it were set to "000000."

5.3.4.18.4.2.3 **[FY2008-FY2012]** If the interworking AS-SIP signaling appliance recognizes the value of the network domain and the r-priority field has an authorized value for the network domain but the precedence-domain subfield has a text string that is syntactically invalid or does not consist of the text string "000000," then the precedence-domain subfield is treated as if it were set to "000000."

After FY2012

5.3.4.18.4.3 **[After FY2012]** When the interworking AS-SIP signaling appliance receives a SIP request with one (1) or more Resource Priority headers intended for a destination on the TDM network and the SIP request either does not have a Require header or has a Require header but not the option tag 'resource-priority', then:

5.3.4.18.4.3.1 **[After FY2012]** If there is either one (1) Resource Priority header with at least two (2) namespaces or if there are two (2) or more Resource Priority headers (i.e., two (2) or more different namespaces) and the interworking AS-SIP signaling appliance does not recognize the value of the network domain subfield in any of the namespaces, then the interworking AS-SIP signaling appliance MUST treat the network domain as if it were "dsn" and treat the r-priority value as if it were set to "0." If the precedence-domain subfield has a text string that is invalid syntactically, then the precedence-domain subfield is treated as if it were set to "000000." NOTE: In the conversion to the Precedence Level Information Element, the Network Identity digits are set to "0000," the MLPP precedence level bits are set to "0100" (routine), and the service domain is set to 0x000000.

5.3.4.18.4.3.2 **[After FY2012]** If there are multiple resource values having valid network domains then in any case where the r-priority value associated with the valid network domain is not an authorized value it is treated as if it were set to the lowest priority level. When the priority levels of the resource values are compared to determine which resource value will be used for precedence and preemption purposes, then the resource values with valid network

domains but having unauthorized r-priority values will be treated as having the lowest precedence level when the comparison is made and the resource value with the highest priority will be selected. In each case the precedence-domain is interpreted as is unless it is syntactically flawed in which case it is treated as the text string "000000."

5.3.4.18.4.4 **[After FY2012]** When the interworking AS-SIP signaling appliance receives a SIP request with at least one (1) Resource Priority header intended for a destination on the TDM network and the SIP request has a Require header field with an option tag 'resource-priority', then:

5.3.4.18.4.4.1 **[After FY2012]** If there is either one (1) Resource Priority header with at least two (2) namespaces or if there are two (2) or more Resource Priority headers (i.e., two (2) or more different namespaces) and the interworking AS-SIP signaling appliance does not recognize the value of the network domain subfield in any of the namespaces, then the interworking AS-SIP signaling appliance MUST reject the request with a 417 (Unknown Resource-Priority) response code.

5.3.4.18.4.4.2 **[After FY2012]** If there are multiple resource values having valid network domains then in any case where the r-priority value associated with the valid network domain is not an authorized value it is treated as if it were set to the lowest priority level. When the priority levels of the resource values are compared to determine which resource value will be used for precedence and preemption purposes then the resource values with valid network domains but having unauthorized r-priority values will be treated as having the lowest precedence level when the comparison is made and the resource value with the highest priority will be selected. In each case the precedence-domain is interpreted as is unless it is syntactically flawed in which case it is treated as the text string "000000."

Authentication Failure

Interworking AS-SIP signaling appliances directly serving IP end instruments MUST comply with UCR 2008, Section 5.3.4.10.2.4, Error Conditions, Authentication Failure subsection.

Authorization Failure

Interworking AS-SIP signaling appliances directly serving IP end instruments MUST comply with UCR 2008, Section 5.3.4.10.2.4, Error Conditions, Authorization Failure subsection.

Insufficient Resources

5.3.4.18.4.5 If an interworking AS-SIP signaling appliance receives an inbound routine call request over the IP network for a destination on the TDM network and the interworking AS-SIP

signaling appliance has insufficient bandwidth-related resources (e.g., lack of circuit switched trunk capacity for bearer traffic) to handle the call request, the interworking AS-SIP signaling appliance MUST reply with a 488 (Not Acceptable Here) response code and SHOULD include a Warning header with warning code 370 (Insufficient Bandwidth).

5.3.4.18.4.6 If an interworking AS-SIP signaling appliance receives an inbound precedence call request (i.e., with precedence level priority or above) over the IP network for a destination on the TDM network and the interworking AS-SIP signaling appliance has insufficient bandwidth-related resources (e.g., lack of circuit switched trunk capacity for bearer traffic) to handle the call request and if there are insufficient existing calls (and/or call requests) of lower precedence whose removal would provide the necessary resources to support the pending call request, then:

5.3.4.18.4.6.1 The interworking AS-SIP signaling appliance MUST reply with a 488 (Not Acceptable Here) response code and SHOULD include a Warning header with warning code 370 (Insufficient Bandwidth), and

5.3.4.18.4.6.2 The AS-SIP signaling appliance serving the calling IP end instrument MUST arrange for a blocked precedence announcement to be played to the calling IP end instrument before terminating the call.

5.3.4.18.5 Precedence Call Rules

Interworking AS-SIP signaling appliances directly serving IP end instruments MUST comply with the requirements in UCR 2008, Section 5.3.4.10.2.5, Precedence Call Rules.

5.3.4.18.6 ASAC Preemption Requirements

Interworking AS-SIP signaling appliances MUST comply with the requirements in UCR 2008, Section 5.3.4.10.3, ASAC Preemption Requirements.

5.3.4.18.6.1 Reason Header for Preemption

Interworking AS-SIP signaling appliances MUST comply with the requirements in UCR 2008, Section 5.3.4.10.3.1, Reason Header for Preemption.

5.3.4.18.6.2 Preemption at the IP End Instrument

5.3.4.18.6.2.1 General Preemption Rules for Behavior at IP End Instruments

Interworking AS-SIP signaling appliances directly serving IP end instruments MUST comply with the requirements in UCR 2008, Section 5.3.4.10.3.2.1, General Preemption Rules for Behavior at IP End Instrument.

5.3.4.18.6.2.1b Interworking Signaling for BPA and BNEA

5.3.4.18.6.2.1b.1 When a precedence call request originating on the TDM network is blocked due to insufficient network resources on the IP network then the inter-working AS-SIP signaling appliance will receive a 488 response that SHOULD include a "Warning" header with warning code 370 (Insufficient Bandwidth) with either no reason header or a reason header that does NOT include a preemption cause whereupon the inter-working AS-SIP signaling appliance MUST send a REL with Q.850 cause code 46 precedence call blocked (in the case of CCS7 ISUP) or a Disconnect with Q.850 cause code 46 precedence call blocked (in the case of ISDN) onto the TDM network.

5.3.4.18.6.2.1b.2 When an inter-working AS-SIP signaling appliance receives a precedence call request from the IP network that it translates and forwards onto the TDM network and the response from the TDM network is a REL with Q.850 cause code 46 precedence call blocked (in the case of CCS7 ISUP) or a Disconnect with Q.850 cause code 46 precedence call blocked (in the case of ISDN) then the inter-working AS-SIP signaling appliance MUST generate a 488 response that SHOULD include a "Warning" header with warning code 370 (Insufficient Bandwidth) with no reason header which it sends onto the IP network.

5.3.4.18.6.2.1b.3 When a precedence call request originating on the TDM network is blocked due to an endpoint preemption on the IP network then the inter-working AS-SIP signaling appliance will receive a 486 response with either no reason header or a reason header that does NOT include a preemption cause whereupon the inter-working AS-SIP signaling appliance MUST send a REL with Q.850 cause code 46 precedence call blocked (in the case of CCS7 ISUP) or a Disconnect with Q.850 cause code 46 precedence call blocked (in the case of ISDN) onto the TDM network.

5.3.4.18.6.2.1b.4 When a precedence call request originating on the TDM network is blocked due to a busy nonpreemptable endpoint on the IP network then the inter-working AS-SIP signaling appliance will receive a 480 response with either no reason header or a reason header that does NOT include a preemption cause whereupon the inter-working AS-SIP signaling appliance MUST send a REL with Q.850 cause code 46 precedence call blocked (in the case of

CCS7 ISUP) or a Disconnect with Q.850 cause code 46 precedence call blocked (in the case of ISDN) onto the TDM network.

5.3.4.18.6.2.2 Required Behavior at Called IP End Instrument when Active Call is Preempted by Higher Precedence Call Request

Interworking AS-SIP signaling appliances directly serving IP end instruments MUST comply with the requirements in UCR 2008, Section 5.3.4.10.3.2.2, Required Behavior at Called IP End Instrument When Active Call is Preempted by Higher Precedence Call Request, when Active Call is Preempted by Higher Precedence Call Request.

5.3.4.18.6.2.3 Implementing Preemption on Behalf of Called IP End Instruments

Interworking AS-SIP signaling appliances directly serving IP end instruments MUST comply with the requirements in UCR 2008, Section 5.3.4.10.3.2.3, Implementing Preemption on Behalf of Called IP End Instruments. In addition, interworking AS-SIP signaling appliances directly serving IP end instruments MUST meet the following enumerated requirements.

Endpoint Preemption of an Active Call

5.3.4.18.6.2.3.1 When an AS-SIP signaling appliance performs endpoint preemption of an active call on behalf of a called IP end instrument and the AS-SIP signaling appliance is acting as an interworking gateway to the PSTN on behalf of the call to be preempted, the interworking AS-SIP signaling appliance MUST:

5.3.4.18.6.2.3.1.1 Activate user signaling (i.e,. preemption tone) at the local IP end instrument where the existing call is being preempted.

5.3.4.18.6.2.3.1.2 Send a REL with the cause value 8 “Preemption” or 9 “Preemption -- Circuit reserved for reuse” to the CCS7 network.

5.3.4.18.6.2.3.1.3 The end office serving the TDM end instrument will respond with a RLC.

5.3.4.18.6.2.3.1.4 When the local IP end instrument goes on-hook the interworking AS-SIP signaling appliance activates user signaling (i.e. precedence ringing tone) at the local IP end instrument and sends a 180 ringing to the remote AS-SIP signaling appliance serving the calling IP end instrument whose precedence call request has initiated the endpoint preemption. The remote AS-SIP signaling appliance will activate user signaling (i.e. precedence ringback tone) to the calling IP end instrument. And the call setup for the precedence call request continues as usual.

NOTE: If the precedence call request originated at a TDM end instrument then the originating gateway will translate the 180 Ringing into an ACM that is forwarded to the EO serving the calling TDM end instrument which will activate the precedence ringback tone at the calling TDM end instrument.

NOTE: If the precedence call request originated at a TDM end instrument and the interworking AS-SIP signaling appliance that is conducting the endpoint preemption is also the originating gateway for the precedence call request then when the local IP end instrument goes on-hook the interworking AS-SIP signaling appliance will directly create and send the ACM over the CCS7 network to the EO serving the calling TDM end instrument.

Endpoint Preemption of an Inbound Call Request

5.3.4.18.6.2.3.2 When an AS-SIP signaling appliance performs endpoint preemption of an inbound call request on behalf of a called IP end instrument and the AS-SIP signaling appliance is acting as an originating gateway for the inbound call request to be preempted, the interworking AS-SIP signaling appliance MUST:

5.3.4.18.6.2.3.2.1 Send a termination message to the local IP end instrument to end the current inbound call request that is being preempted in favor of the new higher precedence call request. The termination message will terminate the ringing tone.

NOTE: There is no particular purpose to playing the preemption tone as the phone is on-hook.

5.3.4.18.6.2.3.2.2 Send a REL with the cause value 8 “Preemption” or 9 “Preemption -- Circuit reserved for reuse” onto the CCS7 network to the end office serving the calling TDM end instrument.

5.3.4.18.6.2.3.2.3 The end office serving the TDM end instrument will respond with a RLC.

5.3.4.18.6.2.3.2.4 The interworking AS-SIP signaling appliance activates user signaling (i.e. precedence ringing tone) at the local IP end instrument and a 180 ringing to the remote AS-SIP signaling appliance serving the calling IP end instrument whose precedence call request has initiated the endpoint preemption. The remote AS-SIP signaling appliance will activate user signaling (i.e., precedence ringback tone) to the calling IP end instrument. And the call setup for the precedence call request continues as usual.

NOTE: If the precedence call request originated at a TDM end instrument then the originating gateway will translate the 180 Ringing into an ACM that is forwarded to the EO serving the calling TDM end instrument which will activate the precedence ringback tone at the calling TDM end instrument.

NOTE: If the precedence call request originated at a TDM end instrument and the interworking AS-SIP signaling appliance that is conducting the endpoint preemption is also the originating gateway for the precedence call request then the interworking AS-SIP signaling appliance will directly create and send the ACM over the CCS7 network to the EO serving the calling TDM end instrument.

Endpoint Preemption of an Outbound Call Request

5.3.4.18.6.2.3.3 When an AS-SIP signaling appliance performs endpoint preemption of an outbound call request on behalf of a called IP end instrument, and the AS-SIP signaling appliance is acting as a terminating gateway for the outbound call request to be preempted, the AS-SIP signaling appliance MUST:

5.3.4.18.6.2.3.3.1 Interrupt current user signaling associated with the outbound call request (e.g., ringback) and activate user signaling (i.e., preemption tone) at the local IP end instrument where the existing call is being preempted

5.3.4.18.6.2.3.3.2 Send a REL with the cause value 8 “Preemption” or 9 “Preemption -- Circuit reserved for reuse” onto the CCS7 network.

5.3.4.18.6.2.3.3.3 The end office serving the TDM end instrument will respond with a RLC.

5.3.4.18.6.2.3.3.4 Upon the receiver going on-hook, the local interworking AS-SIP signaling appliance will continue the call setup for the higher precedence call by activating user signaling at the local IP end instrument (i.e., precedence ringing tone), sending a 180 ringing response to the remote AS-SIP signaling appliance, and so forth.

NOTE: If the precedence call request originated at a TDM end instrument then the originating gateway will translate the 180 Ringing into an ACM that is forwarded to the EO serving the calling TDM end instrument which will activate the precedence ringback tone at the calling TDM end instrument.

NOTE: If the precedence call request originated at a TDM end instrument and the interworking AS-SIP signaling appliance that is conducting the endpoint preemption is also the originating gateway for the precedence call request then when the local IP end instrument goes on-hook the interworking AS-SIP signaling appliance will directly create and send the ACM over the CCS7 network to the EO serving the calling TDM end instrument.

<u>Remote Signaling Appliance Response to Notification of IP endpoint Preemption</u>

5.3.4.18.6.3 Network Preemption

The Network Preemption requirements set forth in this document specifically cover the network preemption scenarios whereby the interworking AS signaling appliance either:

1. Directly serves an IP end instrument that is the source of the precedence level call request for which preemption is sought and as the terminating gateway for the precedence level call request for which preemption is sought, or

2. Operates as the originating gateway for the precedence level call request for which preemption is sought and directly serves an IP end instrument that is the destination of the precedence level call request for which preemption is sought.

3. Operates as the originating gateway for the precedence level call request for which preemption is sought, or

4. Operates as the terminating gateway for the precedence level call request for which preemption is sought.

5.3.4.18.6.3.1 Circumstances under which an Interworking AS-SIP Signaling Appliance Performs Network Preemption

Interworking AS-SIP signaling appliances directly serving IP end instruments MUST comply with the requirements in UCR 2008, Section 5.3.4.10.3.3.1, Circumstances under which an AS-SIP Signaling Appliance Performs Network Preemption.

5.3.4.18.6.3.2 Implementing the Network Preemption

Interworking AS-SIP signaling appliances directly serving IP end instruments MUST comply with the requirements in UCR 2008, Section 5.3.4.10.3.3.2, Implementing the Network Preemption. In addition, interworking AS-SIP signaling appliances directly serving IP end instruments MUST meet the following enumerated requirements.

Network Preemption of Active Call

EI > CCS7 .> Sig Appl.> EI

5.3.4.18.6.3.2.1 When an interworking AS-SIP signaling appliance performs a network preemption of an active call (wherein the interworking AS-SIP signaling appliance directly serves an IP end instrument whose call is to be preempted AND serves as the inter-working

gateway to the PSTN on behalf of the call to be preempted) then the interworking AS-SIP signaling appliance MUST:

5.3.4.18.6.3.2.1.1 Activate the preemption tone at the local IP end instrument for a minimum of 3 seconds and then send a termination message to the local IP end instrument.

5.3.4.18.6.3.2.1.2 Send a REL with the cause value 8 “Preemption” or 9 “Preemption -- Circuit reserved for reuse” onto the CCS7 network.

5.3.4.18.6.3.2.1.3 The end office serving the TDM end instrument will respond with a RLC.

Network Preemption of an Inbound Call Request

5.3.4.18.6.3.2.2 When an interworking AS-SIP signaling appliance performs a network preemption of an inbound call request to a directly served IP end instrument (receiver is on-hook) and is also acting as an originating gateway for the inbound call request to be preempted, the interworking AS-SIP signaling appliance MUST:

5.3.4.18.6.3.2.2.1 Send a REL with the cause value 8 “Preemption” or 9 “Preemption -- Circuit reserved for reuse” onto the CCS7 network.

5.3.4.18.6.3.2.2.2 The end office serving the TDM end instrument will respond with a RLC.

5.3.4.18.6.3.2.2.3 Conduct call termination with the local IP end instrument which deactivates the ringing tone.

Network Preemption of an Outbound Call Request

5.3.4.18.6.3.2.3 When an interworking AS-SIP signaling appliance performs a network preemption of an outbound call request from a directly served IP end instrument that has not received a 2xx response and is also acting as a terminating gateway for the outbound call request being preempted, the interworking AS-SIP signaling appliance MUST:

5.3.4.18.6.3.2.3.1 Send a REL with the cause value 8 “Preemption” or 9 “Preemption -- Circuit reserved for reuse” onto the CCS7 network.

5.3.4.18.6.3.2.3.2 The end office serving the TDM end instrument will respond with a RLC.

5.3.4.18.6.3.2.3.3 Deactivate any user signaling (e.g., ringback), activate the preemption tone for a minimum of 3 seconds and then conduct call termination.

Network Preemption of Call Request (Interworking AS-SIP Signaling Appliance does not directly serve one of the preempted IP End Instruments)

5.3.4.18.6.3.2.4 When an interworking AS-SIP signaling appliance acting as an originating gateway for a call request intended for a remote EI not directly served by the interworking AS-SIP signaling appliance initiates a preemption of the call request (for which a 2xx response has not yet been received) the interworking AS-SIP signaling appliance MUST:

5.3.4.18.6.3.2.4.1 If an early dialog has been established, send a BYE or CANCEL request to the-AS-SIP signaling appliance directly serving the called IP end instrument in the preempted call request or to the interworking AS-SIP signaling appliance acting as a terminating gateway when the destination of the preempted call request is a TDM end instrument.

- If the preemption was caused by a lack of network resources on the IP side (e.g., call count at provisioned threshold) then the BYE or CANCEL request MUST include a Reason header whose reason-params has the value preemption ;cause=5 ;text="Network Preemption".

- If the preemption was caused by a lack of network resources on the TDM side (e.g., all TDM circuits on inter-working gateway are busy) then the BYE or CANCEL request MUST have a Reason header whose reason-params has the value preemption ;cause=4 ;text="Non-IP Preemption"

5.3.4.18.6.3.2.4.2 If an early dialog has NOT been established, then if a provisional response has already been received or if, not, then upon receipt of a provisional response send a CANCEL[4] request to the-AS-SIP signaling appliance directly serving the called IP end instrument in the preempted call request or to the interworking AS-SIP signaling appliance acting as a terminating gateway when the destination of the preempted call request is a TDM end instrument.

- If the preemption was caused by a lack of network resources on the IP side (e.g., call count at provisioned threshold) then the CANCEL request MUST include a Reason header whose reason-params has the value preemption ;cause=5 ;text="Network Preemption".

- If the preemption was caused by a lack of network resources on the TDM side (e.g., all TDM circuits on inter-working gateway are busy) then the CANCEL

[4] If the interworking AS-SIP signaling appliance has not received any provisional response it MUST wait to receive a provisional response before sending the CANCEL. In the event the first response is a final response or a provisional response that creates an early dialog (i.e. 101-199 with a tag in the 'To' header) then the interworking AS-SIP signaling appliance sends a BYE instead of a CANCEL.

request MUST include a Reason header whose reason-params has the value preemption ;cause=4 ;text="Non-IP Preemption"

5.3.4.18.6.3.2.4.3 The interworking AS-SIP signaling appliance will receive a 200 OK response to the BYE or CANCEL. In the case of a CANCEL the interworking AS-SIP signaling appliance will usually receive a 487 Request Terminated to the INVITE.

5.3.4.18.6.3.2.4.4 Send a REL with the cause value 8 “Preemption” or 9 “Preemption -- Circuit reserved for reuse” onto the CCS7 network.

5.3.4.18.6.3.2.4.5 The end office serving the TDM end instrument will respond with a RLC.

5.3.4.18.6.3.2.5 When an interworking AS-SIP signaling appliance performs a network preemption of a call request whereby the interworking AS-SIP signaling appliance is acting as a terminating gateway on behalf of the call request to be preempted AND does not directly serve an IP end instrument whose call is to be preempted, then the interworking AS-SIP signaling appliance MUST:

5.3.4.18.6.3.2.5.1 Send a 488 (Not Acceptable Here) response code that SHOULD include a “Warning” header with warning code 370 (Insufficient Bandwidth) over the IP network toward the AS-SIP signaling appliance directly serving the IP end instrument whose call request is being preempted or to the interworking AS-SIP signaling appliance acting as an originating gateway when a TDM end instrument is the originator of the call.[5]

- If the preemption was caused by a lack of network resources on the IP side (e.g., call count at provisioned threshold) then the 488 response MUST include a Reason header whose reason-params has the value preemption ;cause=5 ;text="Network Preemption".

- If the preemption was caused by a lack of network resources on the TDM side (e.g., all TDM circuits on inter-working gateway are busy) then the 488 response MUST include a Reason header whose reason-params has the value preemption ;cause=4 ;text="Non-IP Preemption"

5.3.4.18.6.3.2.5.2 The interworking AS-SIP signaling appliance will receive an ACK response to the 488 response.

[5] Call has not progressed to the point that the interworking AS-SIP signaling appliance has received an ACK to a 200 OK INVITE.

5.3.4.18.6.3.2.5.3 Send a REL with the cause value 8 “Preemption” or 9 “Preemption -- Circuit reserved for reuse” onto the CCS7 network.

5.3.4.18.6.3.2.5.4 The end office serving the TDM end instrument will respond with a RLC.

Network Preemption of an Active Call (Interworking AS-SIP Signaling Appliance Receives REL)

5.3.4.18.6.3.2.6 When an interworking AS-SIP signaling appliance receives a REL with a cause value of 8 “Preemption” or 9 “Preemption -- Circuit reserved for reuse” for an active call and does NOT directly serve an IP end instrument whose call is to be preempted, the interworking AS-SIP signaling appliance MUST:

5.3.4.18.6.3.2.6.1 Send an RLC response onto the CCS7 network.

5.3.4.18.6.3.2.6.2 Send a BYE with a Reason header with a reason-value of preemption ;cause=4 ;text="Non-IP Preemption" intended for either the AS-SIP signaling appliance directly serving the IP end instrument whose call is to be preempted or another interworking AS-SIP signaling appliance in a TDM bridging scenario.

5.3.4.18.6.3.2.6.3 The interworking gateway will receive a 200 OK response.

5.3.4.18.6.3.2.7 When an interworking AS-SIP signaling appliance receives a REL with a cause value of 8 “Preemption” or 9 “Preemption -- Circuit reserved for reuse” for an active call AND directly serves the IP end instrument whose call is to be preempted then the interworking AS-SIP signaling appliance MUST:

5.3.4.18.6.3.2.7.1 Send a RLC response onto the CCS7 network.

5.3.4.18.6.3.2.7.2 Activate the preemption tone at the local IP end instrument for a minimum of 3 seconds and then send a termination message to the local IP end instrument.

NOTE: In the case of a SIP end instrument, it is recommended that the interworking AS-SIP signaling appliance send a SIP BYE request with a Reason header whose reason-params has the value preemption ;cause=4 ;text="Non-IP Preemption").

Network Preemption of Call Request (Interworking AS-SIP Signaling Appliance Receives REL)

5.3.4.18.6.3.2.8 When an interworking AS-SIP signaling appliance is acting as an originating gateway for a call request (call request originated on TDM network) for which the interworking AS-SIP signaling appliance receives a REL with a cause value of 8 “Preemption” or 9 “Preemption -- Circuit reserved for reuse,” and the interworking AS-SIP signaling appliance

does NOT directly serve an IP end instrument whose call is to be preempted, and has not yet received a 2xx response, the interworking AS-SIP signaling appliance MUST:

5.3.4.18.6.3.2.8.1 Send a RLC response onto the CCS7 network.

5.3.4.18.6.3.2.8.2 If an early dialog has been established, send a BYE or CANCEL request with a Reason header whose reason-params has the value preemption ;cause=4 ;text="Non-IP Preemption" either to the AS-SIP signaling appliance directly serving the called IP end instrument in the preempted call request or to the interworking AS-SIP signaling appliance acting as a Terminating Gateway if the destination of the preempted call request is a TDM end instrument.

5.3.4.18.6.3.2.8.3 If an early dialog has not been established, then if a provisional response has already been received or if, not, then upon receipt of a provisional response send a CANCEL[6] request with a Reason header whose reason-params has the value preemption ;cause=4 ;text="Non-IP Preemption" either to the AS-SIP signaling appliance directly serving the called IP end instrument in the preempted call request or to the interworking AS-SIP signaling appliance acting as a terminating gateway if the destination of the preempted call request is a TDM end instrument.

5.3.4.18.6.3.2.8.4 The interworking AS-SIP signaling appliance will receive a 200 OK response to the BYE or CANCEL. The interworking AS-SIP signaling appliance will usually receive a 487 Request Terminated to the INVITE.

5.3.4.18.6.3.2.9 When an interworking AS-SIP signaling appliance is acting as a terminating gateway for a call request for which the interworking AS-SIP signaling appliance receives a REL with a cause value of 8 “Preemption” or 9 “Preemption -- Circuit reserved for reuse,” and the interworking AS-SIP signaling appliance does NOT directly serve an IP end instrument whose call is to be preempted, the interworking AS-SIP signaling appliance MUST:

5.3.4.18.6.3.2.9.1 Send an RLC response onto the CCS7 network.

5.3.4.18.6.3.2.9.2 Send a 488 (Not Acceptable Here) response code that SHOULD include a “Warning” header with warning code 370 (Insufficient Bandwidth) with a Reason header whose Reason-params has the value preemption;cause=4 ;text=“Non-IP Preemption” over the IP network toward the AS-SIP signaling appliance directly serving the IP end instrument whose call

[6] If interworking AS-SIP signaling appliance has not received any provisional response it MUST wait to receive a provisional response before sending the CANCEL. In the event the first response is a final response or a provisional response that creates an early dialog (i.e. 101-199 with a tag in the ‘To’ header) then the interworking AS-SIP signaling appliance sends a BYE instead of a CANCEL.

request is being preempted or to the interworking AS-SIP signaling appliance acting as an originating gateway when a TDM end instrument is the originator of the call.

5.3.4.18.6.3.2.10 When an interworking AS-SIP signaling appliance receives a REL with a cause value of 8 “Preemption” or 9 “Preemption – Circuit reserved for reuse” for a call request initiated by a TDM end instrument and whose destination is an IP end instrument directly served by the interworking AS-SIP signaling appliance then the interworking AS-SIP signaling appliance MUST:

5.3.4.18.6.3.2.10.1 Send an RLC response onto the CCS7 network

5.3.4.18.6.3.2.10.2 Deactivate the ringing tone at the local IP end instrument, and conduct call termination with the local IP end instrument

NOTE: In the case of a SIP end instrument, it is recommended that the call termination message sent by the interworking AS-SIP signaling appliance consist of a SIP BYE request or CANCEL request (as appropriate) with a Reason header whose reason-params has the value preemption ;cause=4 ;text="Non-IP Preemption").

5.3.4.18.6.3.2.11 When an interworking AS-SIP signaling appliance receives a REL with a cause value of 8 “Preemption” or 9 “Preemption – Circuit reserved for reuse” for a call request initiated by a directly served IP end instrument then the interworking AS-SIP signaling appliance MUST:

5.3.4.18.6.3.2.11.1 Send an RLC response onto the CCS7 network.

5.3.4.18.6.3.2.11.2 Deactivate user signaling (e.g. ringback), activate the preemption tone for a minimum of 3 seconds and then conduct call termination.

NOTE: In the case of a SIP end instrument, it is recommended that the call termination message sent by the interworking AS-SIP signaling appliance consist of a 488 response with a Reason header whose reason-params has the value preemption ;cause=4 ;text="Non-IP Preemption").

5.3.4.19 Supplementary Services

5.3.4.19.1 Introduction

Many calling features are traditional to the TDM network and the PSTN. Within the PSTN, some calling features are required by law and regulated by the Federal Communications Commission (FCC). This specification is used within the context of a private network and thus is not necessarily subject to the same laws and regulations

The focus of this specification is on the signaling-related functions and interfaces supported by the signaling appliances interfacing with the DISN WAN. This document places no restrictions on the line-side signaling method employed between AS-SIP signaling appliances and the IP end instruments served by those AS-SIP signaling appliances. The IP telephony signaling employed by and with the end instrument may be SIP, H.323, or proprietary. The only requirements on the line side are of a functional nature relating to the user experience (for example, the sequence of events experienced by a user of an IP end instrument when a call is to be preempted). In every case, the primary call flow diagram and description depicts and details the signaling flow across the DISN WAN but not the signaling across the LAN between the AS-SIP signaling appliance serving an IP end instrument and the end instrument. In some cases, a secondary call flow diagram is provided that does depict SIP signaling down to the SIP end instrument in order to enhance the reader's understanding of the given call flow. However, it is the AS-SIP message sequences across the WAN and the AS-SIP/ISUP translations and message sequences that are governed by this specification. When depicted, the SIP message flows across the LAN are merely instructional.

The call flow diagrams assume the two-tier hierarchical architecture whereby for incoming or outgoing calls to be established across the DISN WAN, the LSC at a B/P/C/S exchanges its AS-SIP messages with an assigned Softswitch.

Call features 1, 2, 3, 4, and 5 are required for the near-term open loop architecture. In addition, the near-term open loop architecture calls for AS-SIP to support the fax and modem services per UCR 2008, Section 5.3.4.13.9, Modem on IP Networks.

5.3.4.19.2 Point-to-Point Call

Signaling requirements for point-to-point calls are described for the following three call conditions:

- No precondition
- Segmented precondition
- End-to-end precondition

5.3.4.19.2.1 IP-to-IP Call Type

See UCR 2008, Section 5.3.4.13.2.1, IP-to-IP Call Type.

5.3.4.19.2.2 TDM Bridging Call Type

5.3.4.19.2.2.1 Figure 5.3.4-35, Successful Basic TDM Bridging Call (No Preconditions), depicts the sequence of AS-SIP and ISUP messages between the end office serving TDM Party A and

the end office serving TDM Party B employed to establish and then tear down a telephony session traversing the IP WAN. The call flow diagram depicts reliable provisional responses but not the use of preconditions.

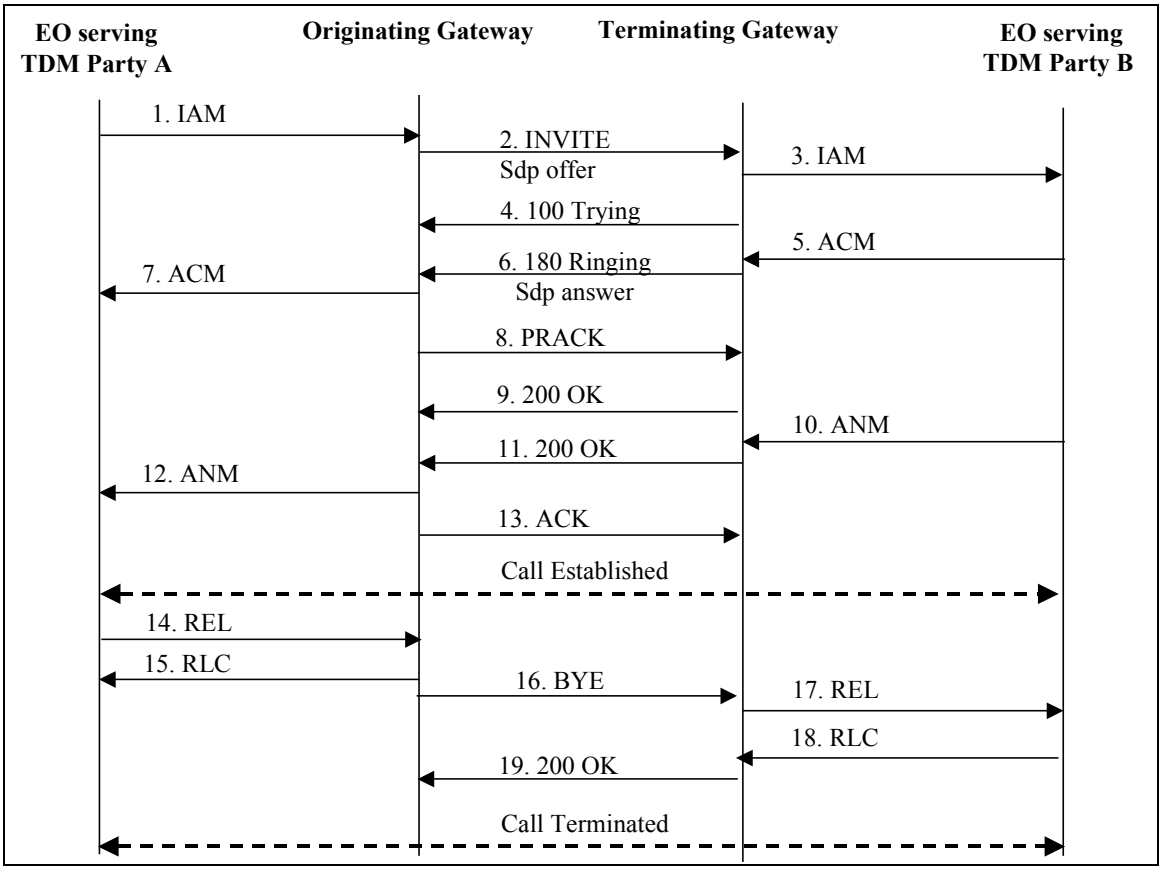


Figure 5.3.4-35. Successful Basic TDM Bridging Call (No Preconditions)

Call Establishment

STEP	INSTRUCTION
1	The end office serving TDM Party A detects an off-hook and receives the dialed string. The end office sends an IAM through the CCS7 network to the originating gateway.
2	The originating gateway receives the IAM, creates an INVITE, and sends the INVITE to the terminating gateway.
3	The terminating gateway receives the INVITE, creates an IAM, and sends the IAM to the end office serving TDM Party B.
4	The terminating gateway sends a 100 (Trying) response code to the originating gateway.

STEP	INSTRUCTION
5	The end office serving TDM Party B initiates ringing of the end instrument and sends an ACM to the terminating gateway.
6	The terminating gateway creates a 180 (Ringing) response code and sends the 180 (Ringing) response to the originating gateway.
7	The originating gateway receives the 180 (Ringing), creates an ACM, and sends the ACM to the end office serving TDM Party A.
8	The originating gateway sends a PRACK to the terminating gateway.
9	The terminating gateway sends a 200 (OK) PRACK to the originating gateway.
10	When TDM Party B goes off hook (i.e., answers the call), the end office serving TDM Party B sends an ANM to the terminating gateway.
11	The terminating gateway creates a 200 (OK) response code and sends the 200 (OK) response code to the originating gateway.
12	The originating gateway receives the 200 (OK), creates an ANM, and sends the ANM to the end office serving TDM Party A.
13	The originating gateway sends an ACK to the terminating gateway.

Call Release

STEP	INSTRUCTION
14	The end office serving TDM Party A detects an on-hook and sends an REL to the originating gateway.
15	The originating gateway sends an RLC to the end office serving TDM Party A.
16	The originating gateway receives the RLC and sends a BYE over the IP network to the terminating gateway.
17	The terminating gateway receives the BYE and sends REL to the end office serving TDM Party A.
18	The end office serving TDM Party A sends an RLC to the terminating gateway.
19	The terminating gateway sends a 200 (OK) response to the originating gateway.

5.3.4.19.2.2.2 Figure 5.3.4-36 depicts the sequence of AS-SIP and ISUP messages between the end office serving TDM Party A and the end office serving TDM Party B employed to establish a telephony session across the IP WAN, employing a segmented precondition.

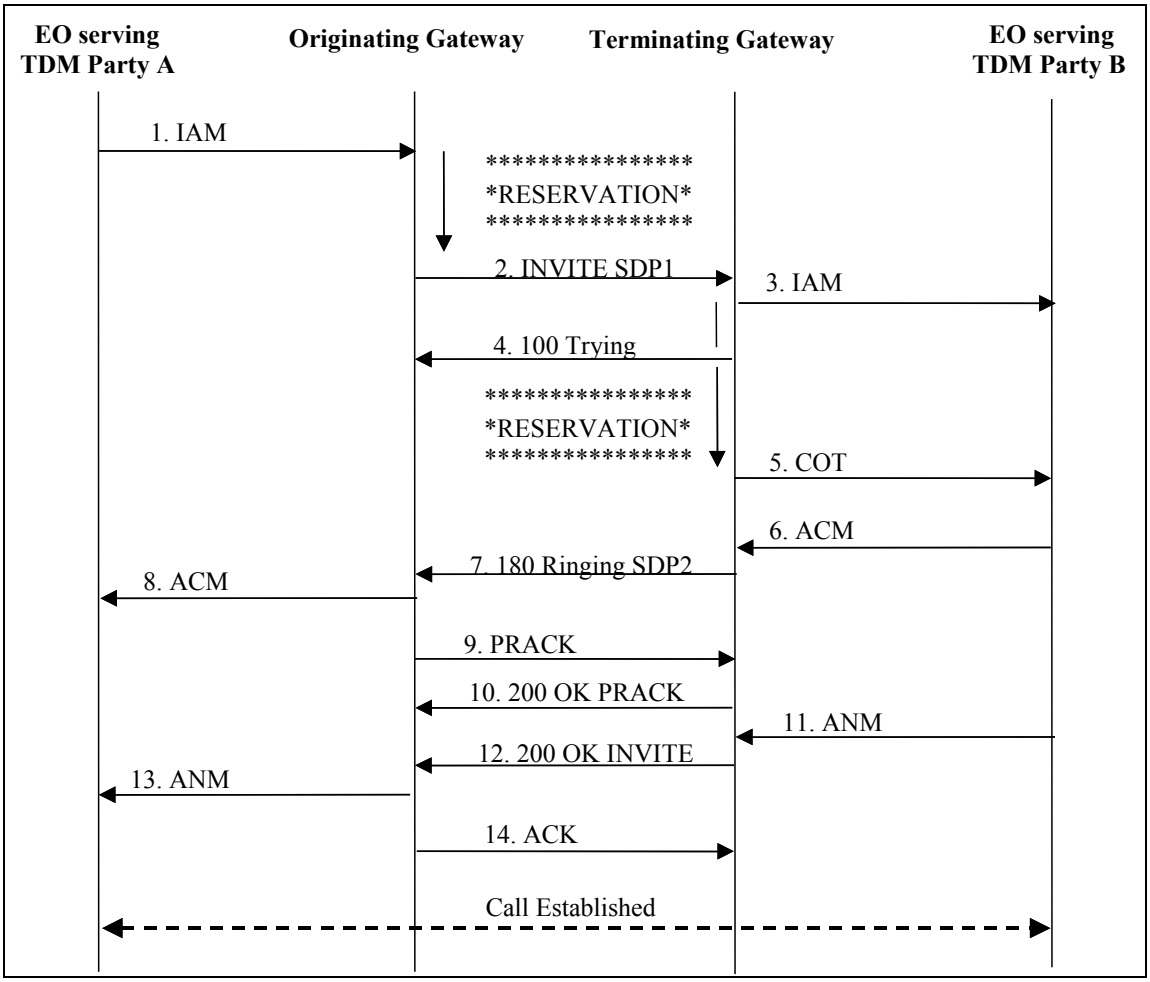


Figure 5.3.4-36. Successful Basic TDM Bridging Call (Segmented Precondition)

Call Establishment

STEP	INSTRUCTION
1	The end office serving TDM Party A detects an off-hook and receives the dialed string. The end office sends an IAM through the CCS7 network to the originating gateway.
2	Upon receiving the IAM from the end office serving TDM Party A, the originating gateway satisfies its local precondition before sending an INVITE to the terminating gateway. The INVITE contains a segmented precondition offer using SDP attributes described in RFC 3312. The precondition offer includes, at a minimum, a media ("m=") line, a connection ("c=") line, at least two current-status lines (local and remote), and at least two desired-status lines (local and remote). The originating gateway forwards the INVITE to the terminating gateway.
3	The terminating gateway receives the INVITE, creates an IAM, sets the Continuity check indicator of the Nature of Connection Indicators to "Continuity check performed on a previous circuit," or "Continuity check required on this circuit," and sends the IAM to the end office serving TDM Party B. In addition, the terminating gateway goes about satisfying its local preconditions. NOTE: If the Terminating Gateway does not make use of the COT message then the Terminating Gateway can refrain from initiating any CCS7 messaging until after the resources have been reserved.
4	The terminating gateway sends a 100 (Trying) to the originating gateway.
5	After all SIP preconditions have been met, the terminating gateway sends a Continuity Testing (COT) message to the end office serving TDM Party B so that the end office can send a ring tone to TDM Party B. NOTE: If the Terminating Gateway did not send an IAM in step 3 then the Terminating Gateway sends an IAM with the continuity check indicator of the Nature of Connection Indicators set to '00' "continuity check not required".
6	The end office serving TDM Party B sends an ACM to the terminating gateway.
7	When the terminating gateway receives an ACM from the end office serving TDM Party B, it creates a 180 (Ringing) with an answer to the segmented precondition offer that includes, at a minimum, a media ("m=") line, a connection ("c=") line, at least two current-status lines, and at least two desired-status lines. The terminating gateway sends the 180 (Ringing) to the originating gateway.
8	The originating gateway receives the 180 (Ringing) and sends the ACM to the end office serving TDM Party A.
9	The originating gateway sends a PRACK to the terminating gateway.
10	The terminating gateway sends a 200 (OK) PRACK to the originating gateway.

STEP	INSTRUCTION
11	When TDM Party B goes off hook (i.e., answers the call), the end office serving TDM Party B sends an ANM to the terminating gateway.
12	The terminating gateway receives the ANM, creates a 200 (OK) INVITE, and sends the 200 (OK) INVITE to the originating gateway.
13	The originating gateway receives the 200 (OK), creates an ANM, and sends the ANM to the end office serving TDM Party A.
14	The originating gateway sends an ACK to the terminating gateway.

The call is now established.

5.3.4.19.2.2.3 Figure 5.3.4-37, Successful Basic TDM Bridging Call (End-to-End Precondition), depicts the sequence of AS-SIP and ISUP messages between the end office serving TDM Party A and the end office serving TDM Party B employed to establish a telephony session across the IP WAN, employing a status-type end-to-end precondition.

Call Establishment

STEP	INSTRUCTION
1	The end office serving TDM Party A detects an off-hook and receives the dialed string. The end office sends an IAM through the CCS7 network to the originating gateway.
2	The originating gateway creates an INVITE containing an end-to-end precondition offer using SDP attributes described in RFC 3312. The precondition offer includes, at a minimum, a media (“m=”) line, a connection (“c=”) line, at least one current-status line, and at least one desired-status line. The originating gateway forwards the INVITE to the terminating gateway.
3	The terminating gateway receives the INVITE, creates an IAM, sets the Continuity check indicator of the Nature of Connection Indicators to “Continuity check performed on a previous circuit,” or “Continuity check required on this circuit,” and sends the IAM to the end office serving TDM Party B. NOTE: If the Terminating Gateway does not make use of the COT message then the Terminating Gateway can refrain from initiating any CCS7 messaging until after the it receives confirmation that the resources have been reserved and sends its acknowledgement in step 9.

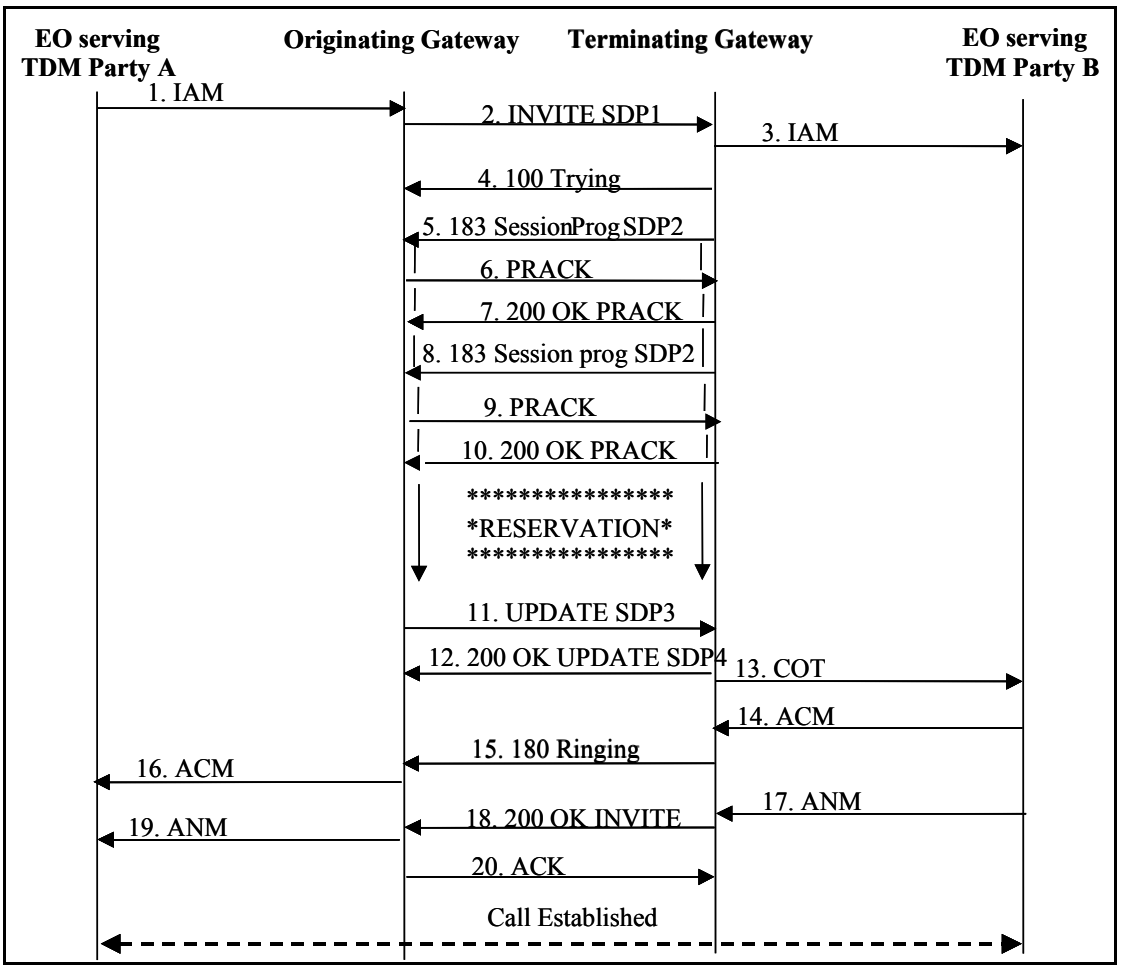


Figure 5.3.4-37. Successful Basic TDM Bridging Call (End-to-End Precondition)

STEP	INSTRUCTION
4	The terminating gateway sends a 100 (Trying) to the originating gateway.
5	The terminating gateway sends a 183 (Session Progress) to the originating gateway with an answer to the e2e precondition offer that includes, at a minimum, a media ("m=") line, a connection ("c=") line, at least one current-status line, at least one desired-status line, and at least one confirm-status line. The terminating gateway sends the 183 (Session Progress) to the originating gateway. The terminating gateway and the originating gateway attempt to reserve the resources needed to fulfill the preconditions.
6	The originating gateway sends a PRACK to the terminating gateway.
7	The terminating gateway sends a 200 (OK) PRACK to the originating gateway.

STEP	INSTRUCTION
8	The terminating gateway sends a 183 Session Progress with sdp (wherein the contents of the sdp body is an exact duplicate of the contents of sdp2 sent in step 5) to the originating gateway immediately after sending the 200 OK PRACK in order to notify the originating hateway that early media will be sent over the backward bearer path
9	The originating gateway sends a PRACK to the terminating gateway.
10	The terminating gateway sends a 200 (OK) PRACK to the originating gateway.
11	When the originating gateway receives a confirmation that it has met its precondition (e.g., receives an RSVP RESV message), then it sends an UPDATE to the terminating gateway with an updated offer reflecting compliance with its part of the precondition. The updated precondition offer includes, at a minimum, a media ("m=") line, a connection ("c=") line, at least one current-status line, and at least one desired-status line.
12	The terminating gateway receives a confirmation that it has met its precondition (e.g., receives an RSVP RESV message) and sends a 200 (OK) UPDATE to the originating gateway with an updated precondition answer reflecting compliance with its part of the precondition as well as the most recent updated information from the UPDATE offer. The updated answer includes, at a minimum, a media ("m=") line, a connection ("c=") line, at least one current-status line, at least one desired-status line.
13	Now that all SIP preconditions have been met, the terminating gateway sends a COT message to the end office serving TDM Party B so that the end office can send a ring tone to TDM Party B. NOTE: If the Terminating Gateway did not send an IAM in step 3 then the Terminating Gateway sends an IAM with the continuity check indicator of the Nature of Connection Indicators set to '00' "continuity check not required".
14	The end office serving TDM Party B sends an ACM to the terminating gateway.
15	The terminating gateway receives the ACM, creates a 180 (Ringing), and sends the 180 (Ringing) to the originating gateway.
16	The originating gateway receives the 180 (Ringing), creates an ACM, and sends the ACM to the end office serving TDM Party A.
17	When TDM Party B goes off hook (i.e., answers the call), the end office serving TDM Party B sends an ANM to the terminating gateway.
18	The terminating gateway receives the ANM, creates a 200 (OK) INVITE, and sends the 200 (OK) INVITE to the originating gateway.
19	The originating gateway receives the 200 (OK), creates an ANM, and sends the ANM to the end office serving TDM Party A.
20	The originating gateway sends an ACK to the terminating gateway.

The call is now established.

5.3.4.19.2.3 TDM-to-IP Call Type

5.3.4.19.2.3.1 Figure 5.3.4-38, Successful Basic TDM-to-IP Call (No Preconditions), depicts the sequence of AS-SIP and ISUP messages between the end office serving TDM Party A and the LSC serving IP Party B employed to establish and then tear down a telephony session. The call flow diagram does not depict the use of preconditions.

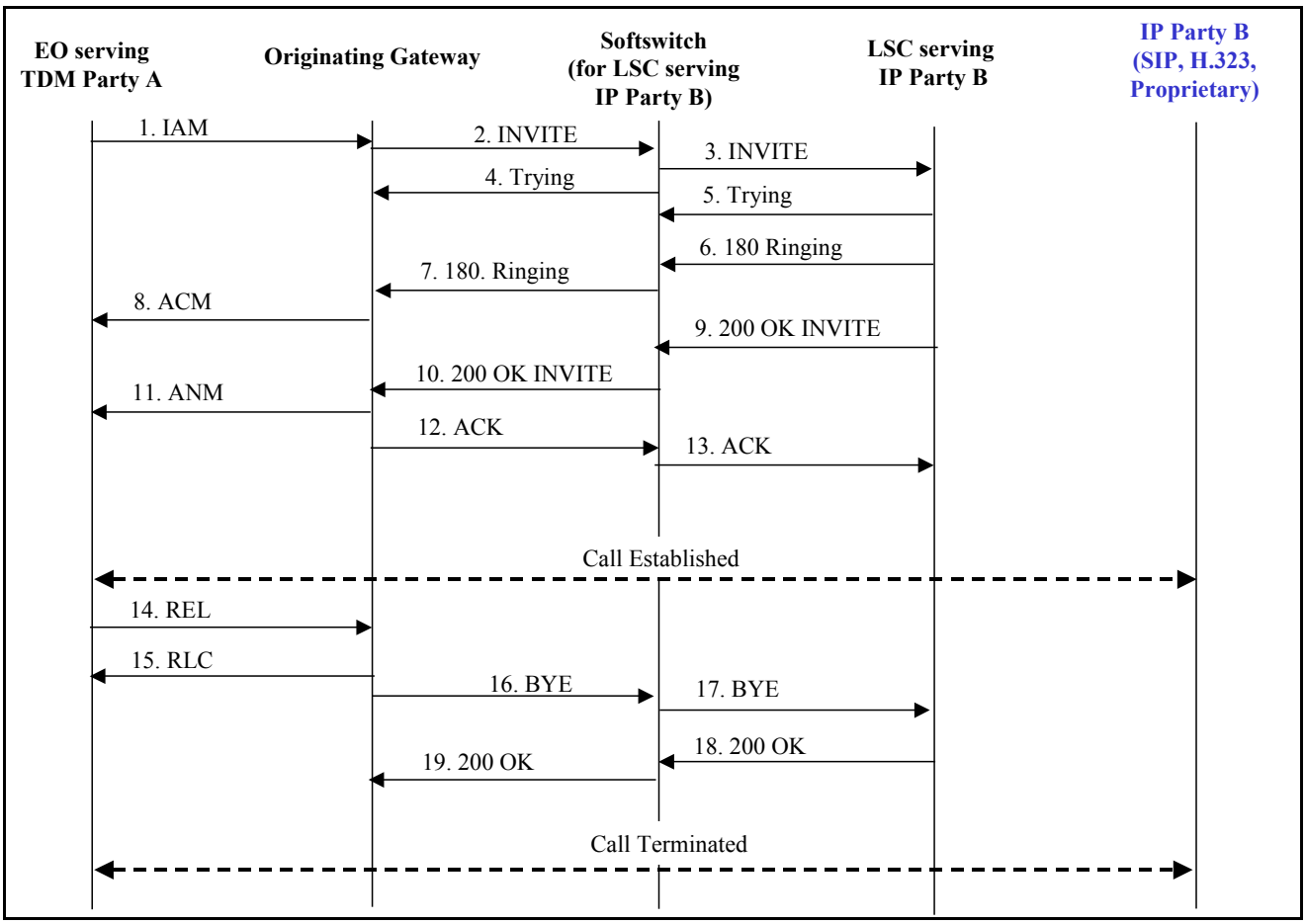


Figure 5.3.4-38. Successful Basic TDM-to-IP Call (No Preconditions)

Call Establishment

STEP	INSTRUCTION
1	The end office serving TDM Party A detects an off-hook and receives the dialed string. The end office sends an IAM through the CCS7 network to the originating gateway.
2	The originating gateway receives the IAM, creates an INVITE, and sends the INVITE to the Softswitch assigned to the LSC serving IP Party B.
3	The Softswitch receives the INVITE and forwards the INVITE to the LSC serving IP Party B. NOTE: Signaling between the LSC serving IP Party B and the end instrument serving IP Party B is not depicted.
4	The Softswitch sends a 100 (Trying) to the originating gateway.
5	The LSC serving IP Party B sends a 100 (Trying) to the Softswitch.
6,7	Assuming the end instrument is not busy, the LSC serving IP Party B sends a 180 (Ringing) to the Softswitch, and the Softswitch forwards the 180 (Ringing) to the originating gateway. NOTE: Signaling between the end instrument serving IP Party B and the LSC serving IP Party B is not depicted.
8	The originating gateway creates an ACM and sends it to the end office serving TDM Party A.
9, 10	When IP Party B goes off hook (i.e., answers the call), the LSC serving IP Party B sends a 200 (OK) to the Softswitch. It forwards the 200 (OK) to the originating gateway. NOTE: Signaling between the end instrument serving IP Party B and the LSC serving IP Party B is not depicted.
11	The originating gateway creates an ANM and sends it to the end office serving TDM Party A.
12, 13	The originating gateway sends an ACK to the Softswitch. The Softswitch forwards the ACK to the LSC serving IP Party B. NOTE: Signaling between the LSC serving IP Party B and the end instrument serving IP Party B is not depicted.

Call Release

STEP	INSTRUCTION
14	The end office serving TDM Party A detects on-hook and sends a REL to the originating gateway.
15	The originating gateway sends a RLC to the end office serving TDM Party A.
16	The originating gateway sends a BYE over the IP network to the Softswitch.
17	The Softswitch forwards the BYE to the LSC serving IP Party B. NOTE: Signaling between the LSC serving IP Party B and the end instrument serving IP Party B is not depicted.
18, 19	The LSC serving IP Party B sends a 200 (OK) to the Softswitch, and the Softswitch forwards the 200 (OK) to the originating gateway. NOTE: Signaling between the end instrument serving IP Party B and the LSC serving IP Party B is not depicted.

5.3.4.19.2.3.2 Figure 5.3.4-39 depicts the sequence of AS-SIP and ISUP messages between the end office serving TDM Party A and the LSC serving IP Party B employed to establish a telephony session, using a segmented precondition.

Call Establishment

STEP	INSTRUCTION
1	The end office serving TDM Party A detects an off-hook and receives the dialed string. The end office sends an IAM through the CCS7 network to the originating gateway.
2	Upon receiving the IAM from the end office serving TDM Party A, the originating gateway satisfies its local precondition before sending an INVITE to the Softswitch for the LSC serving IP Party B. The INVITE contains a segmented precondition offer using SDP attributes described in RFC 3312. The precondition offer includes, at a minimum, a media (“m=”) line, a connection (“c=”) line, at least two current-status lines (local and remote), and at least two desired-status lines (local and remote).
3	The Softswitch forwards the INVITE to the LSC serving IP Party B.
4	The Softswitch sends a 100 (Trying) to the originating gateway.

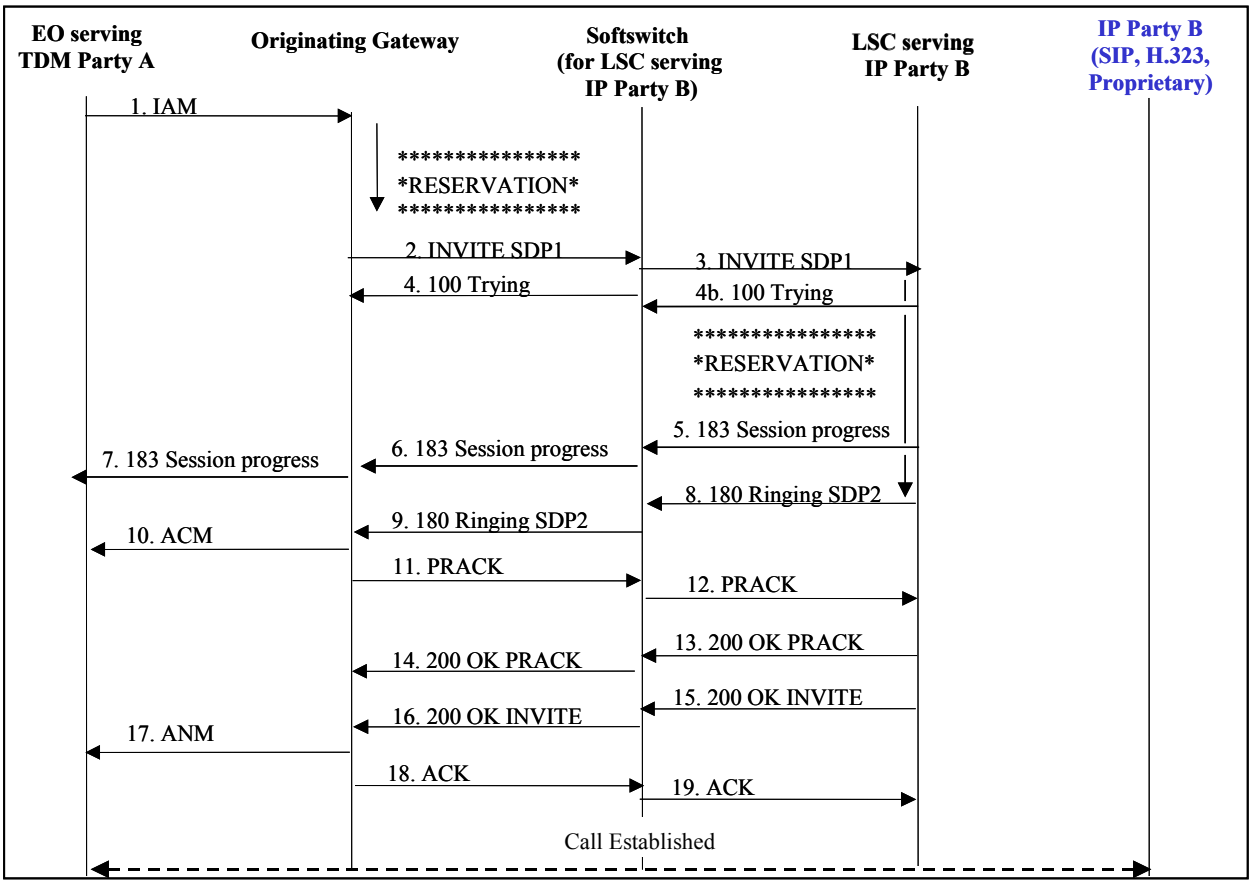


Figure 5.3.4-39. Successful Basic TDM-to-IP Call (Segmented Precondition)

STEP	INSTRUCTION
4b	The LSC serving IP Party B sends a 100 Trying to the Softswitch.
5, 6, 7	The LSC serving IP party B sends a 183 Session Progress with no sdp prior to sending the 180 ringing with an answer to the segmented precondition offer in order to notify the originating gateway that there is no early media and ring back must be generated locally.
8, 9	The LSC serving IP Party B satisfies its local precondition, notifies the IP end instrument of the pending call and sends a 180 (Ringing) with an answer to the segmented precondition offer that includes, at a minimum, a media (“m=”) line, a connection (“c=”) line, at least two current-status lines, and at least two desired-status lines to the Softswitch. The Softswitch forwards the 180 (Ringing) to the originating gateway. NOTE: Signaling between the LSC serving IP Party B and the end instrument serving IP Party B is not depicted.
10	The originating gateway receives the 180 (Ringing) and sends an ACM to the end office serving TDM Party A.

STEP	INSTRUCTION
11, 12	The originating gateway sends a PRACK to the Softswitch, and the Softswitch forwards the PRACK to the LSC serving IP Party B.
13, 14	The LSC serving IP Party B sends a 200 (OK) PRACK to the Softswitch, and the Softswitch forwards the 200 (OK) PRACK to the originating gateway.
15, 16	The LSC serving IP Party B sends a 200 (OK) INVITE to the Softswitch. The Softswitch forwards the 200 (OK) INVITE to the originating gateway. NOTE: Signaling between the IP end instrument serving IP Party B and the LSC serving IP Party B is not depicted.
17	The originating gateway receives the 200 (OK) INVITE and sends an ANM to the end office serving TDM Party A.
18, 19	The originating gateway sends the ACK to the Softswitch, which forwards the ACK to the LSC serving IP Party B. NOTE: Signaling between the LSC serving IP Party B and the IP end instrument serving IP Party B is not depicted.

The call is now established.

5.3.4.19.2.3.3 Figure 5.3.4-40 depicts the sequence of AS-SIP and ISUP messages between the end office serving TDM Party A and the LSC serving IP Party B employed to establish a telephony session-using a status-type end-to-end precondition.

Call Establishment

STEP	INSTRUCTION
1	The end office serving TDM Party A detects an off-hook and receives the dialed string. The end office sends an IAM through the CCS7 network to the originating gateway.
2	Upon receiving the IAM from the end office serving TDM Party A, the originating gateway sends an INVITE to the Softswitch for the LSC serving IP Party B. The INVITE contains an end-to-end (e2e) precondition offer using SDP attributes described in RFC 3312. The precondition offer includes, at a minimum, a media (“m=”) line, a connection (“c=”) line, at least 1 current-status line, and at least 1 desired-status line.
3	The Softswitch receives and forwards the INVITE to the LSC serving IP Party B.
4	The Softswitch sends a 100 (Trying) to the originating gateway.

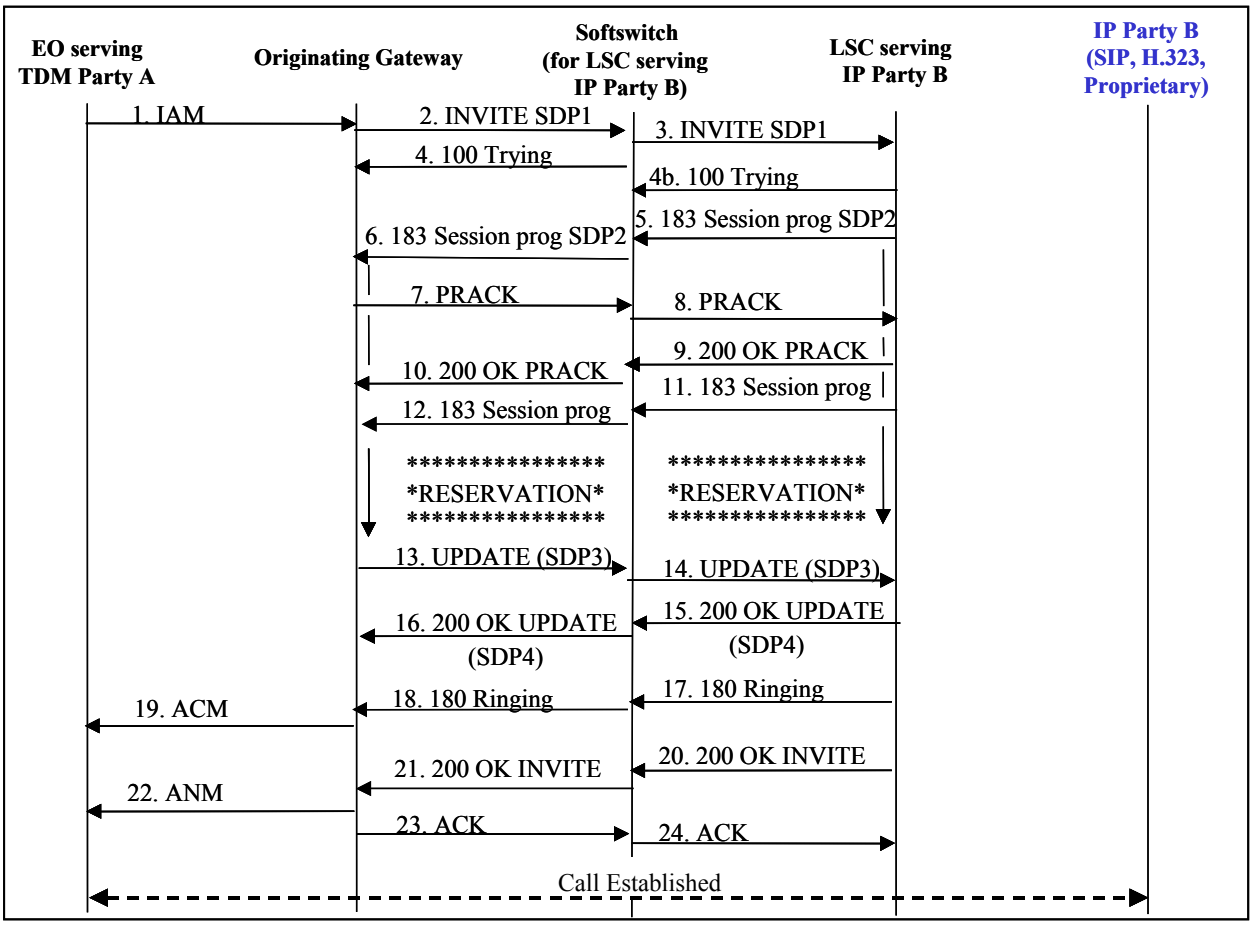


Figure 5.3.4-40. Successful Basic TDM-to-IP Call (End-to-End Precondition)

STEP	INSTRUCTION
4b	The LSC serving IP Party B sends a 100 Trying to the Softswitch
5, 6	The LSC serving IP Party B sends a 183 (Session Progress) to the Softswitch with an answer to the e2e precondition offer that includes, at a minimum, a media ("m=") line, a connection ("c=") line, at least one current-status line, at least one desired-status line, and at least one confirm-status line. The Softswitch forwards the 183 (Session Progress) to the originating gateway. The LSC serving IP Party B and the originating gateway attempt to reserve the resources needed to fulfill the preconditions.
7, 8	The originating gateway sends a PRACK to the Softswitch, and the Softswitch forwards the PRACK to the LSC serving IP Party B.
9, 10	The LSC serving IP Party B sends a 200 (OK) PRACK to the Softswitch, and the Softswitch forwards the 200 (OK) PRACK to the originating gateway.

STEP	INSTRUCTION
11, 12	The LSC serving IP party B sends a 183 Session Progress with no sdp immediately after sending the 200 OK PRACK in order to notify the originating gateway that it will not be receiving early media over the backward bearer path.
13, 14	When the originating gateway receives a confirmation that it has met its precondition (e.g., receives an RSVP RESV message), then it sends an UPDATE to the Softswitch with an updated offer reflecting compliance with its part of the precondition. The updated precondition offer includes, at a minimum, a media ("m=") line, a connection ("c=") line, at least one current-status line, and at least one desired-status line. The Softswitch forwards the UPDATE to the LSC serving IP Party B.
15, 16	The LSC serving IP Party B receives a confirmation that it has met its precondition (e.g., receives an RSVP RESV message) and sends a 200 (OK) UPDATE to the Softswitch with an updated precondition answer reflecting compliance with its part of the precondition as well as the most recent updated information from the UPDATE offer. The updated answer includes, at a minimum, a media ("m=") line, a connection ("c=") line, at least one current-status line, at least one desired-status line. The Softswitch forwards the 200 (OK) UPDATE to the originating gateway.
17, 18	The preconditions have been met so the LSC serving IP Party B notifies the IP end instrument of the pending call and sends a 180 (Ringing) to the Softswitch. The Softswitch forwards the 180 (Ringing) to the originating gateway. NOTE: Signaling between the LSC serving IP Party B and the end instrument serving IP Party B is not depicted.
19	The originating gateway receives the 180 (Ringing) and sends an ACM to the end office serving TDM Party A.
20, 21	The LSC serving IP Party B sends a 200 (OK) INVITE to the Softswitch. The Softswitch forwards the 200 (OK) INVITE to the originating gateway. NOTE: Signaling between the IP end instrument serving IP Party B and the LSC serving IP Party B is not depicted.
22	The originating gateway receives the 200 (OK) INVITE and sends an ANM to the end office serving TDM Party A.
23, 24	The originating gateway sends an ACK to the Softswitch and the Softswitch forwards the ACK to the LSC serving IP Party B. NOTE: Signaling between the LSC serving IP Party B and the end instrument serving IP Party B is not depicted.

The call is now established.

5.3.4.19.2.4 IP-to-TDM Call Type

5.3.4.19.2.4.1 Figure 5.3.4-41, Successful Basic IP-to-TDM Call (No Preconditions), depicts the sequence of AS-SIP and ISUP messages between the LSC serving IP Party A and the end office serving TDM Party B employed to establish and then tear down a telephony session. The call flow diagram does not depict the use of preconditions.

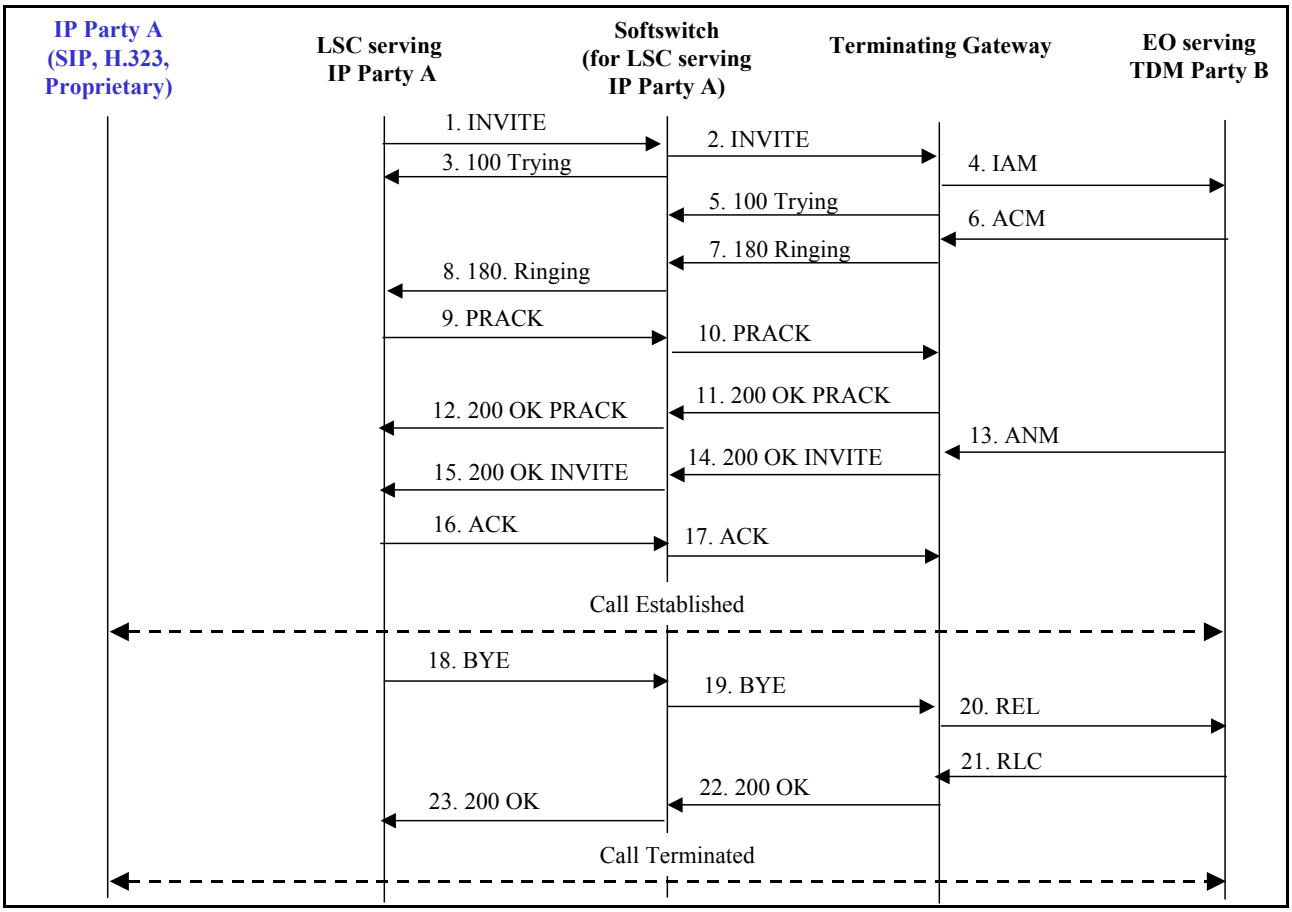


Figure 5.3.4-41. Successful Basic IP-to-TDM Call (No Preconditions)

Call Establishment

STEP	INSTRUCTION
1, 2	Upon receiving an initial call request message from IP Party A (not depicted in the call flow diagram), the LSC serving IP Party A sends an INVITE to its assigned Softswitch. The Softswitch forwards the INVITE to the terminating gateway. NOTE: Signaling between the end instrument serving Party A and the LSC serving IP Party A is not depicted.
3	The Softswitch sends 100 Trying to the LSC serving IP Party A.
4	The terminating gateway creates an IAM and sends the IAM to the end office serving TDM Party B.
5	The terminating gateway sends a 100 (Trying) to the Softswitch.
6	The end office serving TDM Party B initiates ringing of the end instrument and sends an ACM to the terminating gateway.
7, 8	The terminating gateway creates a 180 (Ringing) and sends the 180 (Ringing) to the Softswitch. The Softswitch forwards the 180 (Ringing) to the LSC serving IP Party A. NOTE: Signaling between the LSC serving IP Party A and the end instrument serving IP Party A is not depicted.
9, 10	The LSC serving IP Party A sends a PRACK to the Softswitch and it sends the PRACK to the terminating gateway. NOTE: Signaling between the end instrument serving IP Party A and the LSC serving IP Party A is not depicted.
11, 12	The terminating gateway sends a 200 (OK) PRACK to the Softswitch. The Softswitch sends the 200 (OK) PRACK to the LSC serving IP Party A.
13	When TDM Party B goes off hook (i.e., answers the call), the end office serving TDM Party B sends an ANM to the terminating gateway.
14, 15	The terminating gateway creates a 200 (OK) and sends the 200 (OK) to the Softswitch. The Softswitch forwards the 200 (OK) to the LSC serving IP Party A. NOTE: Signaling between the LSC serving IP Party A and the end instrument serving IP Party A is not depicted.

STEP	INSTRUCTION
16, 17	The LSC serving IP Party A sends an ACK to the Softswitch. The Softswitch forwards the ACK to the terminating gateway. NOTE: Signaling between the end instrument serving IP Party A and the LSC serving IP Party A is not depicted.

Call Release

STEP	INSTRUCTION
18, 19	The LSC serving IP Party A sends a BYE to the Softswitch, which in turn sends the BYE to the terminating gateway. NOTE: Signaling between the end instrument serving IP Party A and the LSC serving IP Party A that initiated the call release is not depicted.
20	The terminating gateway sends an REL to the end office serving TDM Party B.
21	The end office serving TDM Party B sends an RLC to the terminating gateway.
22, 23	The terminating gateway sends a 200 (OK) to the Softswitch and the Softswitch forwards the 200 (OK) to the LSC serving IP Party A. NOTE: Signaling between the LSC serving IP Party A and the end instrument serving IP Party A is not depicted.

5.3.4.19.2.4.2 Figure 5.3.4-42 depicts the sequence of AS-SIP and ISUP messages between the LSC serving IP Party A and the end office serving TDM Party B employed to establish a telephony session using a segmented precondition.

Call Establishment

STEP	INSTRUCTION
1, 2	Upon receiving an initial call request message from IP Party A (not depicted in call flow diagram), the LSC serving IP Party A satisfies its local precondition before sending an INVITE to its assigned Softswitch. The INVITE contains a segmented precondition offer using SDP attributes described in RFC 3312. The precondition offer includes, at a minimum, a media (“m=”) line, a connection (“c=”) line, at least 2 current-status lines (local and remote), and at least 2 desired-status lines (local and remote). The Softswitch forwards the INVITE to the terminating gateway.
3	The Softswitch sends a 100 Trying to the LSC serving IP Party A.

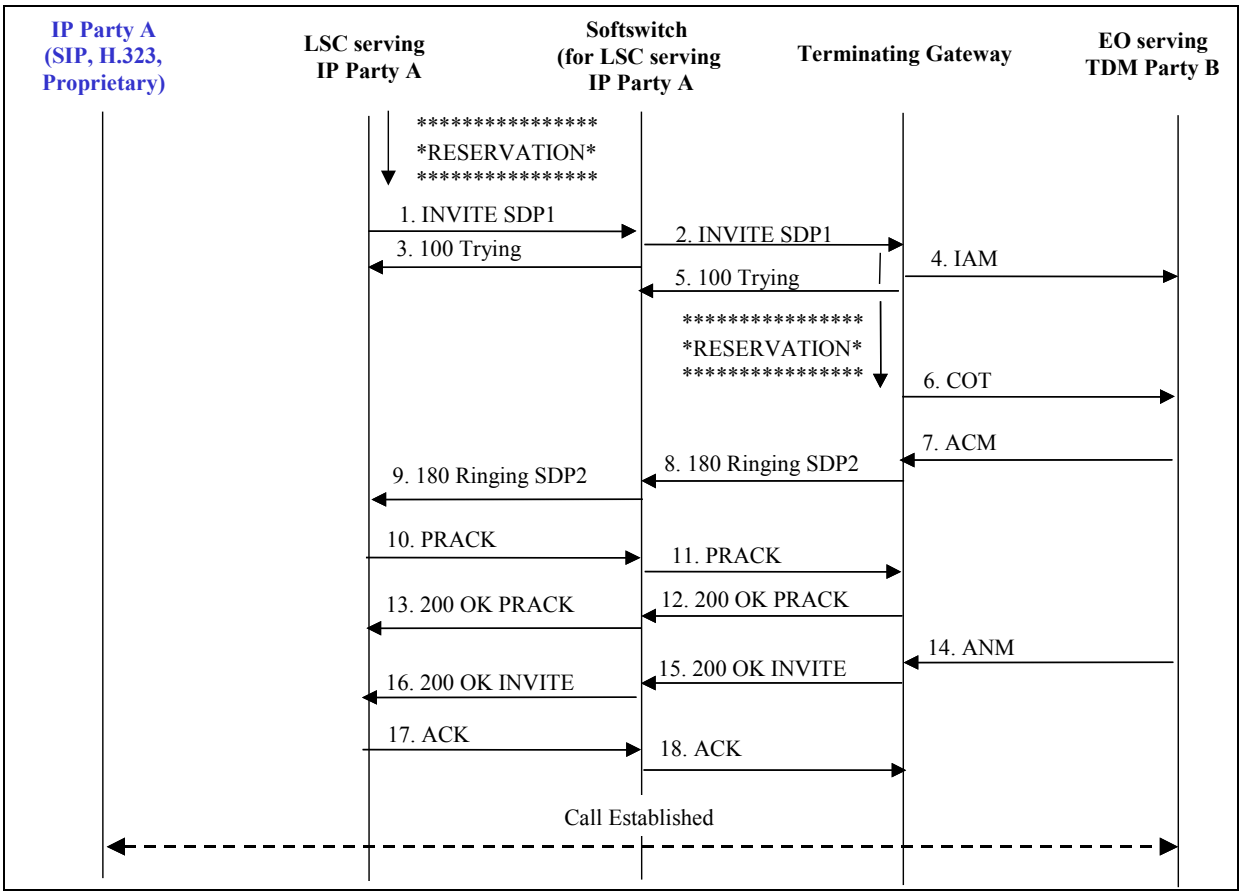


Figure 5.3.4-42. Successful Basic IP-to-TDM Call (Segmented Precondition)

STEP	INSTRUCTION
4	The terminating gateway receives the INVITE creates an IAM, sets the Continuity check indicator of the Nature of Connection Indicators to "Continuity check performed on a previous circuit" or " Continuity check required on this circuit", and sends the IAM to the end office serving TDM Party B. The terminating gateway also goes about satisfying its local preconditions. NOTE: If the Terminating Gateway does not make use of the COT message then the Terminating Gateway can refrain from initiating any CCS7 messaging until after the resources have been reserved.
5	The terminating gateway sends a 100 (Trying) to the Softswitch.
6	Once the SIP preconditions have all been met the terminating gateway sends a COT message to the end office serving TDM Party B so that the end office can send a ring tone to TDM Party B.

STEP	INSTRUCTION
	NOTE: If the Terminating Gateway did not send an IAM in step 3 then the Terminating Gateway sends an IAM with the continuity check indicator of the Nature of Connection Indicators set to '00' "continuity check not required".
7	The end office sends an ACM to the terminating gateway.
8, 9	When the terminating gateway receives an ACM from the end office serving TDM Party B, it creates a 180 (Ringing) with an answer to the segmented precondition offer that includes, at a minimum, a media ("m=") line, a connection ("c=") line, at least 2 current-status-lines, and at least 2 desired-status lines. The terminating gateway sends the 180 (Ringing) to the Softswitch, which forwards the 180 (Ringing) to the LSC serving IP Party A.
10, 11	The LSC serving IP Party A sends a PRACK to the Softswitch, which forwards the PRACK to the terminating gateway. NOTE: Signaling between the LSC serving IP Party A and the end instrument serving IP Party A is not depicted.
12, 13	The terminating gateway sends a 200 (OK) PRACK to the Softswitch, which forwards the 200 (OK) PRACK to the LSC serving IP Party A.
14	When TDM Party B goes off hook (i.e., answers the call) the end office serving TDM Party B sends an ANM to the terminating gateway.
15, 16	The terminating gateway creates a 200 (OK) INVITE response and sends the 200 (OK) INVITE response to the Softswitch, which forwards the 200 (OK) to the LSC serving IP Party A. NOTE: Signaling between the end instrument serving IP Party A and the LSC serving IP Party A is not depicted.
17, 18	The LSC serving IP Party A sends an ACK to the Softswitch, which forwards the ACK to the terminating gateway.

The call is now established.

5.3.4.19.2.4.3 Figure 5.3.4-43 depicts the sequence of AS-SIP and ISUP messages between the LSC serving IP Party A and the end office serving TDM Party B to establish a telephony session employing a status-type end-to-end precondition.

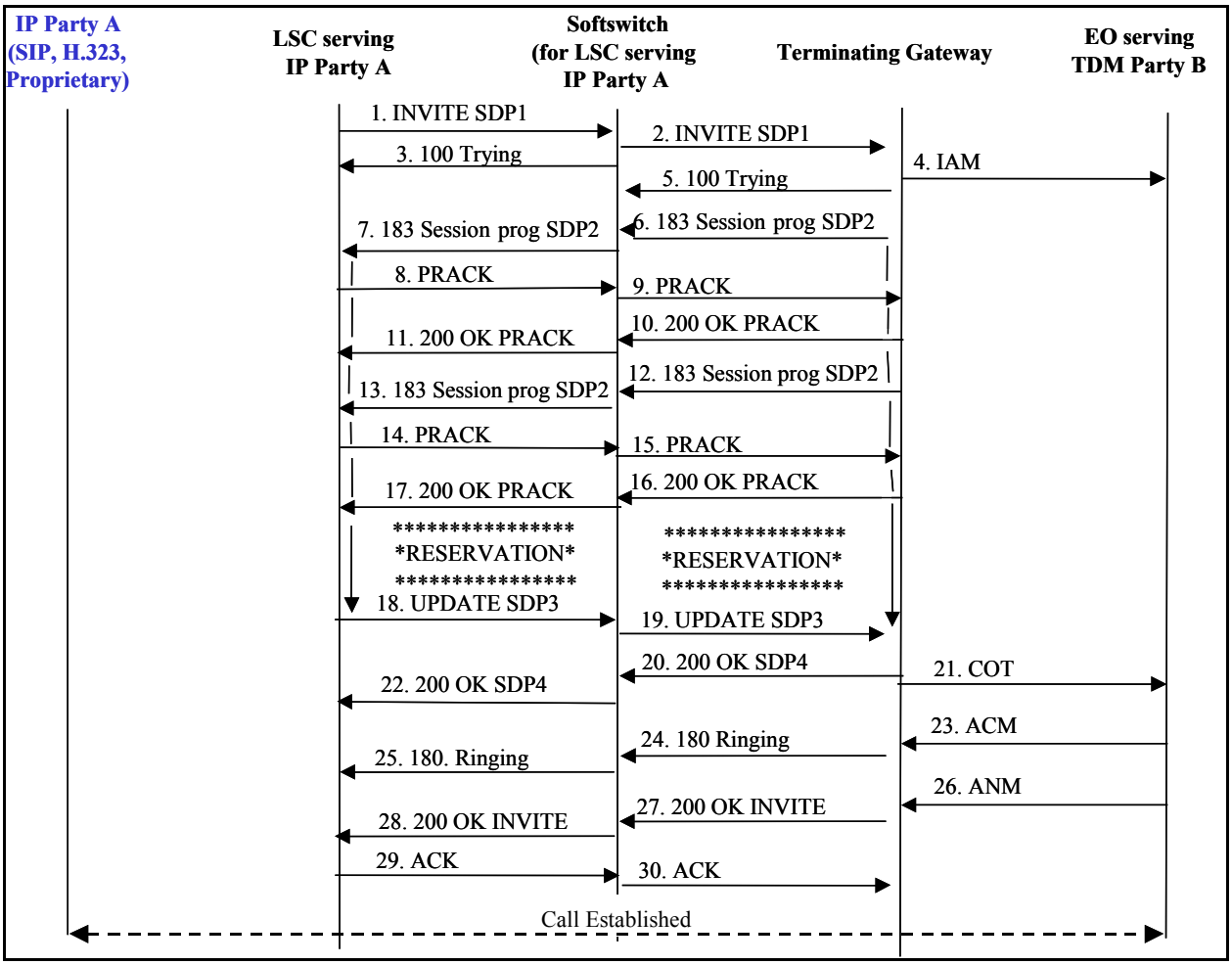


Figure 5.3.4-43. Successful Basic IP-to-TDM Call (End-to-End Precondition)

Call Establishment

STEP	INSTRUCTION
1, 2	Upon receiving an initial call request message from IP Party A (not depicted in call flow diagram), the LSC serving IP Party A sends an INVITE to its assigned Softswitch. The INVITE contains an end-to-end (e2e) precondition offer using SDP attributes described in RFC 3312. The precondition offer includes, at a minimum, a media ("m=") line, a connection ("c=") line, at least one (1) current-status line, and at least one (1) desired-status line. The Softswitch forwards the INVITE to the terminating gateway.
3	The Softswitch sends a 100 Trying to the LSC serving IP Party A.

STEP	INSTRUCTION
4	The terminating gateway receives the INVITE creates an IAM, sets the Continuity check indicator of the Nature of Connection Indicators to "Continuity check performed on a previous circuit" or "Continuity check required on this circuit", and sends the IAM to the end office serving TDM Party B. NOTE: If the Terminating Gateway does not make use of the COT message then the Terminating Gateway can refrain from initiating any CCS7 messaging until after it receives confirmation that the resources have been reserved and sends its acknowledgement in step 14.
5	The terminating gateway sends a 100 (Trying) to the Softswitch.
6, 7	The terminating gateway sends a 183 Session Progress to the Softswitch with an answer to the e2e precondition offer that includes, at a minimum, a media ("m=") line, a connection ("c=") line, at least one (1) current-status line, at least one (1) desired-status line, and at least 1 confirm-status line. The Softswitch sends the 183 session progress to the LSC serving IP Party A. The terminating gateway and the LSC serving IP Party A attempt to reserve the resources needed to fulfill the preconditions.
8, 9	The LSC serving IP Party A sends a PRACK to the Softswitch, which forwards the PRACK to the terminating gateway.
10, 11	The terminating gateway sends a 200 (OK) PRACK response to the Softswitch, which forwards the 200 (OK) PRACK to the LSC serving IP Party A.
12, 13	The terminating gateway sends a 183 Session Progress with sdp (wherein the contents of the sdp body is an exact duplicate of the contents of sdp2 sent in step 6) to the LSC serving IP party A immediately after sending the 200 OK PRACK in order to notify the LSC serving IP party A that early media will be sent to EI A over the backward bearer path.
14, 15	The LSC serving IP Party A sends a PRACK to the Softswitch, which forwards the PRACK to the terminating gateway.
16, 17	The terminating gateway sends a 200 (OK) PRACK response to the Softswitch, which forwards the 200 (OK) PRACK to the LSC serving IP Party A.
18, 19	When the LSC serving IP Party A receives confirmation that it has met its precondition (e.g., receives RSVP RESV message) then the LSC serving IP Party A sends an UPDATE to the Softswitch with an updated offer reflecting compliance with its part of the precondition. The updated precondition offer includes, at a minimum, a media line, a connection data line, at least one (1) current-status line, and at least one (1) desired-status line. The Softswitch forwards the UPDATE to the terminating gateway.

STEP	INSTRUCTION
20	The terminating gateway receives confirmation that it has met its precondition (e.g., receives RSVP RESV message) and sends a 200 (OK) UPDATE to the Softswitch with an updated precondition answer reflecting compliance with its part of the precondition as well as the most recent updated information from the UPDATE offer. The updated answer includes, at a minimum, a media line, a connection data line, at least one (1) current-status line, at least one (1) desired-status line.
21	Now that the SIP preconditions have all been met, the terminating gateway sends a COT message to the end office serving TDM Party B so that the end office can send a ring tone to TDM Party B. NOTE: If the Terminating Gateway did not send an IAM in step 3, then the Terminating Gateway sends an IAM with the continuity check indicator of the Nature of Connection Indicators set to '00' "continuity check not required".
22	The Softswitch forwards the 200 (OK) UPDATE to the LSC serving IP Party A.
23	The end office serving TDM Party B sends an ACM to the terminating gateway.
24, 25	The terminating gateway creates a 180 (Ringing) response and sends the 180 (Ringing) response to the Softswitch, which forwards the 180 (Ringing) response to the LSC serving IP Party A. NOTE: Signaling between the LSC serving IP Party A and the end instrument serving IP Party A is not depicted.
26	When TDM Party B goes off hook (i.e., answers the call), the end office serving TDM Party B sends an ANM to the terminating gateway.
27, 28	The terminating gateway creates a 200 (OK) INVITE response and sends the 200 (OK) INVITE response to the Softswitch, which forwards the 200 (OK) INVITE response to the LSC serving IP Party A. NOTE: Signaling between the LSC serving IP Party A and the end instrument serving IP Party A is not depicted.
29, 30	The LSC serving IP Party A sends an ACK to the Softswitch, which forwards the ACK to the terminating gateway. NOTE: Signaling between the end instrument serving IP Party A and the LSC serving IP Party A that initiated the call release is not depicted.

The call is now established.

5.3.4.19.3 Call Hold

Party A and Party B are engaged in a conversation. Party A places the call on hold. Later, Party A resumes the call (removes the call from hold).

5.3.4.19.3.1 IP-to-IP Call Type

See UCR 2008, Section 5.3.4.13.3.1, IP-to-IP Call Type.

5.3.4.19.3.2 TDM Bridging Call Type

5.3.4.19.3.2.1 In the DSN TDM network today when a party engaged in an ongoing call places the call on hold or resumes the call after placing the call on hold the only signaling exchanged in support of the call hold or call resume is between the end instrument and its local switch. The local switch does not transmit signaling into the network to indicate to the remote switch serving the other party to the call that a call hold or a call resume has been initiated. Figure 5.3.4-44 reflects this by indicating the user signaling to the local TDM switch but no signaling thereafter across the TDM network to the remote TDM switch. When the call has been placed on hold the local TDM switch does not forward outbound bearer traffic received from the end instrument to the next TDM switch and does not forward inbound bearer traffic received from the network to the end instrument. When the call is resumed, the local TDM switch again forwards outbound bearer traffic received from the end instrument to the next TDM switch and forwards inbound bearer traffic received from the network to the end instrument.

5.3.4.19.3.3 TDM-to-IP Call Type

5.3.4.19.3.3.1 In the DSN TDM network today when a party engaged in an ongoing call places the call on hold or resumes the call after placing the call on hold the only signaling exchanged in support of the call hold or call resume is between the end instrument and its local switch. The local switch does not transmit signaling into the network to indicate to the remote switch serving the other party to the call that a call hold or a call resume has been initiated. Figure 5.3.4-45 reflects this by indicating the user signaling to the EO serving TDM Party A but indicating no ISUP signaling from the EO to the originating gateway. When the call has been placed on hold the local TDM switch does not forward outbound bearer traffic received from the end instrument to the next TDM switch and does not forward inbound bearer traffic received from the network to the end instrument. When the call is resumed, the local TDM switch again forwards outbound bearer traffic received from the end instrument to the next TDM switch and forwards inbound bearer traffic received from the network to the end instrument.

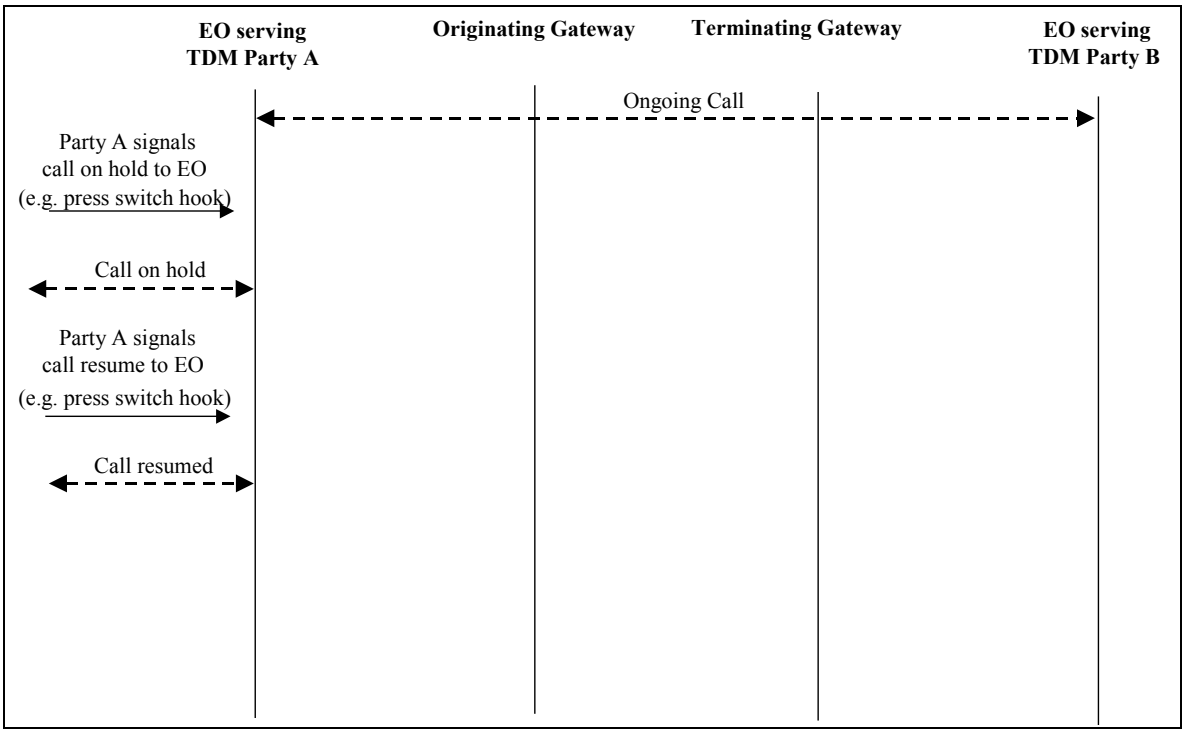


Figure 5.3.4-44. TDM Bridging Call Hold

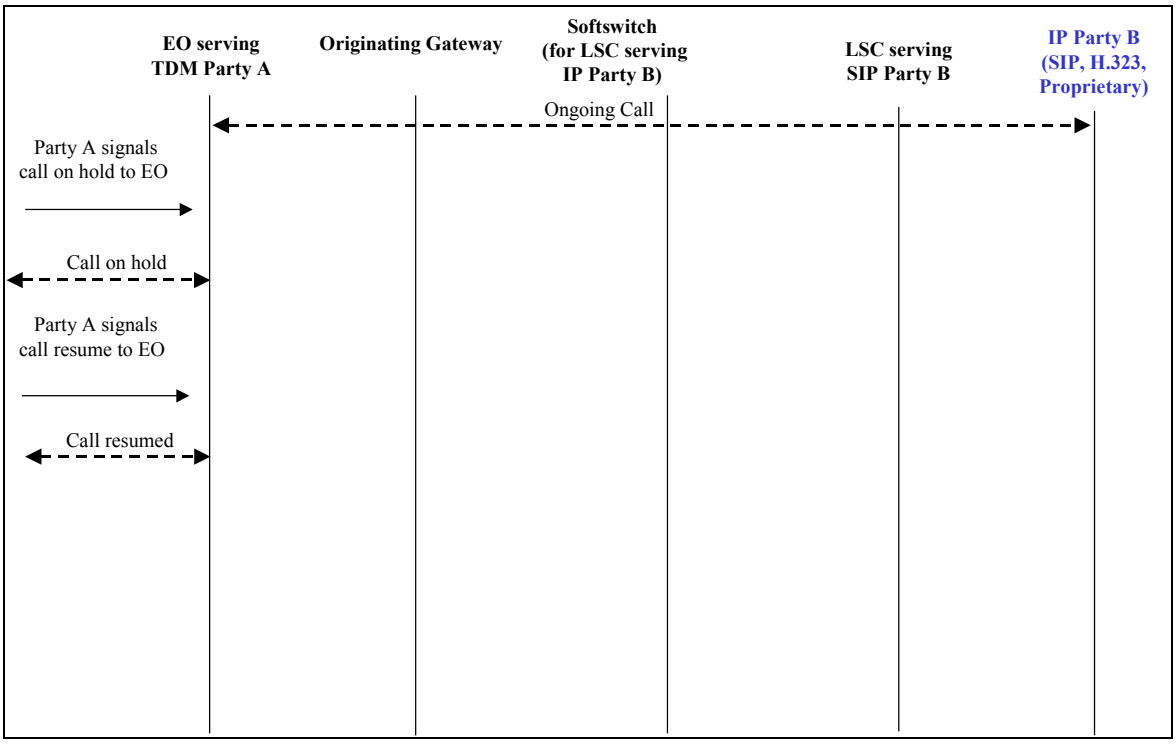


Figure 5.3.4-45. TDM-to-IP Call Hold; TDM Party Places Call On Hold

5.3.4.19.3.3.2 Figure 5.3.4-46 depicts the sequence of AS-SIP messages between the originating gateway and the LSC serving IP Party B that are employed when IP Party B places the current call on hold and then resumes the call.

Figure 5.3.4-47 at the end of this subsection offers an illustrative example of the call signaling with a standard SIP end instrument.

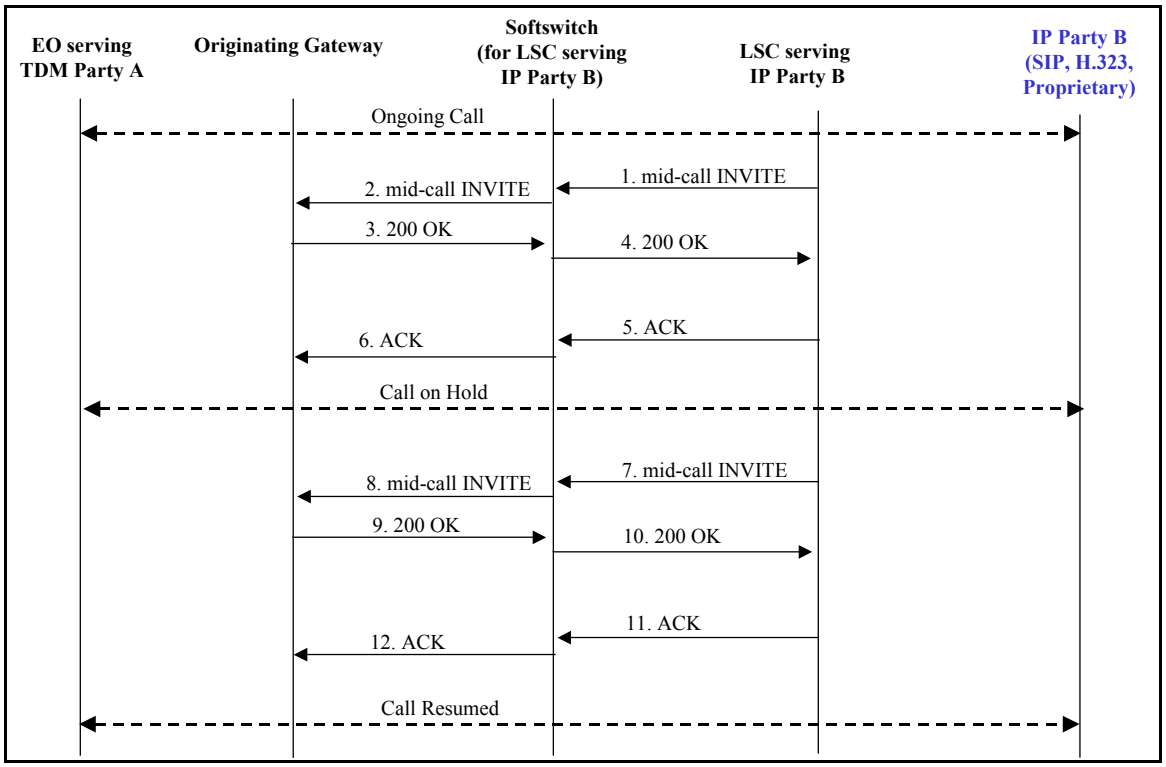


Figure 5.3.4-46. TDM-to-IP Call Hold; IP Party Places Call On Hold

Call Hold

STEP	INSTRUCTION
1, 2	In response to a request on the part of IP Party B, the LSC serving IP Party B sends a mid-call INVITE to the Softswitch assigned to the LSC serving IP Party B. The Softswitch forwards the mid-call INVITE to the originating gateway. The INVITE includes the attribute line “a=sendonly” or “a=inactive” if the stream had been a sendrecv media stream or “a=inactive” if the stream had been a recvonly stream. NOTE: The SIP UA MAY also support establishing a call hold by sending a mid-call INVITE that includes a session description that is the same as in the original request, but the "c" destination addresses for the media streams to be put on hold are set to zero. c=IN IP4 0.0.0.0

STEP	INSTRUCTION
	NOTE: Signaling between the end instrument serving IP Party B and the LSC serving IP Party B is not depicted. The originating gateway does not translate the re-INVITE into TDM signaling for forwarding onto the TDM network however the originating gateway instructs its media gateway component not to forward bearer traffic for the given call that is received on the TDM channel to the IP network and not to forward rtp packets for the given call that are received from the IP network to the TDM bearer channel.
3, 4	The originating gateway sends a 200 (OK) INVITE to the Softswitch, which forwards the 200 (OK) INVITE to the LSC serving IP Party B. NOTE: Signaling between the LSC serving IP Party B and the end instrument serving IP Party B is not depicted
5, 6	The LSC serving IP Party B sends an ACK to the Softswitch, which forwards the ACK to the originating gateway. NOTE: Signaling between the end instrument serving IP Party B and the LSC serving IP Party B is not depicted.

The call is now on hold.

Call Resumed

STEP	INSTRUCTION
7, 8	In response to a request on the part of IP Party B, the LSC serving Party B sends a mid-call INVITE to the Softswitch, which forwards it to the originating gateway. The re-INVITE includes the attribute line "a=sendrecv" if the stream had originally been a sendrecv media stream or "a=recvonly" if the stream had been a recvonly stream. NOTE: In the case of a call hold established by setting the "c" destination address to 0.0.0.0, another re-INVITE with the original address parameter terminates the call hold. NOTE: Signaling between the end instrument serving IP Party B and the LSC serving IP Party B is not depicted. The originating gateway does not translate the re-INVITE into TDM signaling for forwarding onto the TDM network however the originating gateway instructs its media gateway component to again forward bearer traffic for the given call that is received on the TDM channel to the IP network and to forward rtp packets for the given call that are received from the IP network to the TDM bearer channel.
9, 10	The originating gateway sends a 200 (OK) to the Softswitch, which forwards the 200 (OK) to the LSC serving IP Party B.

STEP	INSTRUCTION
	NOTE: Signaling between the LSC serving IP Party B and the end instrument serving IP Party B is not depicted.
11, 12	The LSC serving IP Party B sends an ACK to the Softswitch, which forwards the ACK to the originating gateway. NOTE: Signaling between the end instrument serving IP Party B and the LSC serving IP Party B is not depicted.

The call is now resumed.

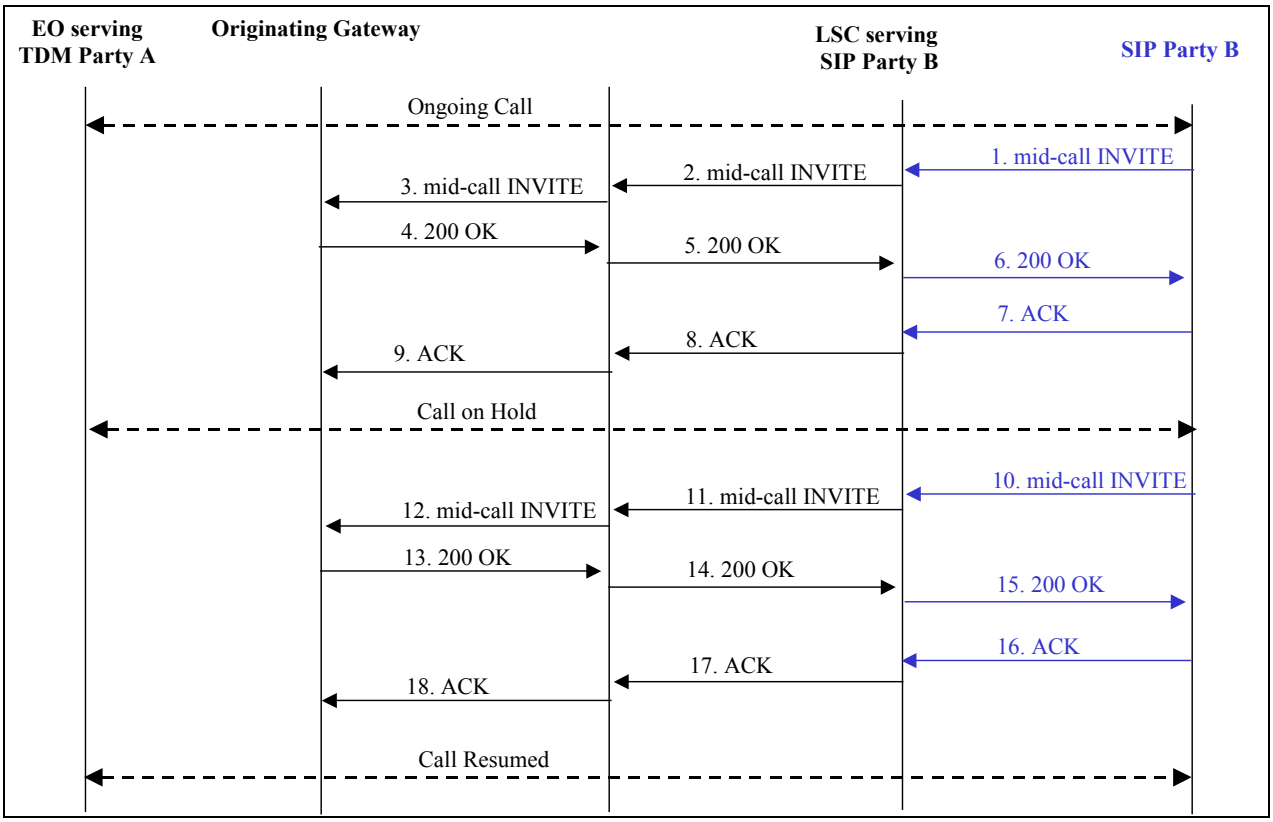


Figure 5.3.4-47. TDM-SIP Call Hold; IP Party Places Call On Hold (SIP Signaling to a SIP End Instrument is Added for Illustrative Purposes)

5.3.4.19.3.4 IP-to-TDM Call Type

5.3.4.19.3.4.1 Figure 5.3.4-48 depicts the sequence of AS-SIP and ISUP messages between the LSC serving IP Party A and the terminating gateway that are employed when IP Party A places the current call on hold and then resumes the call.

Figure 5.3.4-49 at the end of this subsection offers an illustrative example of the call signaling to a standard SIP end instrument.

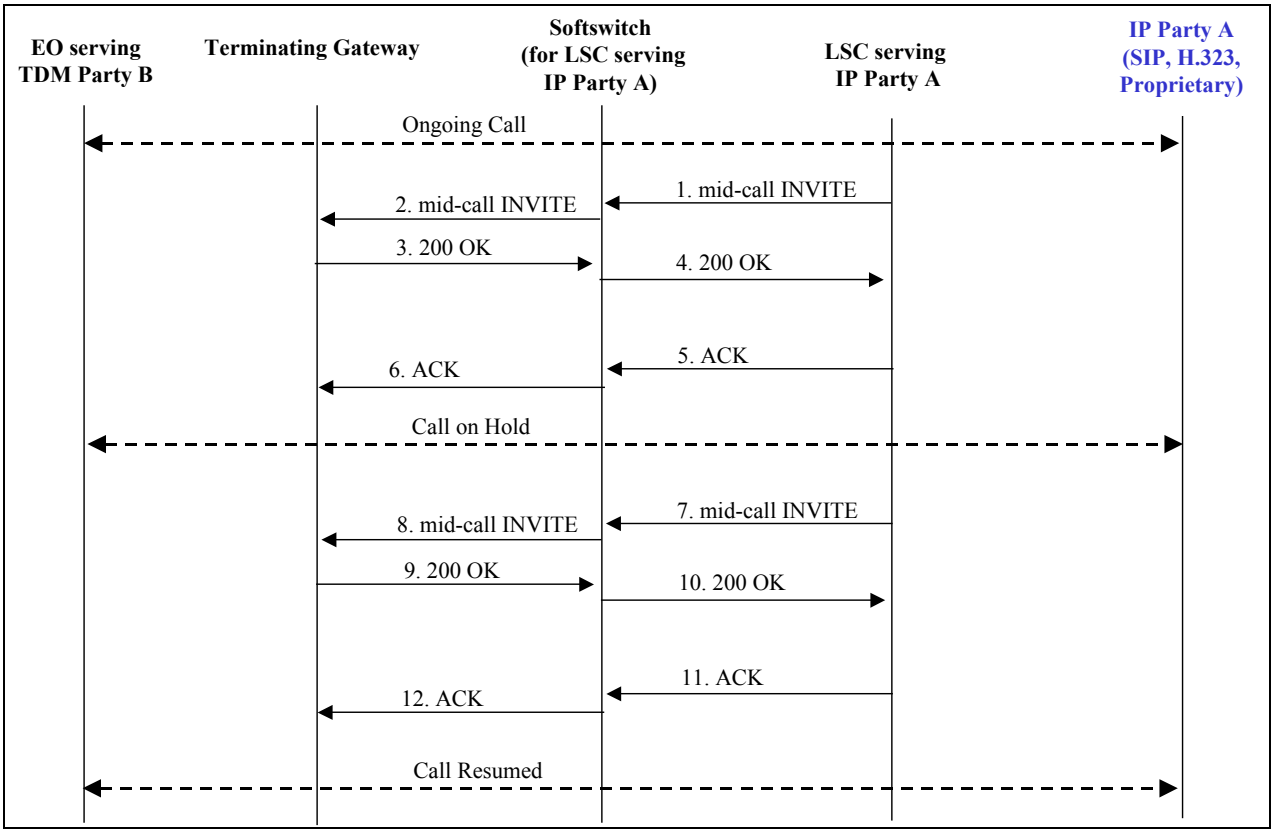


Figure 5.3.4-48. IP-to-TDM Call Hold; IP Party Places Call On Hold

Call Hold

STEP	INSTRUCTION
1, 2	In response to a request on the part of IP Party A, the LSC serving IP Party A sends a mid-call INVITE to the Softswitch assigned to the LSC serving IP Party A. The INVITE includes the attribute line “a=sendonly” or “a=inactive” if the stream had been a sendrecv media stream or “a=inactive” if the stream had been a recvonly stream. The Softswitch forwards the mid-call INVITE to the terminating gateway. NOTE: The SIP UA MAY also support establishing a call hold by sending a mid-call INVITE that includes a session description that is the same as in the original request, but the "c" destination addresses for the media streams to be put on hold are set to zero: c=IN IP4 0.0.0.0. NOTE: Signaling between the end instrument serving IP Party A and the LSC serving IP Party A is not depicted.

STEP	INSTRUCTION
	The terminating gateway does not translate the re-INVITE into TDM signaling for forwarding onto the TDM network however the terminating gateway instructs its media gateway component not to forward bearer traffic for the given call that is received on the TDM channel to the IP network and not to forward rtp packets for the given call that are received from the IP network to the TDM bearer channel.
3, 4	The terminating gateway sends a 200 (OK) response to the Softswitch, which forwards the 200 (OK) response to the LSC serving IP Party A. NOTE: Signaling between the LSC serving IP Party A and the end instrument serving IP Party A is not depicted.
5, 6	The LSC serving IP Party A sends an ACK to the Softswitch and the Softswitch forwards the ACK to the terminating gateway.

The call is now on hold.

Call Resumed

STEP	INSTRUCTION
7, 8	In response to a request on the part of IP Party A, the LSC serving IP Party A sends a mid-call INVITE to the Softswitch, which forwards it to the terminating gateway. The re-INVITE includes the attribute line "a=sendrecv" if the stream had originally been a sendrecv media stream or "a=recvonly" if the stream had been a recvonly stream. NOTE: In the case of a call hold established by setting the "c" destination address to 0.0.0.0, another re-INVITE with the original address parameter terminates the call hold. NOTE: Signaling between the end instrument serving IP Party A and the LSC serving IP Party A is not depicted. The terminating gateway does not translate the re-INVITE into TDM signaling for forwarding onto the TDM network however the terminating gateway instructs its media gateway component to again forward bearer traffic for the given call that is received on the TDM channel to the IP network and to forward rtp packets for the given call that are received from the IP network to the TDM bearer channel.
9, 10	The terminating gateway sends a 200 (OK) to the Softswitch, which forwards the 200 (OK) to the LSC serving IP Party A. NOTE: Signaling between the LSC serving IP Party A and the end instrument serving IP Party A is not depicted.

STEP	INSTRUCTION
11, 12	The LSC serving IP Party A sends an ACK to the Softswitch, which forwards the ACK to the terminating gateway. NOTE: Signaling between the end instrument serving IP Party A and the LSC serving IP Party A is not depicted.

The call is now resumed.

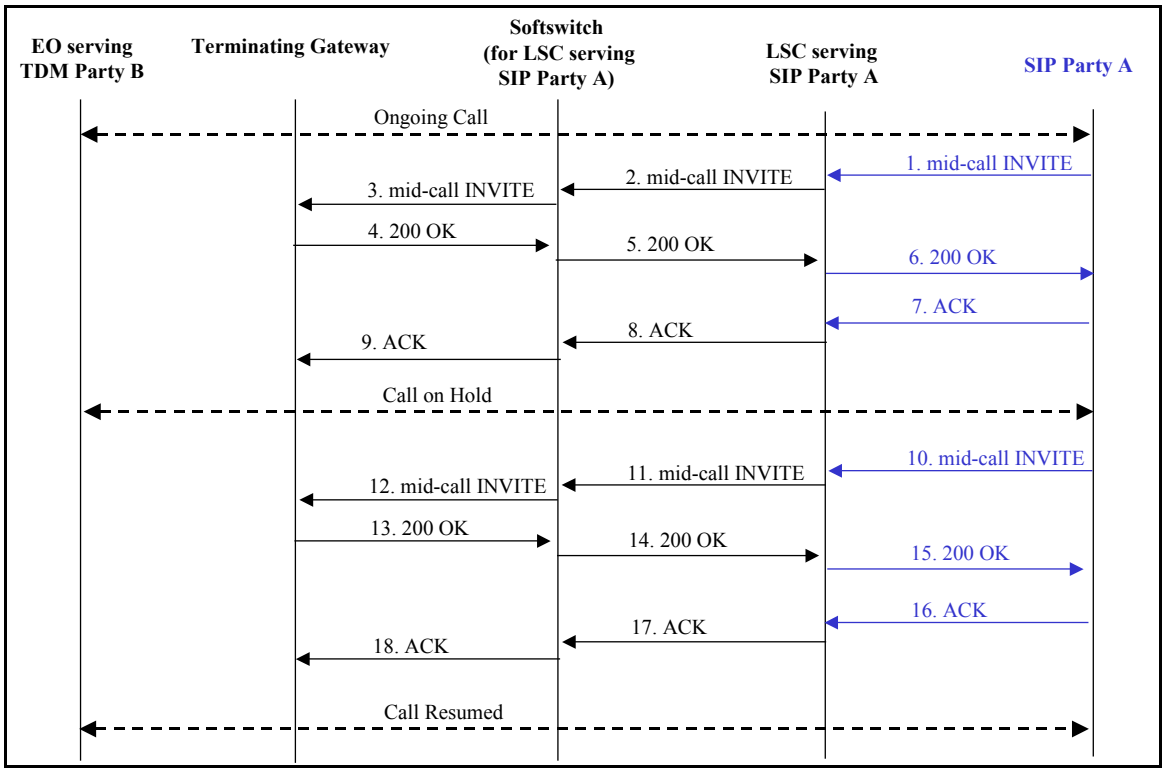


Figure 5.3.4-49. SIP-TDM Call Hold; SIP Party Places Call On Hold (SIP Signaling to a SIP End Instrument is Added for Illustrative Purposes)

5.3.4.19.3.4.2 Figure 5.3.4-50 is intended to depict a call hold performed by the TDM party in an IP-TDM call. As we have seen previously a call hold or call resume conducted by an EI on the TDM network does not result in signaling outside the local TDM switch. Figure 5.3.4-50 reflects this by indicating the user signaling to the EO serving TDM Party A but indicating no ISUP signaling from the EO to the originating gateway.

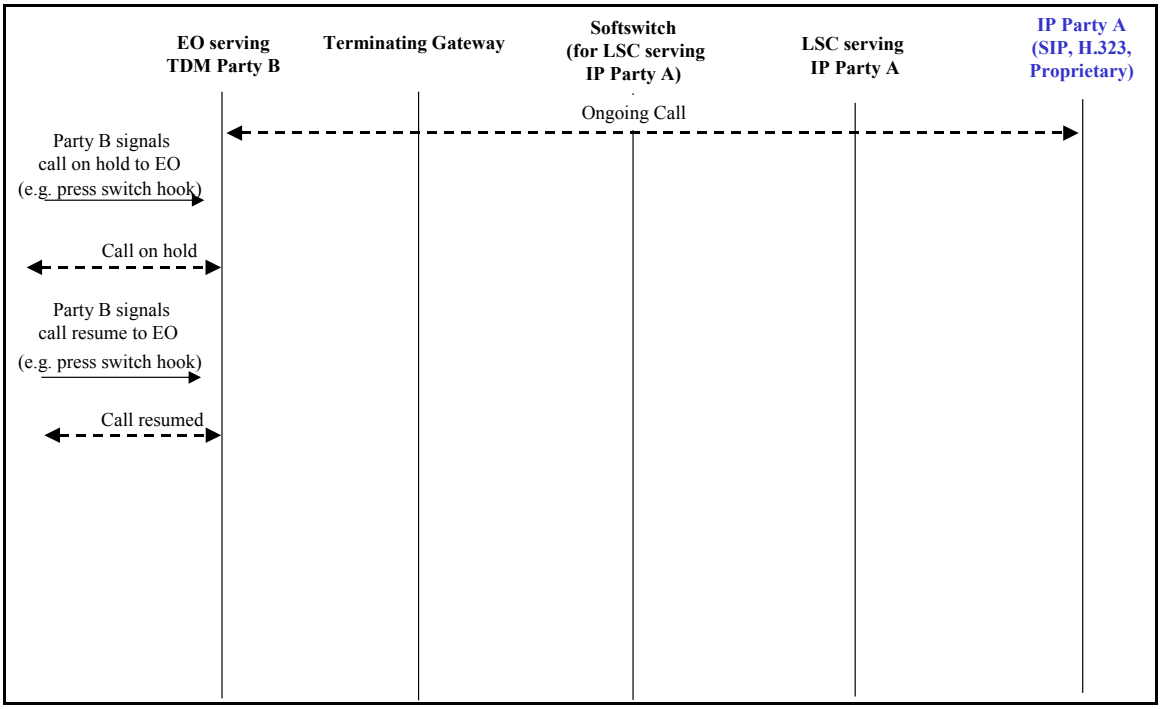


Figure 5.3.4-50. IP-to-TDM Call Hold; TDM Party Places Call On Hold

5.3.4.19.4 Call Waiting

Party A and Party B are engaged in a conversation. Call waiting consists of one party placing the other party on hold while either accepting or resuming a call with a third party.

5.3.4.19.4.1 IP-to-IP Call Type

See UCR 2008, Section 5.3.4.13.4.1, IP-to-IP Call Type.

5.3.4.19.4.2 TDM Bridging Call Type

5.3.4.19.4.2.1 Figure 5.3.4-51 depicts call waiting in which there is an existing session between TDM Party A and TDM Party B and IP Party C initiates a call request to TDM Party B. Upon receiving the call waiting tone triggered by the call request from IP Party C, TDM Party B conducts a call hold on the existing session with TDM Party A and completes the call establishment with IP Party C. When TDM Party B is ready to return to the original call with TDM Party A, then TDM Party B resumes the call with TDM Party B and IP Party C hangs up terminating the call with TDM Party B. Note: When TDM Party B signals its EO to place the call with TDM Party A on hold, the EO does not transmit signaling into the TDM network to indicate the call hold. Similarly, When TDM Party B signals its EO to resume the call with

TDM Party A the EO does not transmit signaling into the TDM network to indicate the call resume.

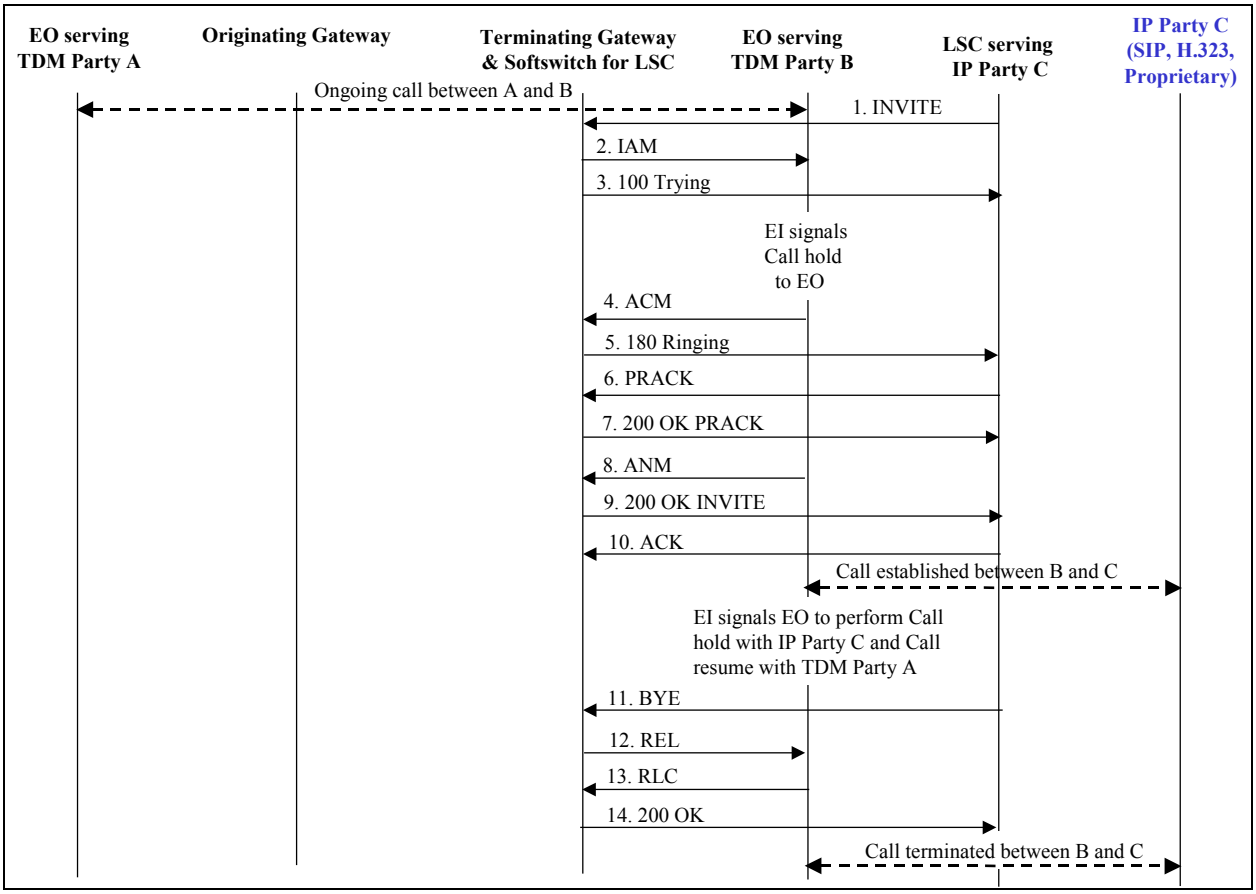


Figure 5.3.4-51. TDM Bridging Call Waiting

When the call is placed on hold the local TDM switch serving TDM Party B does not forward outbound bearer traffic received from TDM Party B destined for TDM Party A and does not forward inbound bearer traffic received from remote TDM Party A to TDM Party B. When the call is resumed, the EO once again forwards bearer traffic received from TDM Party A to TDM Party B and bearer traffic received from TDM Party B to TDM Party A and no longer forwards bearer traffic between TDM Party B and IP Party C.

NOTE: A valid alternative scenario for resuming the call with TDM Party A would have IP Party C terminate its call with TDM Party B whereupon TDM Party B resumes its call with TDM Party A.

Due to real estate constraints the Softswitch assigned to the LSC serving IP Party C is also the terminating gateway for the call between TDM Party A and TDM Party B.

Figure 5.3.4-52 at the end of this subsection offers an illustrative example of the call signaling when IP Party C is a standard SIP end instrument.

STEP	INSTRUCTION
1	Upon receiving an initial call request message from IP Party C (not depicted in call flow diagram), the LSC serving IP Party C sends an INVITE to its Softswitch which in this example also happens to be the terminating gateway for the end office serving TDM Party B. NOTE: Signaling between the end instrument serving IP Party C and the LSC serving IP Party C is not depicted.
2	The terminating gateway receives the INVITE and sends an IAM to the end office serving TDM Party B.
3	The terminating gateway sends a 100 (Trying) to the LSC serving IP Party C.
Call Hold	TDM Party B receives the call waiting tone and signals call hold to its local end office. The local EO ceases forwarding any bearer traffic between TDM Party B and TDM Party A. The original call between TDM Party A and TDM Party B is now on hold.

The original call between TDM Party A and TDM Party B is now on hold.

STEP	INSTRUCTION
4	The end office serving TDM Party B sends an ACM to the terminating gateway.
5	The terminating gateway translates the ACM to a 180 (Ringing) and sends the 180 (Ringing) to the LSC serving IP Party C. NOTE: Signaling between the LSC serving IP Party C and the end instrument serving IP Party C is not depicted.
6	The LSC serving IP Party C sends a PRACK to the terminating gateway.
7	The terminating gateway sends a 200 OK PRACK to the LSC serving IP Party C.
8	The end office serving TDM Party B sends an ANM to the terminating gateway.
9	The terminating gateway receives the ANM and sends a 200 (OK) to the LSC serving IP Party C. NOTE: Signaling between the LSC serving IP Party C and the end instrument serving IP Party C is not depicted.

STEP	INSTRUCTION
10	The LSC serving IP Party C sends an ACK to the terminating gateway. NOTE: Signaling between the end instrument serving IP Party C and the LSC serving IP Party C is not depicted.

The call between IP Party C and TDM Party B is now established.

STEP	INSTRUCTION
Call Hold C Call Resume A	TDM Party B signals its local EO to hold the call with IP Party C and resume the call with TDM Party A. The local EO disables forwarding of bearer traffic between TDM Party B and IP Party C and reenables forwarding of bearer traffic between TDM Party B and TDM Party A.

The call between TDM Party A and TDM Party B is resumed

STEP	INSTRUCTION
11	The LSC serving IP Party C sends a BYE to the terminating gateway. NOTE: Signaling between the end instrument serving IP Party C and the LSC serving IP Party C is not depicted.
12	When the terminating gateway receives the BYE, the terminating gateway sends a REL to the EO serving TDM Party B.
13	The end office serving TDM Party B sends a RLC to the terminating gateway.
14	The terminating gateway sends a 200 (OK) to the LSC serving IP Party C NOTE: Signaling between the LSC serving IP Party C and the end instrument serving IP Party C is not depicted.

The call between IP Party C and TDM Party B has been terminated.

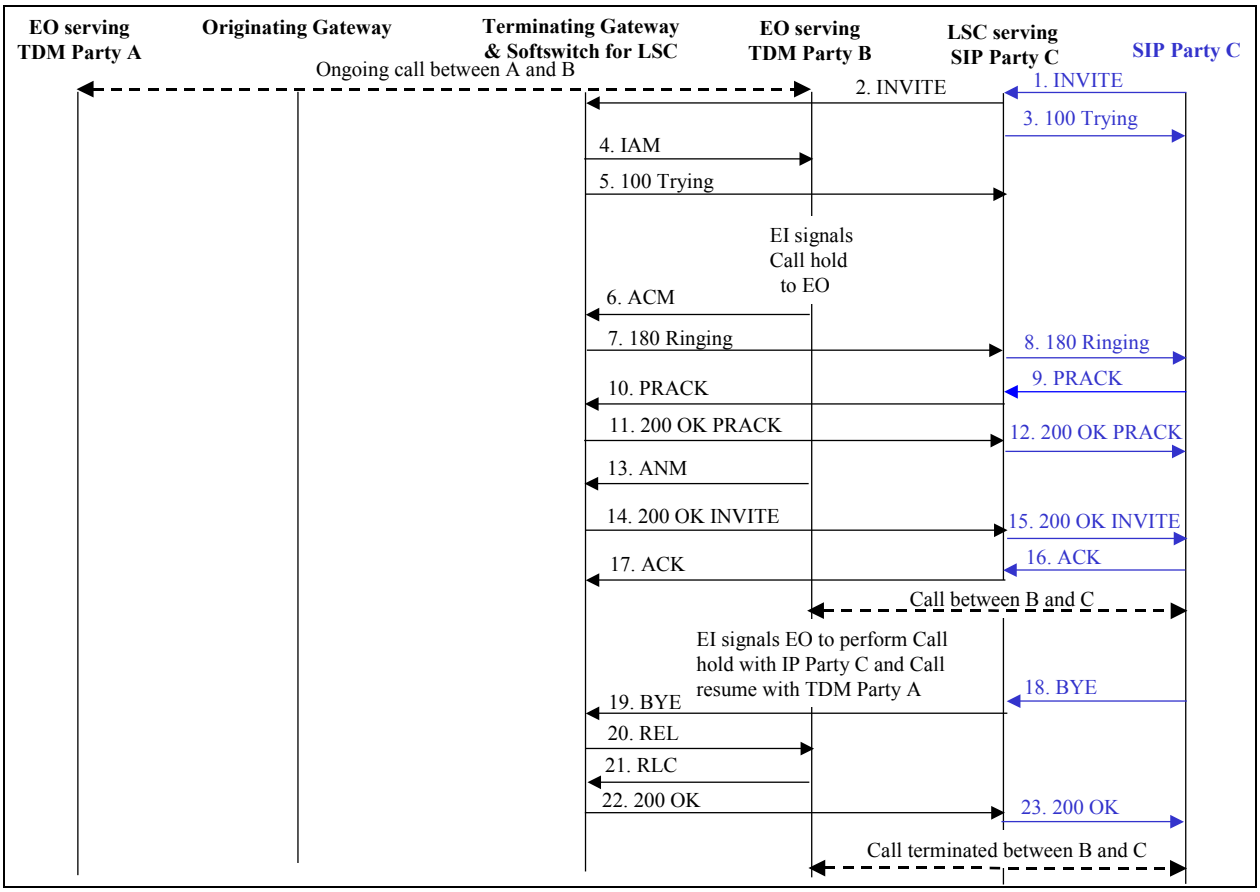


Figure 5.3.4-52. TDM Bridging Call Waiting
(SIP Signaling to a Third Party SIP End Instrument is Depicted for Illustrative Purposes)

5.3.4.19.4.3 TDM-to-IP Call Type

5.3.4.19.4.3.1 Figure 5.3.4-53 depicts the sequence of AS-SIP messages employed to place the current TDM-IP call on hold in order to accept a call from a third party C, and to terminate the call with the third party C in order to resume the original call. (IP party performs the call waiting). NOTE: When the originating gateway receives the SIP message indicating call hold, the originating gateway instucts its media gateway to cease forwarding bearer traffic between TDM Party A and IP Party B and vice versa. However, the originating gateway does not translate the SIP signaling message indicating call hold to ISUP as the DSN TDM network does not signal call hold over the network. Similarly, when the originating gateway receives the SIP message indicating call resume, the originating gateway instucts its media gateway to resume forwarding bearer traffic between TDM Party A and IP Party B and vice versa. However, the originating gateway does not translate the SIP signaling message indicating call resume into an ISUP message.

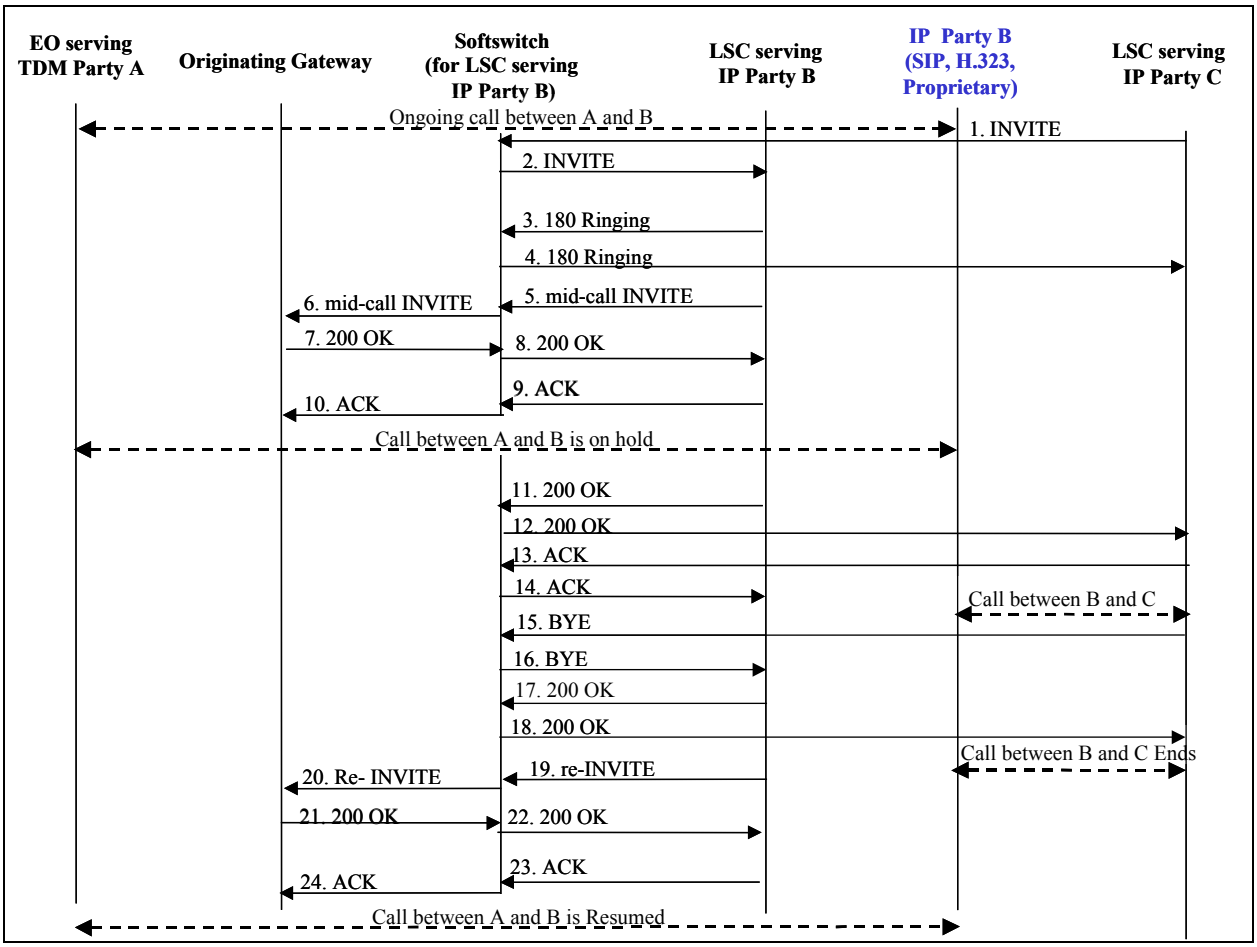


Figure 5.3.4-53. TDM-to-IP Call Waiting (Performed at IP Party B)

In this scenario when IP Party B and IP Party C have completed their call, IP Party C terminates the call with IP Party B and then IP Party B resumes its call with TDM Party A.

NOTE: A valid alternative scenario for resuming the call with TDM Party A would have IP Party B place IP Party C on hold, and resume the call with TDM Party A whereupon IP Party C disconnects the call with IP Party B.

Due to real estate constraints, the same Softswitch is assigned to the LSC serving IP Party B and to the LSC serving IP Party C.

Figure 5.3.4-54 at the end of this subsection offers an illustrative example of the call signaling when IP Party B is a standard SIP end instrument.

STEP	INSTRUCTION
1	Upon receiving an initial call request message from IP Party C (not depicted in call flow diagram), the LSC serving IP Party C sends an INVITE to the Softswitch assigned to the LSC serving IP Party B. NOTE: Signaling between the end instrument serving IP Party C and the LSC serving IP Party C is not depicted.
2	The Softswitch sends the INVITE to the LSC serving IP Party B. NOTE: Signaling between the LSC serving IP Party B and the end instrument serving IP Party B is not depicted.
3, 4	The LSC serving IP Party B sends a 180 (Ringing) to the Softswitch, which forwards the 180 (Ringing) to the LSC serving IP Party C. NOTE: Signaling between the end instrument serving IP Party B and the LSC serving IP Party B is not depicted. NOTE: Signaling between the LSC serving IP Party C and the end instrument serving IP Party C is not depicted.
5, 6	The LSC serving IP Party B sends a mid-call INVITE to the Softswitch, which forwards the mid-call INVITE to the originating gateway. The mid-call INVITE includes the attribute line “a=sendonly” or “a=inactive” if the stream had been a sendrecv media stream or “a=inactive” if the stream had been a recvonly stream. NOTE: The LSC serving IP Party B MUST also support establishing a call hold by sending a mid-call INVITE that includes a session description that is the same as in the original request, but the "c" destination addresses for the media streams to be put on hold are set to zero: c=IN IP4 0.0.0.0. NOTE: Signaling between the end instrument serving IP Party B and the LSC serving IP Party B is not depicted. The originating gateway instructs its media gateway to cease forwarding bearer traffic between IP Party B and TDM Party A and vice versa.
7, 8	The originating gateway sends a 200 (OK) INVITE to the Softswitch, which forwards the 200 (OK) INVITE to the LSC serving IP Party B. NOTE: Signaling between the LSC serving IP Party B and the end instrument serving IP Party B is not depicted.

STEP	INSTRUCTION
9, 10	The LSC serving IP Party B sends an ACK to the Softswitch, which forwards the ACK to the originating gateway. NOTE: Signaling between the end instrument serving IP Party B and the LSC serving IP Party B is not depicted.

The original call between TDM Party A and IP Party B is now on hold.

STEP	INSTRUCTION
11, 12	The LSC serving IP Party B sends a 200 (OK) to the Softswitch, which forwards the 200 (OK) to the LSC serving IP Party C. NOTE: Signaling between the end instrument serving IP Party B and the LSC serving IP Party B is not depicted. NOTE: Signaling between the LSC serving IP Party C and the end instrument serving IP Party C is not depicted.
13, 14	The LSC serving IP Party C sends an ACK to the Softswitch, which forwards the ACK to the LSC serving IP Party B. NOTE: Signaling between the end instrument serving IP Party C and the LSC serving IP Party C is not depicted. NOTE: Signaling between the LSC serving IP Party B and the end instrument serving IP Party B is not depicted.

The call between IP Party C and IP Party B is now established.

STEP	INSTRUCTION
15, 16	When IP Party C terminates the session with IP Party B then the LSC serving IP Party C sends a BYE to the Softswitch, which forwards the BYE to the LSC serving IP Party B. NOTE: Signaling between the end instrument serving IP Party C and the LSC serving IP Party C that initiated the call release is not depicted. NOTE: Signaling between the LSC serving IP Party B and the end instrument serving IP Party B is not depicted.

17, 18	The LSC serving IP Party B sends a 200 (OK) response to the Softswitch, which forwards the 200 (OK) response to the LSC serving IP Party C. NOTE: Signaling between the end instrument serving IP Party B and the LSC serving IP Party B is not depicted. NOTE: Signaling between the LSC serving IP Party C and the end instrument serving IP Party C is not depicted.

The call between IP Party C and IP Party B is now terminated.

STEP	INSTRUCTION
19, 20	The LSC serving IP Party B sends a mid-call re-INVITE to the Softswitch, which forwards the mid-call re-INVITE to the originating gateway. The mid-call re-INVITE includes the attribute line "a=sendrecv" if the stream had originally been a sendrecv media stream or "a=recvonly" if the stream had been a recvonly stream. NOTE: In the case of a call hold established by setting the "c" destination address to 0.0.0.0, another re-INVITE with the original address parameter terminates the call hold. NOTE: Signaling between the end instrument serving IP Party B and the LSC serving IP Party B is not depicted. The originating gateway instructs its media gateway to resume forwarding bearer traffic between IP Party B and TDM Party A and vice versa.
21, 22	The originating gateway sends a 200 (OK) to the Softswitch, which forwards the 200 (OK) to the LSC serving IP Party B. NOTE: Signaling between the LSC serving IP Party B and the end instrument serving IP Party B is not depicted.
23, 24	The LSC serving IP Party B sends an ACK to the Softswitch, which forwards the ACK to the originating gateway. NOTE: Signaling between the end instrument serving IP Party B and the LSC serving IP Party B is not depicted.

The original call between TDM Party A and IP Party B is now resumed.

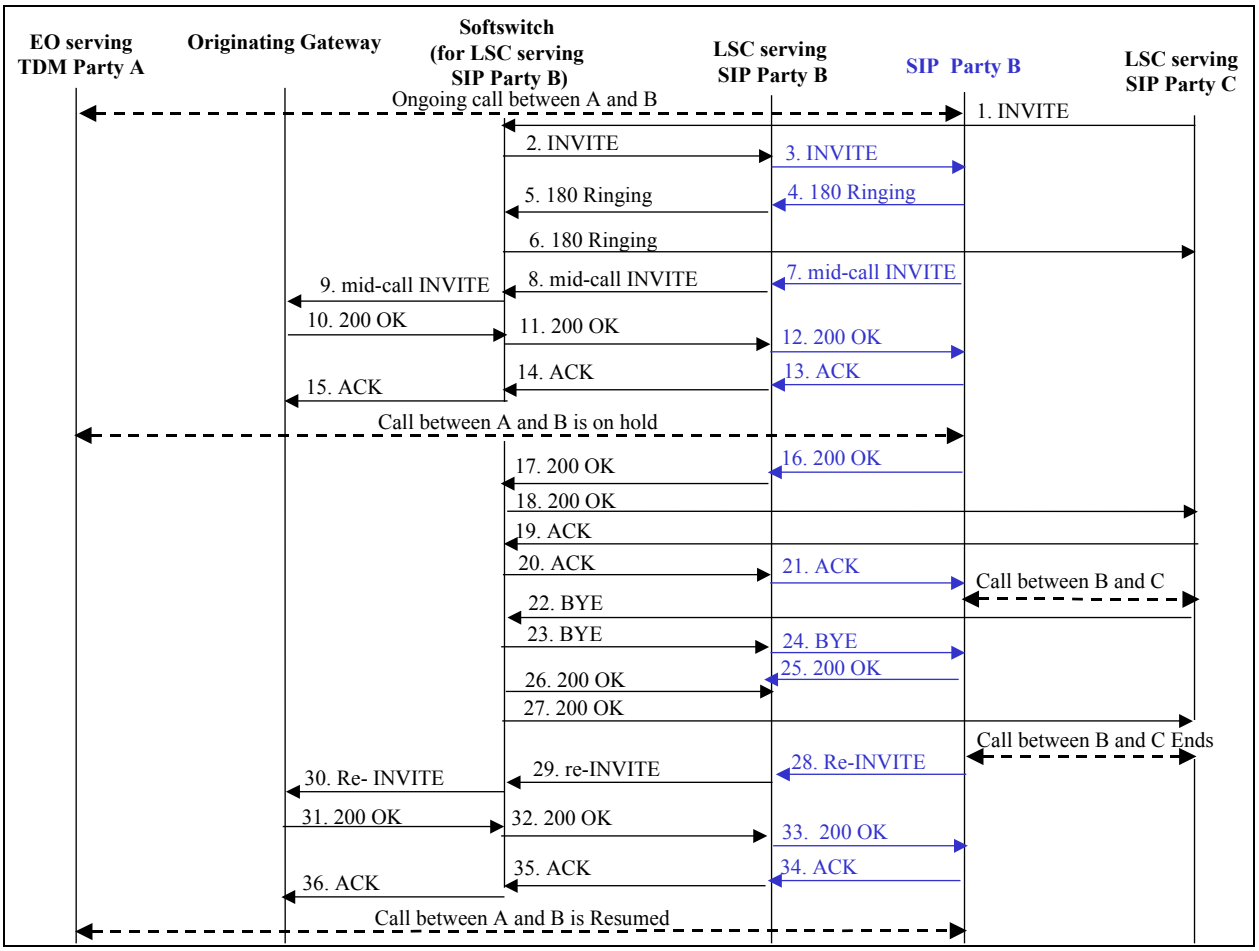


Figure 5.3.4-54. TDM-SIP Call Waiting (Performed at SIP Party B)
(SIP Signaling to SIP Party B End Instrument is Depicted for Illustrative Purposes)

5.3.4.19.4.3.2 Figure 5.3.4-55 depicts call waiting in which TDM Party A conducts a call hold on the existing session with IP Party B upon receiving the call waiting tone triggered by a call request from IP Party C. IP Party C conducts a call with TDM Party A and upon termination of that call TDM Party A resumes the call with IP Party B. NOTE: When TDM Party A signals its EO to place the call with IP Party B on hold, the EO does not transmit signaling therefore to the originating gateway and consequently there is no signaling inter-working for call hold onto the IP network. Similarly, when TDM Party A signals its EO to resume the call with IP Party B there is no signaling interworking with the IP network.

NOTE: A valid alternative scenario for resuming the call with IP Party B would have TDM Party A place the call with IP Party C on hold, resume the call with IP Party B whereupon IP Party C terminates its call with TDM Party A.

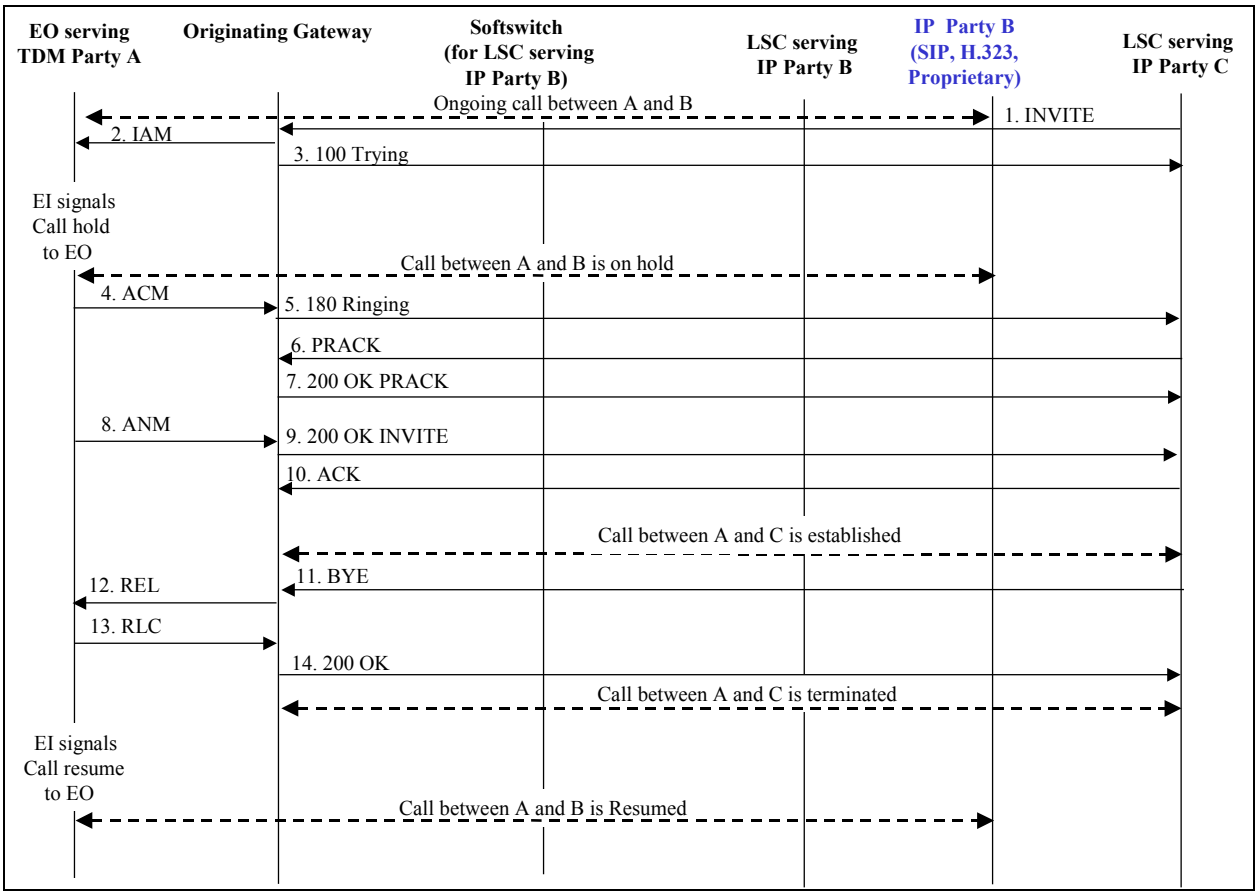


Figure 5.3.4-55. TDM-to-IP Call Waiting (Performed at TDM Party A)

Due to real estate constraints, the Softswitch assigned to the LSC serving IP Party C is also the originating gateway for the call between TDM Party A and IP Party B.

STEP	INSTRUCTION
1	Upon receiving an initial call request message from IP Party C (not depicted in call flow diagram), the LSC serving IP Party C sends an INVITE to its assigned Softswitch which is also the originating gateway. NOTE: Signaling between the end instrument serving IP Party C and the LSC serving IP Party C is not depicted.
2	The originating gateway receives the INVITE and sends an IAM to the end office serving TDM Party A.

STEP	INSTRUCTION
3	The originating gateway sends a 100 (Trying) to the LSC serving IP Party C. NOTE: Signaling between the LSC serving IP Party C and the end instrument serving IP Party C is not depicted.
Call Hold	TDM Party A receives the call waiting tone and signals call hold to its local end office. The local EO ceases forwarding any bearer traffic between TDM Party A and IP Party B. The original call between TDM Party A and TDM Party B is now on hold.

The original call between TDM Party A and IP Party B in now on hold.

STEP	INSTRUCTION
4	The end office serving TDM Party A sends an ACM to the originating gateway.
5	The originating gateway receives the ACM and sends a 180 (Ringing) to the LSC serving IP Party C. NOTE: Signaling between the LSC serving IP Party C and the end instrument serving IP Party C is not depicted.
6	The LSC serving IP Party C sends a PRACK to the originating gateway.
7	The originating gateway sends 200 OK PRACK to the LSC serving IP Party C.
8	The end office serving TDM Party A sends an ANM to the originating gateway.
9	The originating gateway receives the ANM and sends a 200 (OK) to the LSC serving IP Party C. NOTE: Signaling between the LSC serving IP Party C and the end instrument serving IP Party C is not depicted.
10	The LSC serving IP Party C sends an ACK to the originating gateway. NOTE: Signaling between the end instrument serving IP Party C and the LSC serving IP Party C is not depicted.

The call between TDM Party A and IP Party C is now established.

STEP	INSTRUCTION
11	When IP Party C is ready to terminate the call with TDM Party A then the LSC serving IP Party C sends a BYE to the originating gateway.

	NOTE: Signaling between the end instrument serving IP Party C and the LSC serving IP Party C is not depicted.
12	The originating gateway sends a REL to the end office serving TDM Party A.
13	The end office serving TDM Party A sends a RLC to the originating gateway.
14	The originating gateway sends a 200 (OK) to the LSC serving IP Party C. NOTE: Signaling between the LSC serving IP Party C and the end instrument serving IP Party C is not depicted.

The call between IP Party C and TDM Party A is now terminated.

STEP	INSTRUCTION
Call Resume	TDM Party A signals call resume to its local end office. The local EO reenables forwarding of bearer traffic between TDM Party A and IP Party B

The original call between TDM Party A and IP Party B is now resumed.

5.3.4.19.4.4 IP-to-TDM Call Type

5.3.4.19.4.4.1 Figure 5.3.4-56 depicts call waiting in which TDM Party B conducts a call hold on the existing session with IP Party A upon receiving the call waiting tone triggered by a call request from IP Party C. TDM Party B and IP Party C complete call set-up and engage in a conversation. IP Party C then terminates the call with TDM Party B and TDM Party B resumes its call with IP Party A. NOTE: When TDM Party B signals its EO to place the call with IP Party A on hold, the EO does not transmit signaling therefore to the originating gateway and consequently there is no signaling inter-working for call hold onto the IP network. Similarly, when TDM Party B signals its EO to resume the call with IP Party A, there is no signaling interworking with the IP network.

NOTE: A valid alternative scenario for resuming the call with IP Party A would have TDM Party B place the call with IP Party C on hold, resume the call with IP Party A whereupon IP Party C terminates its call with TDM Party B.

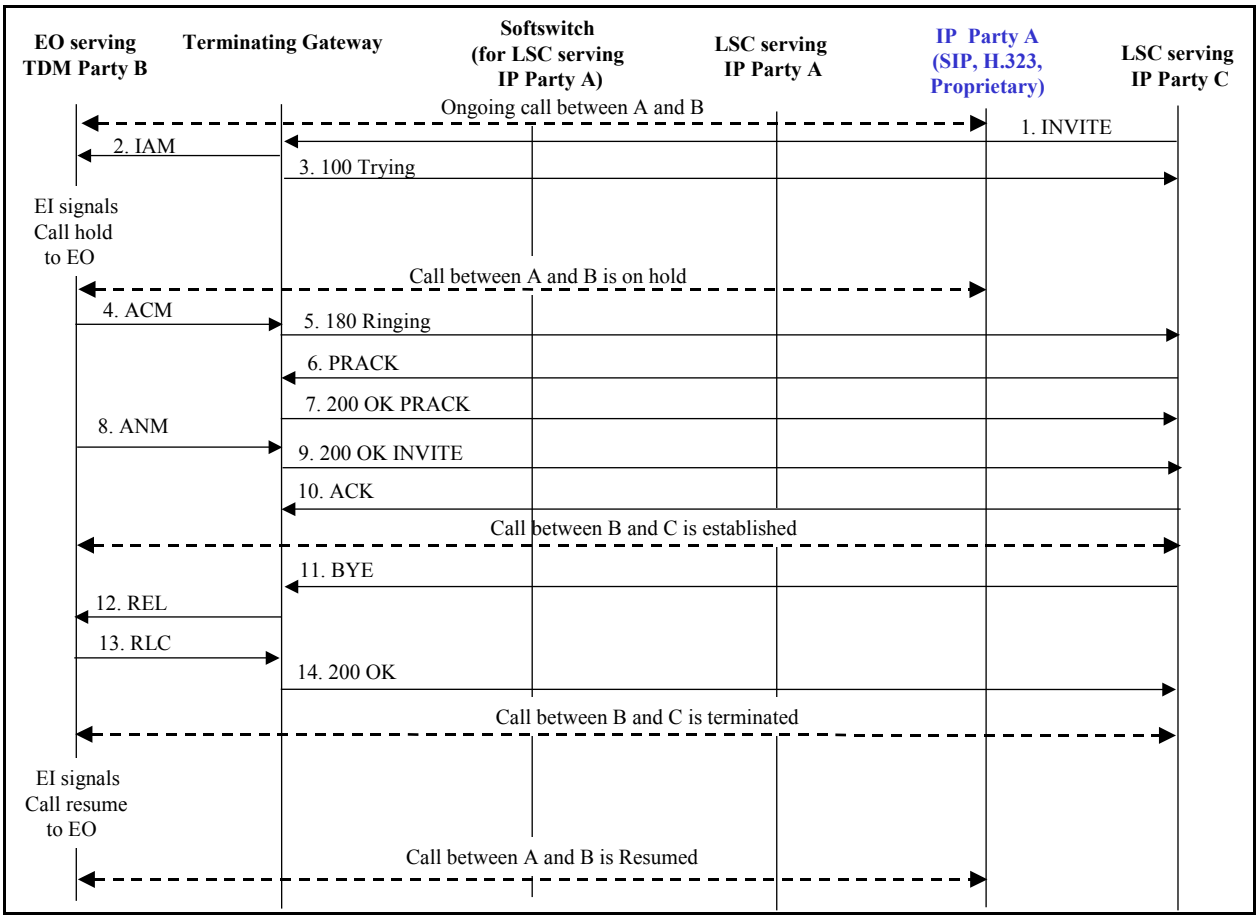


Figure 5.3.4-56. IP-to-TDM Call Waiting (Performed at TDM Party B)

Due to real estate constraints, the Softswitch assigned to the LSC serving IP Party C is also the terminating gateway for the call between TDM Party A and IP Party B.

STEP	INSTRUCTION
1	Upon receiving an initial call request message from IP Party C (not depicted in call flow diagram), the LSC serving IP Party C sends an INVITE to the terminating gateway (which is also the Softswitch for IP Party C). NOTE: Signaling between the end instrument serving IP Party C and the LSC serving IP Party C is not depicted.
2	The terminating gateway receives the INVITE and sends an IAM to the end office serving TDM Party B.

STEP	INSTRUCTION
3	The terminating gateway sends a 100 (Trying) to the LSC serving IP Party C. NOTE: Signaling between the LSC serving IP Party C and the end instrument serving IP Party C is not depicted.
Call Hold	TDM Party B receives the call waiting tone and signals call hold to its local end office. The local EO ceases forwarding any bearer traffic between TDM Party B and IP Party A.

The original call between IP Party A and TDM Party B in now on hold.

STEP	INSTRUCTION
4	The end office serving TDM Party B sends an ACM to the terminating gateway.
5	The terminating gateway receives the ACM and sends a 180 (Ringing) to the LSC serving IP Party C. NOTE: Signaling between the LSC serving IP Party C and the end instrument serving IP Party C is not depicted.
6	The LSC serving IP Party C sends a PRACK to the terminating gateway.
7	The terminating gateway sends a 200 OK to the LSC serving IP Party C.
8	The end office serving TDM Party B sends an ANM to the terminating gateway.
9	The terminating gateway receives the ANM and sends a 200 (OK) to the LSC serving IP Party C. NOTE: Signaling between the LSC serving IP Party C and the end instrument serving IP Party C is not depicted.
10	The LSC serving IP Party C sends an ACK to the terminating gateway. NOTE: Signaling between the end instrument serving IP Party C and the LSC serving IP Party C is not depicted.

The call between TDM Party B and IP Party C is now established.

STEP	INSTRUCTION
11	When IP Party C terminates the session with TDM Party B then the LSC serving IP Party C sends a BYE to the terminating gateway. NOTE: Signaling between the end instrument serving IP Party C and the LSC serving IP Party C is not depicted.
12	The terminating gateway receives the BYE and sends a REL to the end office serving TDM Party B.
13	The EO serving TDM Party B sends a RLC to the terminating gateway. NOTE: Signaling between the LSC serving IP Party C and the end instrument serving IP Party C is not depicted.
14	The terminating gateway sends a 200 (OK) to the LSC serving IP Party C NOTE: Signaling between the LSC serving IP Party C and the end instrument serving IP Party C is not depicted.

The call between IP Party C and TDM Party B is now terminated.

STEP	INSTRUCTION
Call Resume	TDM Party B signals call resume to its local end office. The local EO reenables forwarding of bearer traffic between TDM Party B and IP Party A

The original call between IP Party A and TDM Party B is now resumed.

5.3.4.19.4.4.2 Figure 5.3.4-57 depicts the sequence of AS-SIP messages employed to place the current IP-TDM call on hold in order to accept a call from a third Party C, and to terminate the call with the third Party C in order to resume the original call. (IP Party A performs the call waiting).

NOTE: When the terminating gateway receives the SIP message indicating call hold, the terminating gateway instucts its media gateway to cease forwarding bearer traffic between TDM Party B and IP Party A and vice versa. However, the terminating gateway does not translate the SIP signaling message indicating call hold to ISUP as the DSN TDM network does not signal call hold over the network. Similarly, when the terminating gateway receives the SIP message indicating call resume, the terminating gateway instucts its media gateway to resume forwarding bearer traffic between TDM Party B and IP Party A and vice versa. However, the terminating gateway does not translate the SIP signaling message indicating call resume into an ISUP message.

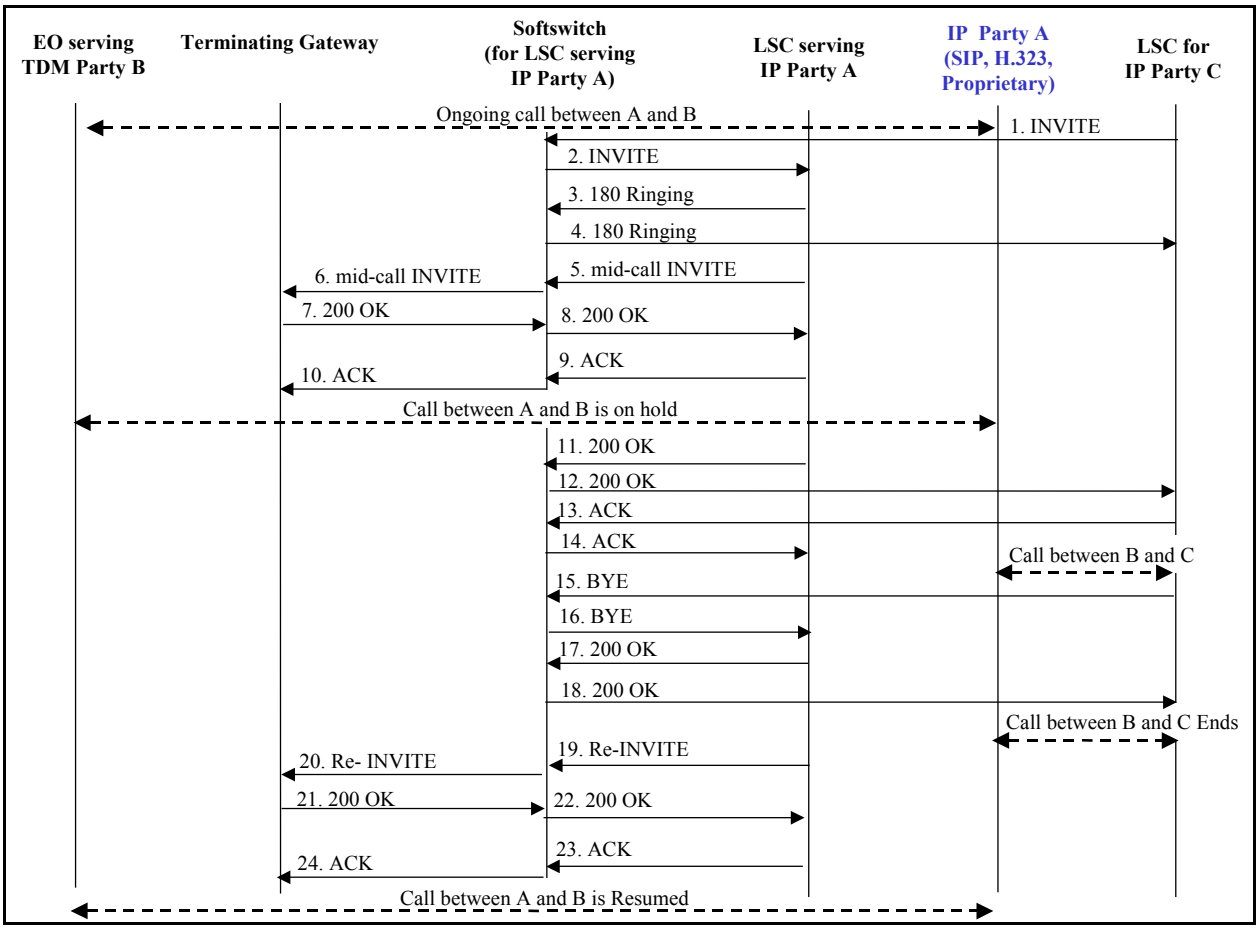


Figure 5.3.4-57. IP-to-TDM Call Waiting (Performed at IP Party A)

NOTE: A valid alternative scenario for resuming the call with TDM Party B would have IP Party A place the call with IP Party C on hold, resume the call with TDM Party B whereupon IP Party C terminates its call with IP Party A.

Due to real estate constraints, the same Softswitch is assigned to the LSC serving IP Party A and to the LSC serving IP Party C.

Figure 5.3.4-58 at the end of this subsection offers an illustrative example of the call signaling when IP Party A is a standard SIP end instrument.

STEP	INSTRUCTION
1	Upon receiving an initial call request message from IP Party C (not depicted in call flow diagram), the LSC serving IP Party C sends an INVITE to the Softswitch assigned to the LSC serving IP Party A. NOTE: Signaling between the end instrument serving IP Party C and the LSC serving IP Party C is not depicted.
2	The Softswitch sends the INVITE to the LSC serving IP Party A. NOTE: Signaling between the LSC serving IP Party A and the end instrument serving IP Party A is not depicted.
3, 4	The LSC serving IP Party A sends a 180 (Ringing) to the Softswitch, which forwards the 180 (Ringing) to the LSC serving IP Party C. NOTE: Signaling between the end instrument serving IP Party A and the LSC serving IP Party A is not depicted. NOTE: Signaling between the LSC serving IP Party C and the end instrument serving IP Party C is not depicted.
5, 6	The LSC serving IP Party A sends a mid-call INVITE to the Softswitch, which forwards the mid-call INVITE to the terminating gateway. The mid-call INVITE includes the attribute line "a=sendonly" or "a=inactive" if the stream had been a sendrecv media stream or "a=inactive" if the stream had been a recvonly stream. The terminating gateway instructs its media gateway to cease forwarding bearer traffic between IP Party B and TDM Party A and vice versa. NOTE: The LSC serving IP Party A MUST also support establishing a call hold by sending a mid-call INVITE that includes a session description that is the same as in the original request, but the "c" destination addresses for the media streams to be put on hold are set to zero: c=IN IP4 0.0.0.0. NOTE: Signaling between the end instrument serving IP Party A and the LSC serving IP Party A is not depicted.
7, 8	The terminating gateway sends a 200 (OK) INVITE to the Softswitch, which forwards the 200 (OK) INVITE to the LSC serving IP Party A. NOTE: Signaling between the LSC serving IP Party A and the end instrument serving IP Party A is not depicted.

STEP	INSTRUCTION
9, 10	The LSC serving IP Party A sends an ACK to the Softswitch, which forwards the ACK to the terminating gateway. NOTE: Signaling between the end instrument serving IP Party A and the LSC serving IP Party A is not depicted.

The original call between IP Party A and TDM Party B is now on hold.

STEP	INSTRUCTION
11, 12	The LSC serving IP Party A sends a 200 (OK) to the Softswitch, which forwards the 200 (OK) to the LSC serving IP Party C. NOTE: Signaling between the end instrument serving IP Party A and the LSC serving IP Party A is not depicted. NOTE: Signaling between the LSC serving IP Party C and the end instrument serving IP Party C is not depicted.
13, 14	The LSC serving IP Party C sends an ACK to the Softswitch, which forwards the ACK to the LSC serving IP Party A. NOTE: Signaling between the end instrument serving IP Party C and the LSC serving IP Party C is not depicted. NOTE: Signaling between the LSC serving IP Party A and the end instrument serving IP Party A is not depicted.

The call between IP Party C and IP Party A is now established.

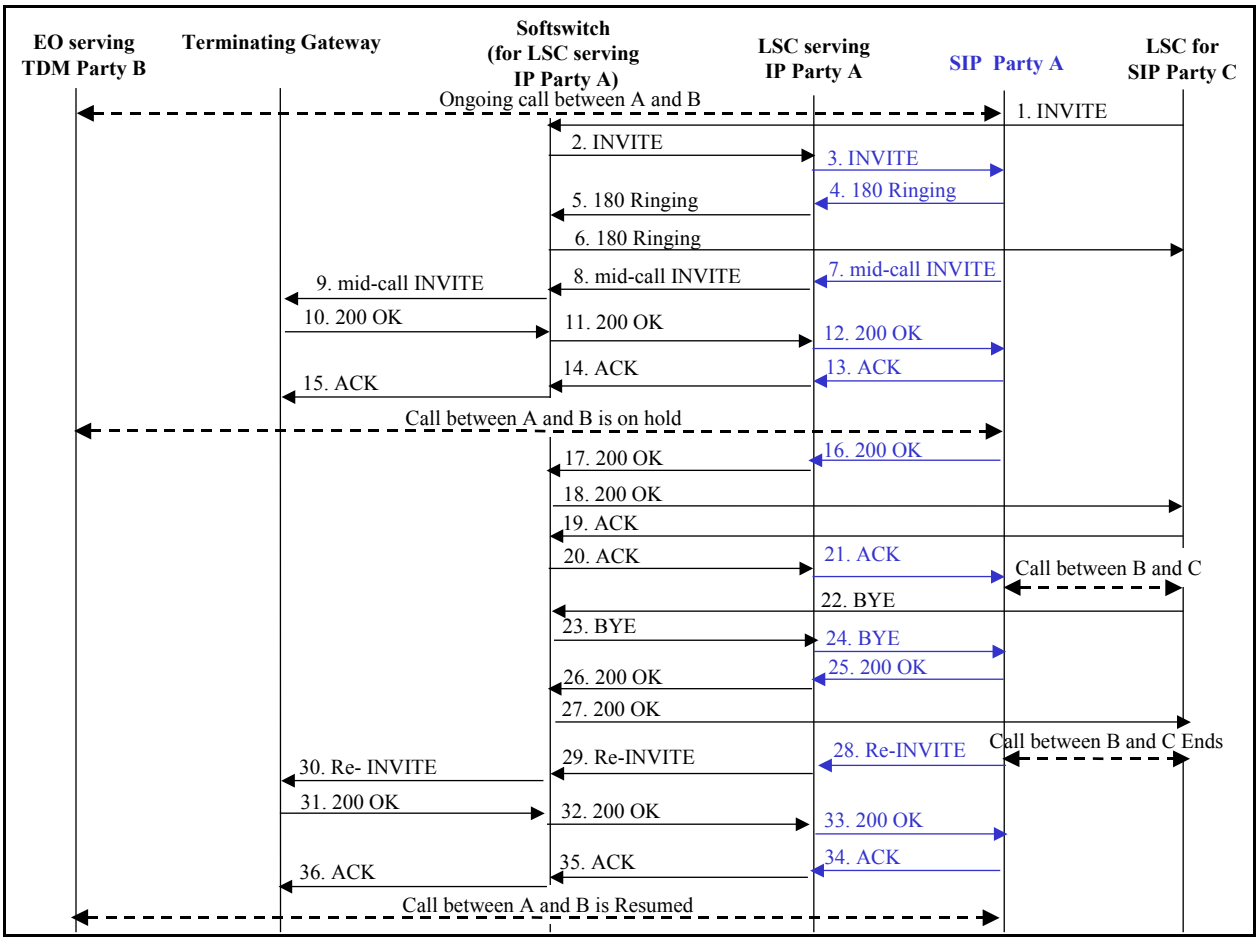
STEP	INSTRUCTION
15, 16	When IP Party C terminates the session with IP Party A then the LSC serving IP Party C sends a BYE to the Softswitch, which forwards the BYE to the LSC serving IP Party A. NOTE: Signaling between the end instrument serving IP Party C and the LSC serving IP Party C that initiated the call release is not depicted. NOTE: Signaling between the LSC serving IP Party A and the end instrument serving IP Party A is not depicted.

17, 18	The LSC serving IP Party A sends a 200 (OK) response to the Softswitch, which forwards the 200 (OK) response to the LSC serving IP Party C. NOTE: Signaling between the end instrument serving IP Party A and the LSC serving IP Party A is not depicted. NOTE: Signaling between the LSC serving IP Party C and the end instrument serving IP Party C is not depicted.

The call between IP Party C and IP Party A is now terminated.

STEP	INSTRUCTION
19, 20	The LSC serving IP Party A sends a mid-call re-INVITE to the Softswitch, which forwards the mid-call re-INVITE to the terminating gateway. The mid-call re-INVITE includes the attribute line "a=sendrecv" if the stream had originally been a sendrecv media stream or "a=recvonly" if the stream had been a recvonly stream. The terminating gateway instructs its media gateway to resume forwarding bearer traffic between IP Party B and TDM Party A and vice versa. NOTE: In the case of a call hold established by setting the "c" destination address to 0.0.0.0, another re-INVITE with the original address parameter terminates the call hold. NOTE: Signaling between the end instrument serving IP Party A and the LSC serving IP Party A is not depicted.
21, 22	The terminating gateway sends a 200 (OK) to the Softswitch, which forwards the 200 (OK) to the LSC serving IP Party A. NOTE: Signaling between the LSC serving IP Party A and the end instrument serving IP Party A is not depicted.
23, 24	The LSC serving IP Party A sends an ACK to the Sofswitch, which forwards the ACK to the terminating gateway. NOTE: Signaling between the end instrument serving IP Party A and the LSC serving IP Party A is not depicted.

The original call between IP Party A TDM and Party B is now resumed.



5.3.4-58. SIP-TDM Call Waiting (Performed at SIP Party A)
(SIP Signaling to SIP Party A End Instrument is Depicted for Illustrative Purposes)

5.3.4.19.5 Call Forward (Unconditional)

A user instructs that call requests to a particular phone number be routed to a different predefined phone number. In the following call flow diagrams user B has instructed that call requests addressed to B's phone number at location 1 be rerouted to a different phone number for an end instrument at location 2.

As specified in UCR 2008, Section 5.3.4.7.6, SIP URI and Mapping of Telephony Number into SIP URI, and UCR 2008, Section 5.3.4.14.3, SIP URI and Mapping of Telephony Number into SIP URI, the addressing format for the SIP messages MUST be a SIP URI having a userinfo part that is either a full 10-digit number from the DSN worldwide numbering plan which may include a phone-context descriptor or an E.164 encoded phone number and having a 'user=phone' field appended to the URI.

5.3.4.19.5.1 IP-to-IP Call Type

See UCR 2008, Section 5.3.4.13.5.1, IP-to-IP Call Type.

5.3.4.19.5.2 TDM Bridging Call Type

5.3.4.19.5.2.1 Figure 5.3.4-59 depicts the sequence of AS-SIP and ISUP messages between the end office serving TDM Party A and the end office serving TDM Party B that are involved in the unconditional forwarding of a call request intended for TDM Party B at location 1 to a forwarded phone number corresponding to a TDM end instrument for Party B at location 2. In this scenario, the call forwarding is conducted within the ISUP network.

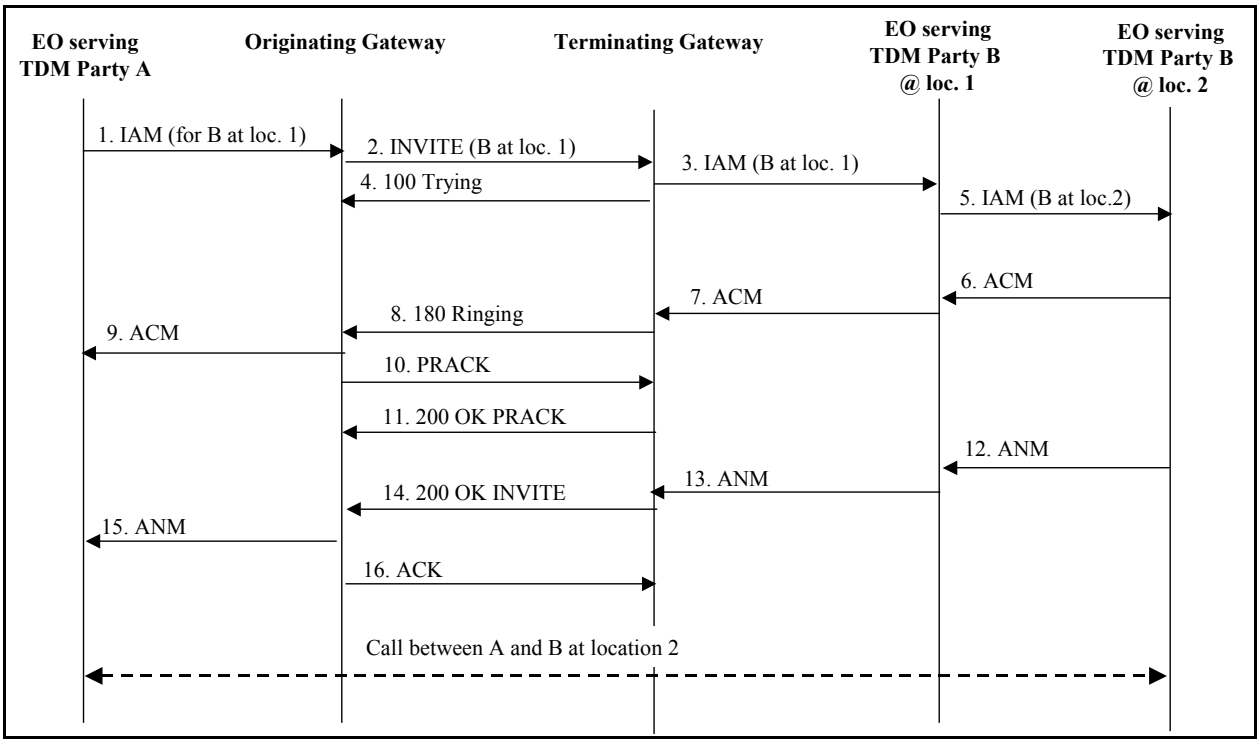


Figure 5.3.4-59. TDM Bridging Call Forward Unconditional (Call Forward Signaling Occurs within ISUP Network)

Call Forward

STEP	INSTRUCTION
1	The end office serving TDM Party A sends an IAM (intended for TDM Party B at location 1) to the originating gateway.

STEP	INSTRUCTION
2	The originating gateway creates an INVITE and sends the INVITE to the terminating gateway providing connectivity to the end office serving TDM Party B at location 1.
3	The terminating gateway receives the INVITE, creates an IAM, translates the fields of the INVITE to those of the IAM, and sends the IAM to the end office serving TDM Party B at location 1.
4	The terminating gateway sends a 100 (Trying) to the originating gateway.
5	The end office serving TDM Party B at location 1 has been notified by user B to forward all calls to another number (i.e., TDM end instrument for Party B at location 2). Upon receiving the IAM from the terminating gateway intended for TDM Party B at location 1, the end office modifies the IAM to reflect the call forward (e.g., adds the Original Called Number (OCN) parameter and the Redirection Information parameter which includes the Original Redirection Reason set to "0011" (Unconditional call forward), the Redirect counter, etc.) and sends the IAM on the CCS7 network to the end office serving TDM Party B at location 2.
6	The end office serving TDM Party B at location 2 initiates the ringing tone on the TDM end instrument at location 2 and sends an ACM to the end office serving TDM Party B at location 1. The Notification Indicators field in the ACM is set to "1111011" (call is forwarded/deflected). The Called Party's Status Indicator of the Backward Call Indicators is set to "01" (Subscriber free).
7	The end office serving TDM Party B at location 1 forwards the ACM to the terminating gateway.
8	The terminating gateway creates a 180 (Ringing) response, and sends the 180 (Ringing) response to the originating gateway.
9	The originating gateway receives the 180 Ringing, creates an ACM and sends the ACM to the end office serving TDM Party A.
10	The originating gateway sends a PRACK to the terminating gateway.
11	The terminating gateway sends a 200 OK PRACK to the originating gateway.
12	The end office serving TDM Party B at location 2 sends an ANM to the end office serving TDM Party B at location 1.
13	The end office serving TDM Party B at location 1 forwards the ANM to the terminating gateway.
14	The terminating gateway creates a 200 (OK) response, and sends the 200 (OK) response to the originating gateway.

STEP	INSTRUCTION
15	The originating gateway receives the 200 (OK), creates an ANM, and sends the ANM to the end office serving TDM Party A.
16	The originating gateway sends an ACK to the terminating gateway.

The forwarded call is now established between TDM Party A and TDM Party B at location 2.

5.3.4.19.5.3 TDM-to-IP Call Type

5.3.4.19.5.3.1 Figure 5.3.4-60 depicts the sequence of AS-SIP and ISUP messages between the end office serving TDM Party A, the LSC serving IP Party B at location 1 (which unconditionally forwards call requests intended for IP Party B at location 1 to IP Party B at location 2), and the LSC serving IP Party B at location 2.

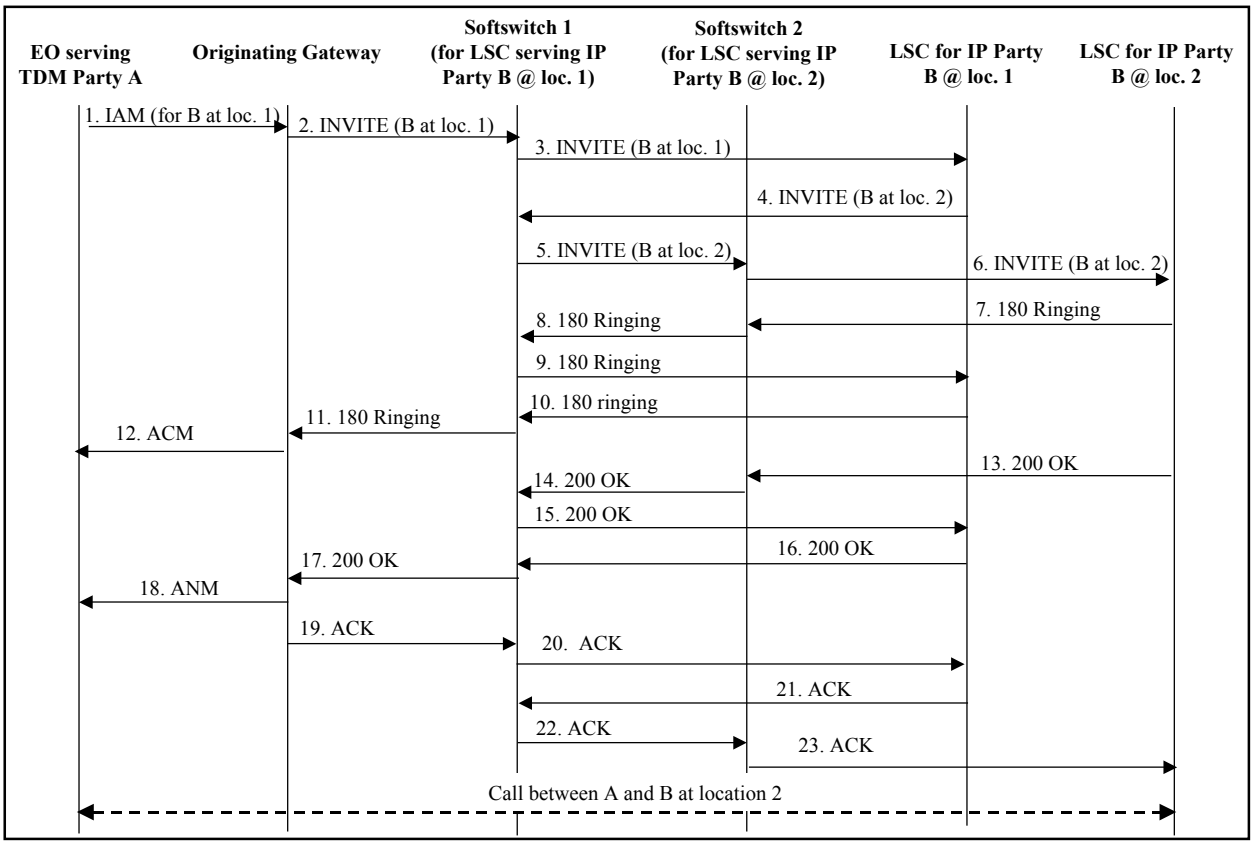


Figure 5.3.4-60. TDM-to-IP Call Forwarding

NOTE: For IP end instruments directly served by a given LSC, said LSC is the signaling platform that will be apprised of the call forwarding preference of the user. This being the case, and given that we are adopting the approach described in draft-ietf-sipping-service-examples~~-10~~ which implements call forward by rewriting the Request-URI field (as opposed to conducting a redirect), the LSC serving IP Party B at location 1 will stay in the call path for the SIP signaling. This means SIP signaling messages will be routed from the Softswitch responsible for the LSC serving IP Party B at location 1 to the LSC serving IP Party B at location 1 and then return back to the Softswitch for routing towards the LSC serving IP Party B at location 2.

NOTE: In order to simplify the call flow diagram the 100 Trying responses have been omitted.

Call Forward

STEP	INSTRUCTION
1	The end office serving TDM Party A sends an IAM (intended for IP Party B at location 1) to the originating gateway.
2	The originating gateway creates an INVITE and sends the INVITE to Softwitch 1 (which is responsible for the LSC serving IP Party B at location 1).
3	Softswitch 1 forwards the INVITE to the LSC serving IP Party B at location 1.
4	The LSC serving IP Party B at location 1 has previously been notified to unconditionally forward call requests intended for the IP end instrument associated with Party B at location 1 to the SIP URI for IP Party B at location 2. The LSC serving IP Party B at location 1 rewrites the request URI and sends the INVITE back to Softswitch 1 for forwarding to IP Party B at location 2.
5	Softswitch 1 sends the INVITE to Softswitch 2 (which is responsible for the LSC serving IP Party B at location 2).
6	Softswitch 2 sends the INVITE to the LSC serving IP Party B at location 2. NOTE: Signaling between the LSC serving IP Party B at location 2 and the IP end instrument at location 2 is not depicted.

STEP	INSTRUCTION
7, 8, 9, 10, 11	The LSC serving IP Party B at location 2 sends a 180 (Ringing) response to Softswitch 2. Softswitch 2 forwards the 180 (Ringing) response to Softswitch 1. Softswitch 1 forwards the 180 (Ringing) response to the LSC serving IP Party B at location 1. The LSC serving IP Party B at location 1 forwards the 180 (Ringing) response back to Softswitch 1. Softswitch 1 forwards the 180 (Ringing) response to the originating gateway. NOTE: Signaling between the IP end instrument serving IP Party B at location 2 and the LSC serving IP Party B at location 2 is not depicted.
12	The originating gateway receives the 180 (Ringing) response and creates an ACM which it sends to the end office serving TDM Party A.
13, 14, 15, 16, 17	The LSC serving IP Party B at location 2 sends a 200 (OK) response to Softswitch 2. Softswitch 2 forwards the 200 (OK) response to Softswitch 1. Softswitch 1 forwards the 200 (OK) response to the LSC serving IP Party B at location 1. The LSC serving IP Party B at location 1 forwards the 200 (OK) response back to Softswitch 1. Softswitch 1 forwards the 200 (OK) response to the originating gateway. NOTE: Signaling between the IP end instrument serving IP Party B at location 2 and the LSC serving IP Party B at location 2 is not depicted.
18	The originating gateway receives the 200 (OK) response and creates an ANM which it sends to the end office serving TDM Party A.
19, 20, 21, 22, 23	The originating gateway sends an ACK to Softswitch 1. Softswitch 1 forwards the ACK to the LSC serving IP Party B at location 1. The LSC serving IP Party B at location 1 forwards the ACK back to Softswitch 1. Softswitch 1 forwards the ACK to Softswitch 2. Softswitch 2 forwards the ACK to the LSC serving IP Party B at location 2. NOTE: Signaling between the LSC serving IP Party B at location 2 and the IP end instrument at location 2 is not depicted.

5.3.4.19.5.4 IP-to-TDM Call Type

5.3.4.19.5.4.2 Figure 5.3.4-61 depicts the sequence of AS-SIP and ISUP messages between the LSC serving IP Party A, the end office serving TDM Party B at location 1, and the end office serving TDM Party B at location 2 that are involved in the unconditional forwarding of a call

request intended for TDM Party B at location 1 to a forwarded phone number corresponding to a TDM end instrument for Party B at location 2. In this scenario, the call forwarding occurs in the ISUP network.

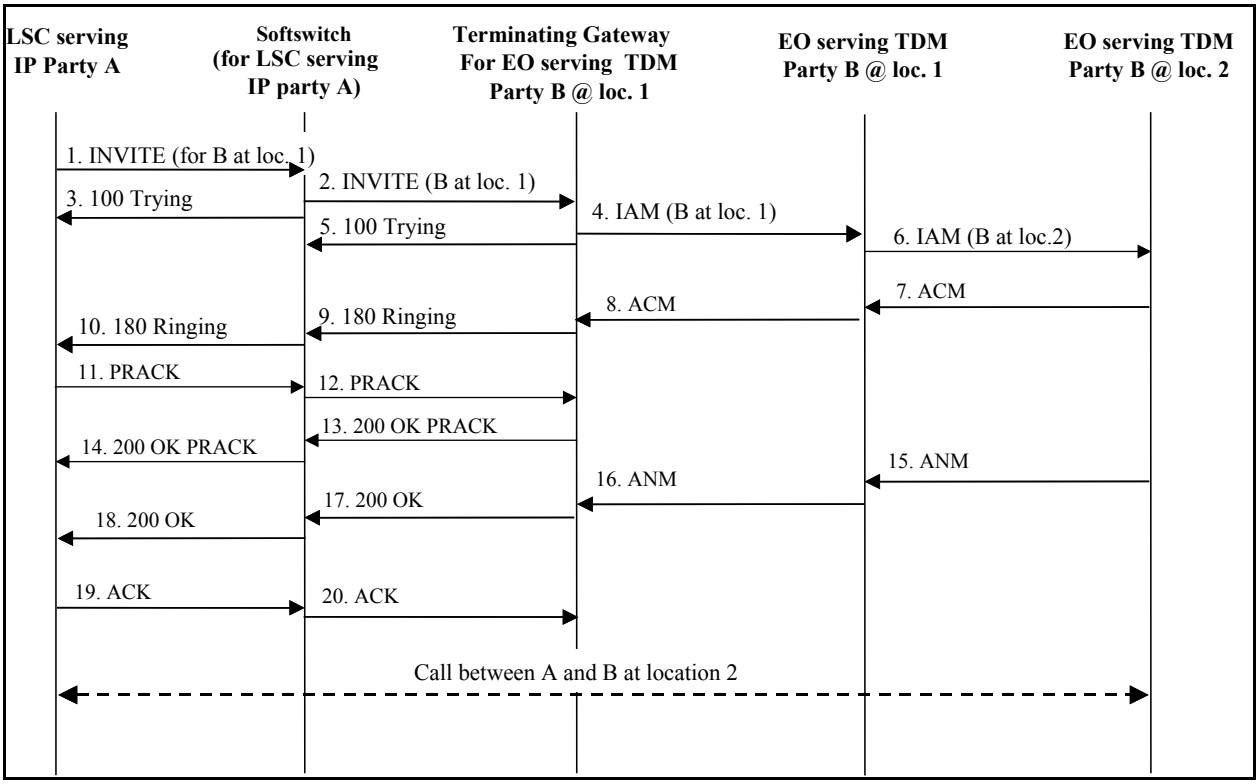


Figure 5.3.4-61. IP-to-TDM Call Forwarding (Call Forward Signaling Occurs in ISUP Network)

Call Forward

STEP	INSTRUCTION
1	The LSC serving IP Party A sends an INVITE to its assigned Softswitch. NOTE: Signaling between the IP end instrument serving IP Party A and the LSC serving IP Party A is not depicted.
2	The Softswitch forwards the INVITE to the terminating gateway.
3	The Softswitch sends a 100 (Trying) to the LSC serving IP Party A.
4	The terminating gateway sends an IAM to the end office serving TDM Party B at location 1.

STEP	INSTRUCTION
5	The terminating gateway sends a 100 (Trying) to the Softswitch.
6	The end office serving TDM Party B at location 1 has been notified by user B to forward all calls to another number (i.e., TDM end instrument for Party B at location 2). Upon receiving the IAM from the terminating gateway intended for TDM Party B at location 1, the end office modifies the IAM to reflect the call forward (e.g., adds the Original Called Number (OCN) parameter and the Redirection Information parameter, which includes the Original Redirection Reason set to "0011" (Unconditional call forward), the Redirect counter, etc.) and sends the IAM on the CCS7 network to the end office serving TDM Party B at location 2.
7	The end office serving TDM Party B at location 2 initiates ringing of the TDM end instrument at location 2 and sends an ACM to the end office serving TDM Party B at location 1. The Notification Indicators field in the ACM is set to "1111011" (call is forwarded/deflected). The Called Party's Status Indicator of the Backward Call Indicators is set to "01" (Subscriber free).
8	The end office serving TDM Party B at location 1 forwards the ACM to the terminating gateway.
9, 10	The terminating gateway receives the ACM, creates a 180 (Ringing) response, and sends the 180 (Ringing) response to the Softswitch, which, in turn, forwards the 180 (Ringing) to the LSC serving IP Party A. NOTE: Signaling between the LSC serving IP Party A and the IP end instrument serving IP Party A is not depicted.
11, 12	The LSC serving IP Party A sends a PRACK to the Softswitch, which forwards the PRACK to the terminating gateway.
13, 14	The terminating gateway sends a 200 OK to the Softswitch which forwards the 200 OK to the LSC serving IP Party A.
15	The end office serving TDM Party B at location 2 sends an ANM to the end office serving TDM Party B at location 1.
16	The end office serving TDM Party B at location 1 forwards the ANM to the terminating gateway.
17, 18	The terminating gateway receives the ANM, creates a 200 (OK) response, and sends the 200 (OK) response to the Softswitch, which forwards the 200 (OK) to the LSC serving IP Party A. NOTE: Signaling between the LSC serving IP Party A and the IP end instrument serving IP Party A is not depicted.

STEP	INSTRUCTION
19, 20	The LSC serving IP Party A sends an ACK to the Softswitch, which forwards the ACK to the terminating gateway. NOTE: Signaling between the IP end instrument serving IP Party A and the LSC serving IP Party A is not depicted.

The forwarded call is now established between IP Party A and TDM Party B at location 2.

5.3.4.19.6 Call Forward (No Answer)

A user instructs that call requests to a particular phone number be routed to a different predefined phone number in the event the call is not answered within some number of rings (No Answer). In the following call flow diagrams, user B has instructed that call requests addressed to B's phone number at location 1, which receive no reply be rerouted to a different phone number for an end instrument at location 2.

5.3.4.19.6.1 IP-to-IP Call Type

See UCR 2008, Section 5.3.4.13.6.1, IP-to-IP Call Type.

5.3.4.19.6.2 TDM Bridging Call Type

5.3.4.19.6.2.1 Figure 5.3.4-62 depicts the sequence of AS-SIP and ISUP messages involved in forwarding of an unanswered call request for TDM Party B at location 1 to a forwarded phone number corresponding to a TDM end instrument for Party B at location 2.

Call Forward

STEP	INSTRUCTION
1	The end office serving TDM Party A sends an IAM (intended for TDM Party B at location 1) to the originating gateway.
2	The originating gateway creates an INVITE and sends the INVITE to the terminating gateway providing connectivity to the end office serving TDM Party B at location 1.
3	The terminating gateway receives the INVITE, creates an IAM (using the information in the INVITE), and sends the IAM to the end office serving TDM Party B at location 1.
4	The terminating gateway sends a 100 (Trying) to the originating gateway.

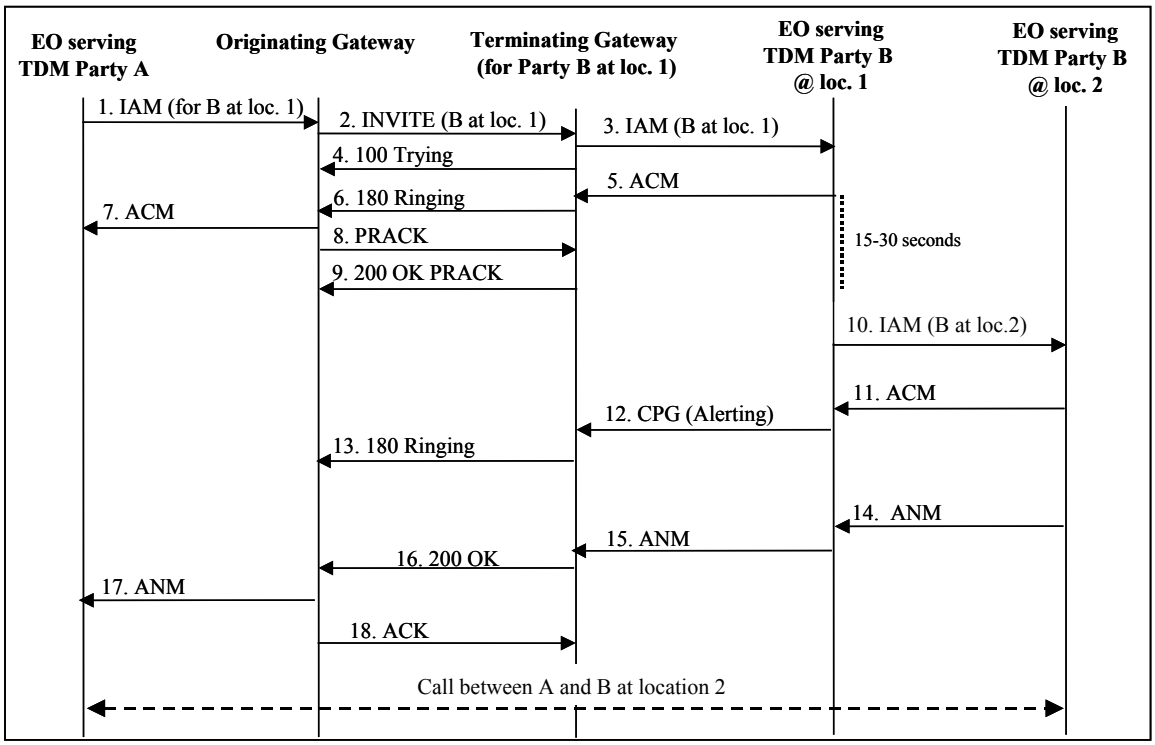


Figure 5.3.4-62. TDM Bridging Call Forwarding on No Answer

STEP	INSTRUCTION
5	The end office serving TDM Party B at location 1 has been notified by user B that in the event of a no reply the call is to be forwarded to another number (located at a different EO). Upon receiving the IAM from the terminating gateway, the end office initiates a ringing tone at the TDM end instrument and sends an ACM to the terminating gateway while waiting between 15 to 30 seconds for Party B to go off-hook. The Called Party's Status Indicator of the Backward Call Indicators is set to "01" (Subscriber free). The Optional Backward Call Indicators parameter is present and the Call Forwarding MAY Occur Indicator of the Optional Backward Call Indicators parameter is set to "1" (Call forwarding may occur).
6	The terminating gateway receives the ACM, creates a 180 Ringing response and sends the 180 Ringing response to the originating gateway.
7	The originating gateway translates the 180 ringing response to an ACM and sends the ACM to the end office serving TDM Party A.
8	The originating gateway sends a PRACK to the terminating gateway.
9	The terminating gateway sends a 200 OK PRACK to the originating gateway.

STEP	INSTRUCTION
10	Upon no reply, the end office serving TDM Party B at location 1 modifies the IAM to reflect the call forward (e.g., adds the Original Called Number (OCN) parameter and the Redirection Information parameter which includes the Original Redirection Reason set to "0010" (No reply), the Redirection counter, etc.) and sends the IAM on the CCS7 network to the end office serving TDM Party B at location 2
11	The end office serving TDM Party B at location 2 initiates the ringing of the end instrument at location 2 and sends an ACM to the end office serving TDM Party B at location 1. The Notification Indicators field in the ACM is set to "1111011" (call is forwarded/deflected). The Called Party's Status Indicator of the Backward Call Indicators is set to "01" (Subscriber free).
12	The end office serving TDM Party B at location 1 receives the ACM and creates a CPG with the event code set to 1 (Alerting) which it sends to the terminating gateway.
13	The terminating gateway creates a 180 ringing response and sends the 180 ringing response to the originating gateway.
14	The end office serving TDM Party B at location 2 sends an ANM to the end office serving TDM Party B at location 1.
15	The end office serving TDM Party B at location 1 forwards the ANM to the terminating gateway.
16	The terminating gateway receives the ANM, creates a 200 (OK) response, and sends the 200 (OK) response to the originating gateway.
17	The originating gateway receives the 200 (OK) response, creates an ANM, and sends the ANM to the end office serving TDM Party A.
18	The originating gateway sends an ACK to the terminating gateway.

The forwarded call is now established between TDM Party A and TDM Party B at location 2.

5.3.4.19.6.3 TDM-to-IP Call Type

5.3.4.19.6.3.1 Figure 5.3.4-63 depicts the sequence of AS-SIP and ISUP messages involved in forwarding an unanswered call request for IP Party B at location 1 to a forwarded phone number (SIP URI) corresponding to an IP end instrument for Party B at location 2. In the present scenario the LSC serving IP Party B at location 1 has previously been notified that upon a 'no answer' the LSC is to forward calls to IP Party B at location 2.

NOTE: In order to simplify the call flow diagram the 100 Trying responses have been omitted.

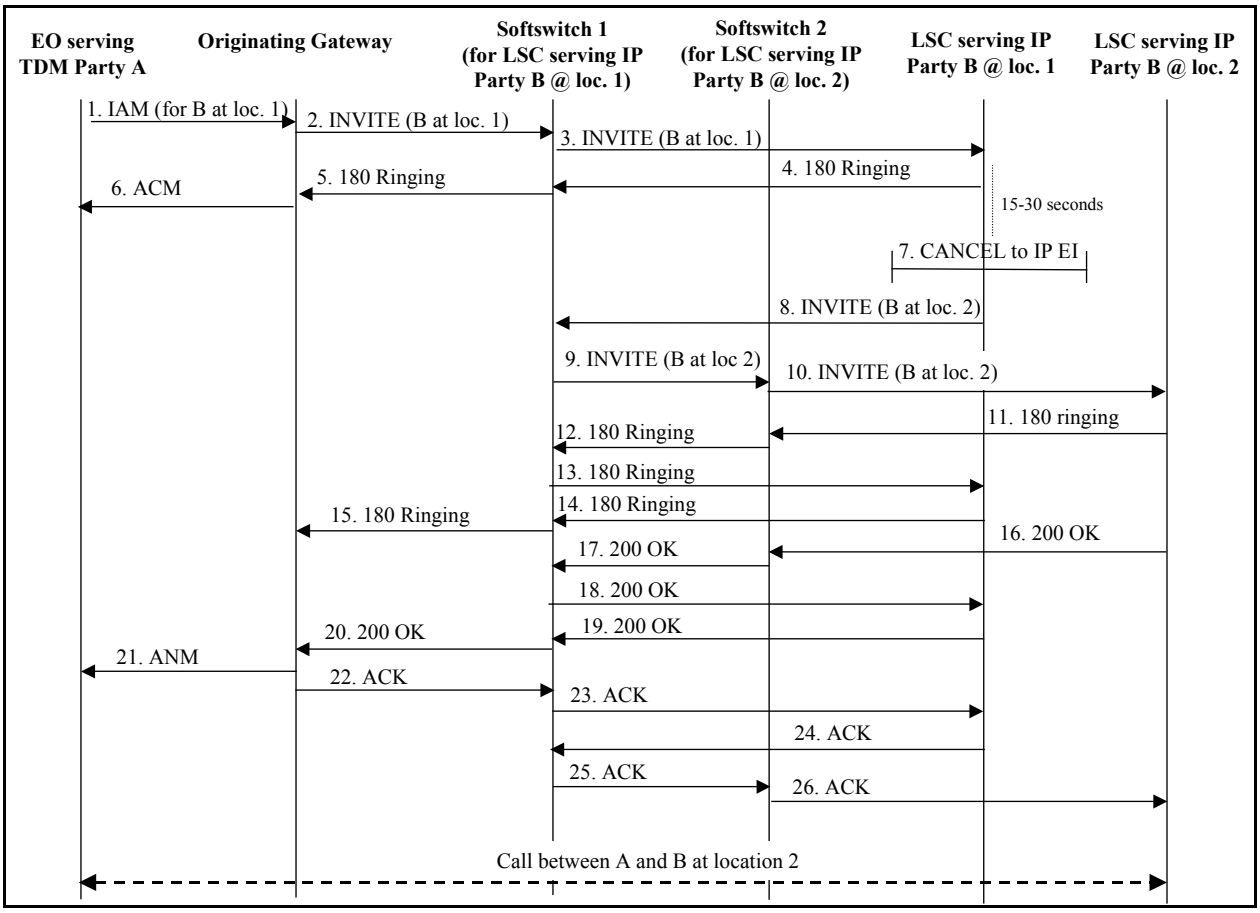


Figure 5.3.4-63. TDM-to-IP Call Forwarding on No Answer

Call Forward

STEP	INSTRUCTION
1	The end office serving TDM Party A sends an IAM (intended for TDM Party B at location 1) to the originating gateway.
2	The originating gateway creates an INVITE, and sends the INVITE to Softswitch 1 (which is responsible for the LSC serving IP Party B at location 1).
3	Softswitch 1 forwards the INVITE to the LSC serving IP Party B at location 1. NOTE: Signaling between the LSC serving IP Party B at location 1 and the IP end instrument serving IP Party B at location 1 is not depicted.

STEP	INSTRUCTION
4, 5	The LSC serving IP Party B at location 1 sends a 180 (Ringing) to Softswitch 1, which forwards the 180 (Ringing) to the originating gateway. NOTE: User B has previously instructed the LSC that in the event of no reply to the call within a predefined time period the call request is to be forwarded to another number (SIP URI) corresponding to an IP end instrument at location 2. NOTE: Signaling between the IP end instrument serving IP Party B at location 1 and the LSC serving IP Party B at location 1 is not depicted.
6	The originating gateway receives the 180 (Ringing) and sends an ACM to the end office serving the TDM end instrument.
7	If there is no answer within the predefined time interval (e.g., 15 to 30 seconds), then the LSC serving IP Party B at location 1 cancels the call request with the IP end instrument for Party B at location 1. NOTE: In the case of a SIP end instrument the LSC sends a CANCEL request, the SIP end instrument sends a 200 OK response to the CANCEL and a 487 (Request terminated) response to the INVITE and the LSC responds with an ACK to the 487 (Request terminated).
8	The LSC serving IP Party B at location 1 rewrites the Request-URI to reflect that the call is now intended for IP Party B at location 2 and sends the INVITE to Softswitch 1.
9, 10	Softswitch 1 sends the INVITE to Softswitch 2 (which is responsible for the LSC serving IP Party B at location 2) and Softswitch 2 sends the INVITE to the LSC serving IP Party B at location 2. NOTE: The signaling between the LSC serving IP Party B at location 2 and the IP end instrument for Party B at location 2 is not depicted.
11, 12, 13, 14, 15	The LSC serving IP Party B at location 2 sends a 180 Ringing to Softswitch 2. Softswitch 2 sends the 180 Ringing to Softswitch 1. Softswitch 1 send the 180 Ringing to the LSC serving IP Party B at location 1. The LSC serving IP Party B at location 1 sends the 180 Ringing back to Softswitch 1. Softswitch 1 sends the 180 Ringing to the originating gateway. NOTE: The signaling between the IP end instrument for Party B at location 2 to the LSC serving IP Party B at location 2 is not depicted.

STEP	INSTRUCTION
16, 17, 18, 19, 20	The LSC serving IP Party B at location 2 sends a 200 OK to Softswitch 2. Softswitch 2 sends the 200 OK to Softswitch 1. Softswitch 1 send the 200 OK to the LSC serving IP Party B at location 1. The LSC serving IP Party B at location 1 sends the 200 OK back to Softswitch 1. Softswitch 1 sends the 200 OK to the originating gateway. NOTE: The signaling between the IP end instrument for Party B at location 2 to the LSC serving IP Party B at location 2 is not depicted.
21	The originating gateway sends an ANM to the EO serving TDM Party A.
22, 23, 24, 25, 26	The originating gateway sends an ACK to Softswitch 1. Softswitch 1 sends the ACK to the LSC serving IP Party B at location 1. The LSC serving IP Party B at location 1 sends the ACK back to Softswitch 1. Softswitch 1 sends the ACK to Softswitch 2. Softswitch 2 sends the ACK to the LSC serving IP Party B at location 2. NOTE: The signaling between the LSC serving IP Party B at location 2 and the IP end instrument serving Party B at location 2 is not depicted.

The forwarded call is now established between TDM Party A and IP Party B at location 2.

5.3.4.19.6.4 IP-to-TDM Call Type

5.3.4.19.6.4.1 Figure 5.3.4-64 depicts the sequence of AS-SIP and ISUP messages involved in forwarding an unanswered call request for TDM Party B at location 1 to a forwarded phone number corresponding to a TDM end instrument for Party B at location 2.

Call Forward

STEP	INSTRUCTION
1	The LSC serving IP Party A sends an INVITE to its assigned Softswitch. NOTE: Signaling between the IP end instrument serving IP Party A and the LSC serving IP Party A is not depicted.
2	The Softswitch sends the INVITE to the terminating gateway providing connectivity to the end office serving TDM Party B at location 1.
3	The Softswitch sends a 100 (Trying) to the LSC serving IP Party A.
4	The terminating gateway creates an IAM that it sends to the end office serving TDM Party B at location 1.
5	The terminating gateway sends a 100 (Trying) to the originating gateway.

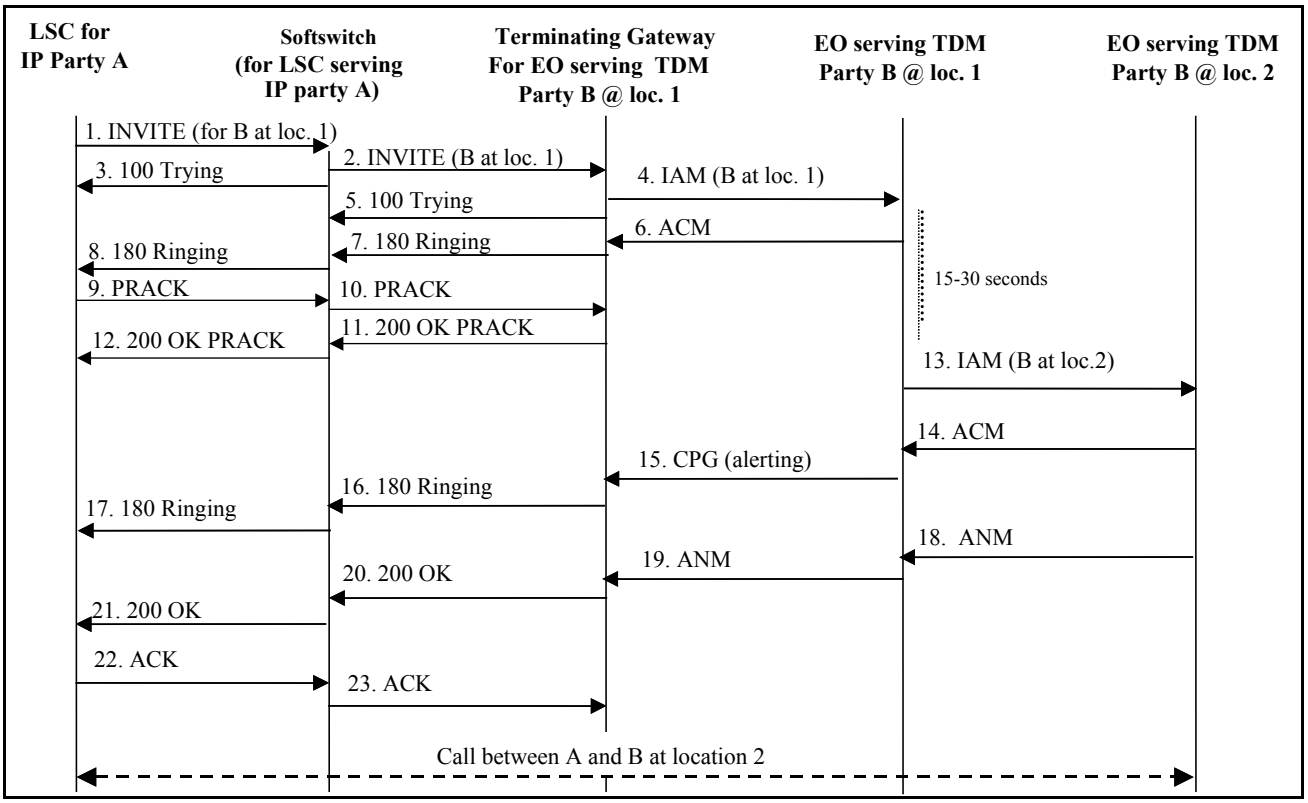


Figure 5.3.4-64. IP-to-TDM Call Forwarding (No Answer)

STEP	INSTRUCTION
6	The end office serving TDM Party B at location 1 has been notified by user B that in the event of 'no reply' the call is to be forwarded to another number (located at a different EO). Upon receiving the IAM from the terminating gateway intended for TDM Party B at location 1, the end office initiates ringing of the end instrument at location 1 and sends an ACM to the terminating gateway while waiting between 15 to 30 seconds for Party B to go off-hook. The Called Party's Status Indicator of the Backward Call Indicators is set to "01" (Subscriber free). The Optional Backward Call Indicators parameter is present and the Call Forwarding MAY Occur Indicator of the Optional Backward Call Indicators parameter is set to "1" (Call forwarding may occur).
7, 8	The terminating gateway receives the ACM, creates a 180 Ringing, and sends the 180 Ringing to the Softswitch. The Softswitch forwards the 180 Ringing to the LSC serving IP Party A. NOTE: Signaling between the LSC serving IP Party A and the IP end instrument serving IP Party A is not depicted.

STEP	INSTRUCTION
9, 10	The LSC serving IP Party A sends a PRACK to the Softswitch, which forwards the PRACK to the terminating gateway.
11, 12	The terminating gateway sends a 200 OK PRACK to the Softswitch, which forwards the 200 OK PRACK to the LSC serving IP Party A.
13	Upon no reply, the end office serving TDM Party B at location 1 modifies the IAM to reflect the call forward (e.g., adds the Original Called Number (OCN) parameter and the Redirection Information parameter, which includes the Original Redirection Reason set to "0010" (No reply), the Redirection counter, etc.) and sends the IAM on the CCS7 network to the end office serving TDM Party B at location 2.
14	The end office serving TDM Party B at location 2 creates an ACM, which it sends to the end office serving TDM Party B at location 1.
15	The end office serving TDM Party B at location 1 receives the ACM and creates a CPG with the event code set to 1 (Alerting), which it sends to the terminating gateway.
16, 17	The terminating gateway creates a 180 Ringing response and sends the 180 Ringing response to the Softswitch. The Softswitch forwards the 180 Ringing response to the LSC serving IP Party A. NOTE: Signaling between the LSC serving IP Party A and the IP end instrument serving IP Party A is not depicted.
18	The end office serving TDM Party B at location 2 sends an ANM to the end office serving TDM Party B at location 1.
19	The end office serving TDM Party B at location 1 forwards the ANM to the terminating gateway.
20, 21	The terminating gateway receives the ANM, creates a 200 (OK) response, and sends the 200 (OK) response to the Softswitch. The Softswitch forwards the 200 (OK) response to the LSC serving IP Party A. NOTE: Signaling between the LSC serving IP Party A and the IP end instrument serving IP Party A is not depicted.
22, 23	The LSC serving IP Party A sends an ACK to the Softswitch, which forwards the ACK to the terminating gateway. The signaling between the IP end instrument and the LSC serving IP Party A is not depicted.

The forwarded call is now established between IP Party A and TDM Party B at location 2.

5.3.4.19.7 Call Forward (BUSY)

A user instructs that call requests to a particular phone number be routed to a different predefined phone number in the event the end instrument is busy with another call. In the following call flow diagrams, user B has instructed that when a call request is addressed to user B's phone at location 1 but the phone is currently busy with another call then the new call request is to be forwarded to an end instrument at location 2.

Recalling UCR 2008, AS-SIP Requirement 5.3.4.10.2.5.5, the new call request will be forwarded only if the existing call has either an equal or higher precedence level than the incoming call request. If the existing call has a lower precedence than the incoming call request then the existing call will be preempted in favor of the new call request.

5.3.4.19.7.1 IP-to-IP Call Type

See UCR 2008, Section 5.3.4.13.7.1, IP-to-IP Call Type.

5.3.4.19.7.2 TDM Bridging Call Type

5.3.4.19.7.2.1 Figure 5.3.4-65 depicts the sequence of AS-SIP and ISUP messages involved in forwarding of a call request intended for TDM Party B at location 1 however the end instrument for TDM Party B at location 1 is currently busy with a call of equal or higher precedence than the incoming call request so the call request is forwarded to TDM Party B at location 2. In this scenario, the call forwarding occurs within the CCS7 network.

Call Forward

STEP	INSTRUCTION
1	The end office serving TDM Party A sends an IAM (intended for TDM Party B at location 1) to the originating gateway.
2	The originating gateway creates an INVITE, and sends the INVITE to the terminating gateway providing connectivity to the end office serving TDM Party B at location 1.
3	The terminating gateway receives the INVITE, creates an IAM (using the information found in the INVITE), and sends the IAM to the end office serving TDM Party B at location 1.
4	The terminating gateway sends a 100 (Trying) to the originating gateway.

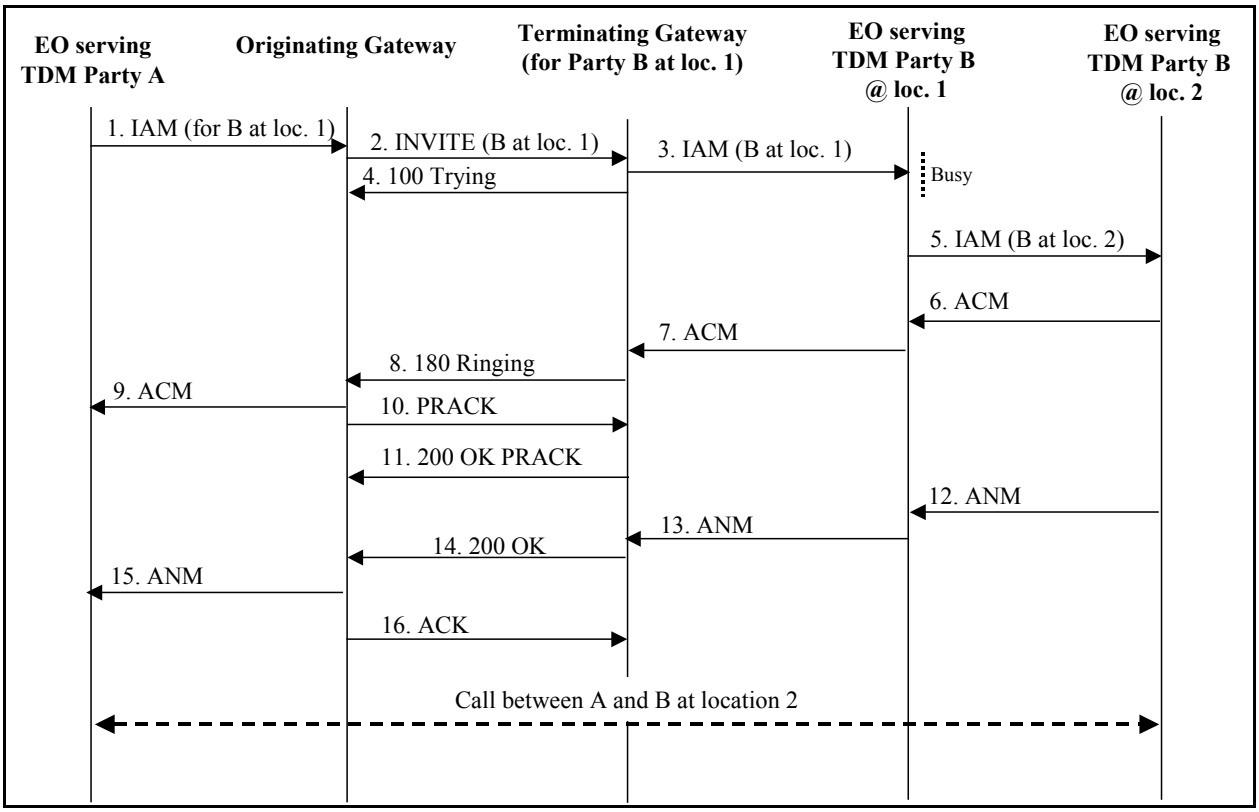


Figure5.3.4-65. TDM Bridging Call Forwarding on Busy (Call Forward Signaling Occurs within ISUP Network)

STEP	INSTRUCTION
5	The end office serving TDM Party B at location 1 has been notified by user B that in the event the end instrument is busy (with a call of equal or higher precedence than the new call request) the new call request is to be forwarded to another number (located at a different EO). Since in this case the TDM end instrument is busy with a call of equal or higher precedence, the end office serving TDM Party B at location 1 modifies the IAM to forward the call (e.g., adds the Original Called Number (OCN) parameter and the Redirection Information parameter which includes the Original Redirection Reason set to "0001" (User Busy), the Redirection counter, etc.) and sends the IAM on the CCS7 network to the end office serving TDM Party B at location 2
6	The end office serving TDM Party B at location 2 initiates ringing the TDM Party B location 2 end instrument and sends an ACM to the end office serving TDM Party B at location 1. The Notification Indicators field in the ACM is set to "1111011" (call is forwarded/deflected). The Called Party's Status Indicator of the Backward Call Indicators is set to "01" (Subscriber free).

STEP	INSTRUCTION
7	The end office serving TDM Party B at location 1 sends the ACM to the terminating gateway.
8	The terminating gateway creates a 180 (Ringing) response, and sends the 180 (Ringing) response to the originating gateway.
9	The originating gateway receives the 180 (Ringing), creates an ACM, and sends the ACM to the end office serving TDM Party A.
10	The originating gazteway sends a PRACK to the terminating gateway.
11	The terminating gateway sends a 200 OK PRACK.
12	The end office serving TDM Party B at location 2 sends an ANM to the end office serving TDM Party B at location 1.
13	The end office serving TDM Party B at location 1 forwards the ANM to the terminating gateway.
14	The terminating gateway receives the ANM, creates a 200 OK, and sends the 200 (OK) response to the originating gateway.
15	The originating gateway receives the 200 (OK), creates an ANM, and sends the ANM to the end office serving TDM Party A.
16	The originating gateway sends an ACK to the terminating gateway.

The forwarded call is now established between TDM Party A and TDM Party B at location 2.

5.3.4.19.7.3 TDM-to-IP Call Type

5.3.4.19.7.3.1 Figure 5.3.4-66 depicts the sequence of AS-SIP and ISUP messages involved in forwarding of a call request for IP Party B at location 1 to a forwarded phone number (SIP URI) corresponding to an IP end instrument for Party B at location 2 when the IP end instrument at location 1 is busy with a call of equal or higher precedence than the new call request. In the present scenario, the LSC serving IP Party B at location 1 has previously been notified that upon a "busy" the LSC is to forward calls for IP Party B at location 1 to IP Party B at location 2.

NOTE: In order to simplify the call flow diagram the 100 Trying responses have been omitted.

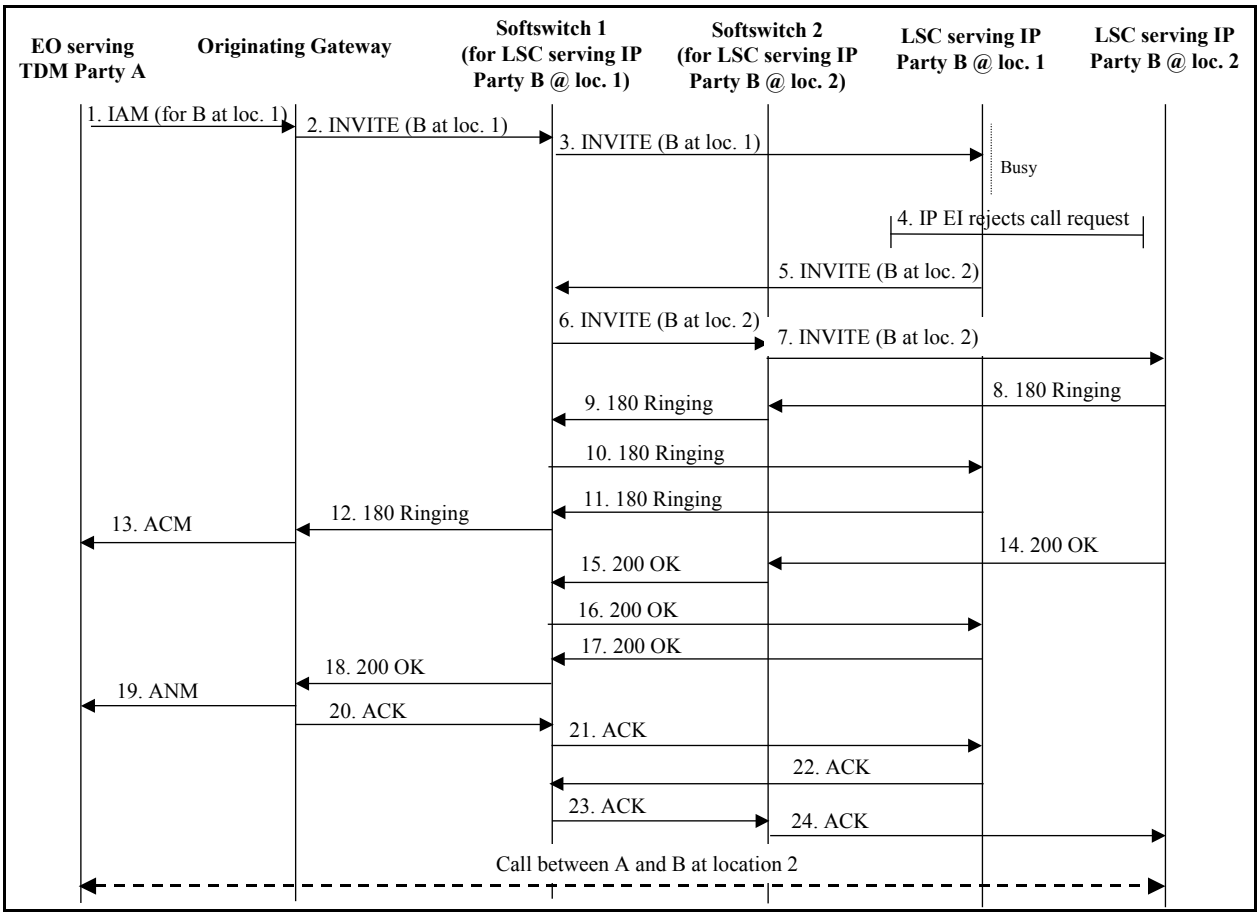


Figure 5.3.4-66. TDM-to-IP Call Forwarding on Busy

Call Forward

STEP	INSTRUCTION
1	The end office serving TDM Party A sends an IAM (intended for TDM Party B at location 1) to the originating gateway.
2	The originating gateway creates an INVITE and sends the INVITE to Softswitch 1 (which is responsible for the LSC serving IP Party B at location 1).
3	Softswitch 1 forwards the INVITE to the LSC serving IP Party B at location 1. Note: Signaling between the LSC serving IP Party B at location 1 and the IP end instrument serving IP Party B at location 1 is not depicted.

STEP	INSTRUCTION
4	The IP end instrument is busy with a call of equal or higher precedence and rejects the call. NOTE: In the case of a SIP end instrument the SIP response is a (486 busy here) and the LSC responds with an ACK.
5	The LSC serving IP Party B at location 1 rewrites the Request-URI to reflect that the call is now intended for IP Party B at location 2 and sends the INVITE to Softswitch 1.
6, 7	Softswitch 1 sends the INVITE to Softswitch 2 (which is responsible for the LSC serving IP Party B at location 2) and Softswitch 2 sends the INVITE to the LSC serving IP Party B at location 2. NOTE: The signaling between the LSC serving IP Party B at location 2 and the IP end instrument for Party B at location 2 is not depicted.
8, 9, 10, 11, 12	The LSC serving IP Party B at location 2 sends a 180 Ringing to Softswitch 2. Softswitch 2 sends the 180 Ringing to Softswitch 1. Softswitch 1 sends the 180 Ringing to the LSC serving IP Party B at location 1. The LSC serving IP Party B at location 1 sends the 180 Ringing back to Softswitch 1. Softswitch 1 sends the 180 Ringing to the originating gateway. NOTE: The signaling between the IP end instrument for Party B at location 2 to the LSC serving IP Party B at location 2 is not depicted.
13	The originating gateway creates an ACM, which it sends to the EO serving TDM Party A.
14, 15, 17, 17, 18	The LSC serving IP Party B at location 2 sends a 200 OK to Softswitch 2. Softswitch 2 sends the 200 OK to Softswitch 1. Softswitch 1 sends the 200 OK to the LSC serving IP Party B at location 1. The LSC serving IP Party B at location 1 sends the 200 OK back to Softswitch 1. Softswitch 1 sends the 200 OK to the originating gateway. NOTE: The signaling between the IP end instrument for Party B at location 2 to the LSC serving IP Party B at location 2 is not depicted.
19	The originating gateway sends an ANM to the EO serving TDM Party A.
20, 21, 22, 23, 24	The originating gateway sends an ACK to Softswitch 1. Softswitch 1 sends the ACK to the LSC serving IP Party B at location 1. The LSC serving IP Party B at location 1 sends the ACK back to Softswitch 1. Softswitch 1 sends the ACK to Softswitch 2. Softswitch 2 sends the ACK to the LSC serving IP Party B at location 2. NOTE: The signaling between the LSC serving IP Party B at location 2 and the IP end instrument serving Party B at location 2 is not depicted.

The forwarded call is now established between TDM Party A and IP Party B at location 2.

5.3.4.19.7.4 IP-to-TDM Call Type

5.3.4.19.7.4.1 Figure 5.3.4-67 depicts the sequence of AS-SIP and ISUP messages involved in forwarding of a call request for TDM Party B at location 1 to a forwarded phone number corresponding to a TDM end instrument for Party B at location 2 when the IP end instrument at location 1 is busy with a call of equal or higher precedence than the new call request. In the present scenario, the EO serving TDM Party B at location 1 has previously been notified that upon a "busy" the EO is to forward calls for TDM Party B at location 1 to the EO serving TDM Party B at location 2.

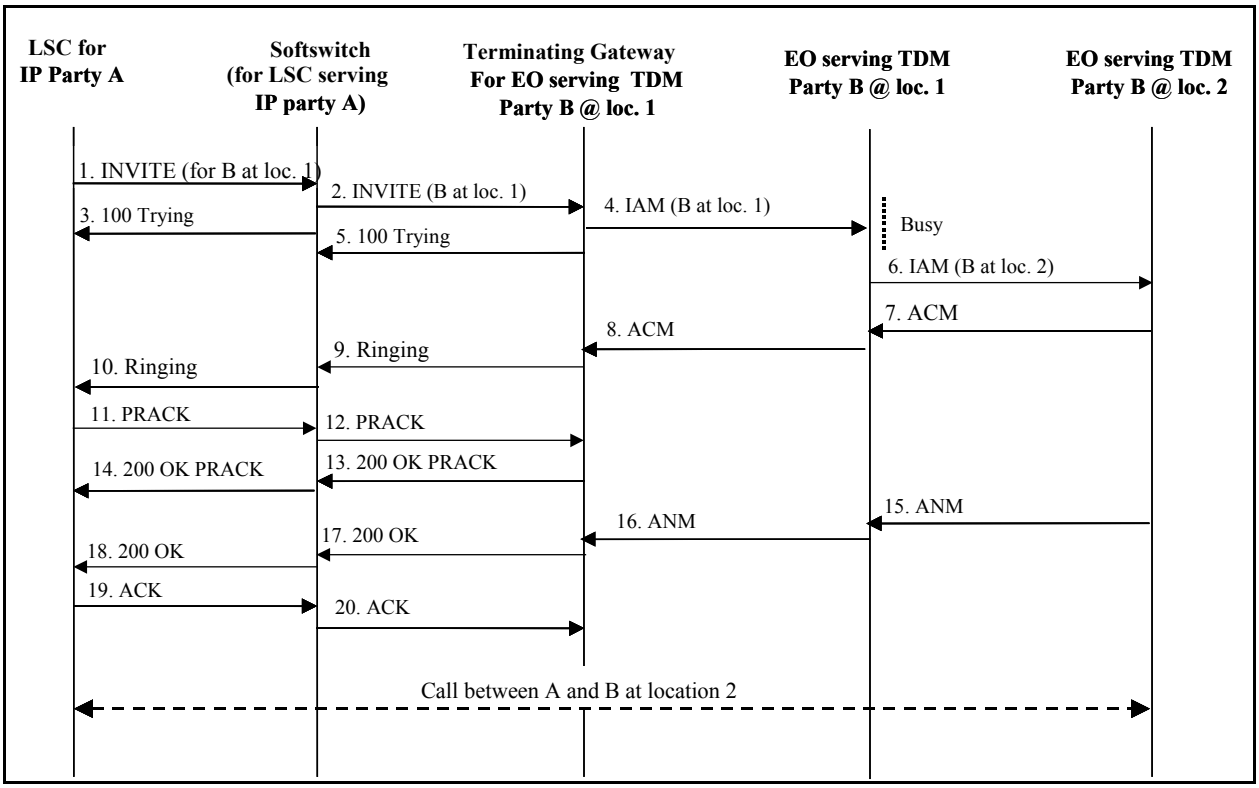


Figure 5.3.4-67. IP-to-TDM Call Forwarding on Busy

Call Forward

STEP	INSTRUCTION
1	The LSC serving IP Party A sends an INVITE to the Softswitch. NOTE: Signaling between the IP end instrument serving IP Party A and the LSC serving IP Party A is not depicted.

STEP	INSTRUCTION
2	The Softswitch sends the INVITE to the terminating gateway providing connectivity to the end office serving TDM Party B at location 1.
3	The Softswitch sends a 100 (Trying) to the LSC serving IP Party A.
4	The terminating gateway creates an IAM that it sends to the end office serving TDM Party B at location 1.
5	The terminating gateway sends a 100 (Trying) to the Softswitch.
6	The end office serving TDM Party B at location 1 has been notified by user B that in the event the end instrument is busy (with a call of equal or higher precedence than the new call request) the new call request is to be forwarded to another number (located at a different EO). Since the TDM end instrument is busy with a call of equal or higher precedence, the end office serving TDM Party B at location 1 modifies the IAM to forward the call (e.g., adds the Original Called Number (OCN) parameter and the Redirection Information parameter which includes the Original Redirection Reason set to "0001" (User Busy), the Redirection counter, etc.) and sends the IAM on the CCS7 network to the end office serving TDM Party B at location 2
7	The end office serving TDM Party B at location 2 initiates a ringing tone at the TDM end instrument at location 2 and sends an ACM to the end office serving TDM Party B at location 1. The Notification Indicators field in the ACM is set to "1111011" (call is forwarded/deflected). The Called Party's Status Indicator of the Backward Call Indicators is set to "01" (Subscriber free).
8	The end office serving TDM Party B at location 1 sends the ACM to the terminating gateway.
9, 10	The terminating gateway creates a 180 (Ringing) response and sends the 180 (Ringing) response to the Softswitch. The Softswitch forwards the 180 (Ringing) response to the LSC serving IP Party A. NOTE: Signaling between the LSC serving IP Party A and the IP end instrument serving IP Party A is not depicted.
11, 12	The LSC serving IP Party A sends a PRACK to the Softswitch, which forwards the PRACK to the terminating gateway.
13, 14	The terminating gateway sends a 200 OK to the Softswitch which forwards the 200 OK to the LSC serving IP Party A.

STEP	INSTRUCTION
15, 16	The end office serving TDM Party B at location 2 sends an ANM to the end office serving TDM Party B at location 1. The end office serving TDM Party B at location 1 forwards the ANM to the terminating gateway.
17, 18	The terminating gateway receives the ANM, creates a 200 (OK) response, and sends the 200 (OK) response to the Softswitch. The Softswitch forwards the 200 (OK) response to the LSC serving IP Party A. NOTE: Signaling between the LSC serving IP Party A and the IP end instrument serving IP Party A is not depicted.
19, 20	The LSC serving IP Party A sends an ACK to the Softswitch, which forwards the ACK to the terminating gateway. NOTE: Signaling between the IP end instrument serving IP Party A and the LSC serving IP Party A is not depicted.

The forwarded call is now established between IP Party A and TDM Party B at location 2.

5.3.4.19.8 Call Transfer

There are three actors in a given TDM transfer event, each playing one of the following roles:

- Transferred Party (or Transferee) - the party being transferred to the Transfer Target.
- Transferring Party (or Transferor) - the party initiating the transfer
- Transfer Target - the new party being introduced into a call with the Transferred Party.

NOTE: In TDM call transfer the Transferor switch stays in the path of the bearer channels between the Transferee and the Transfer Target.

5.3.4.19.8.1 Call Transfer Modes

Call transfer can be operated in two different modes: unattended (blind) and attended (consultation transfer). Blind call transfer will forward transferee to the new destination without talking to the transfer target. The alternative to this type of Call Transfer would be “Consultation

Transfer," where the call transferor will have a chance to talk to the transfer target before making the transfer.

5.3.4.19.8.2 Unattended Transfer – Call Transferor: TDM

As shown in Figure 5.3.4-68, Steps 1-15 are the standard SIP and ISUP signaling for establishing a call between the Transferee (an AS-SIP signaling appliance serving an IP EI) and the Transferor (a TDM switch serving a TDM EI).

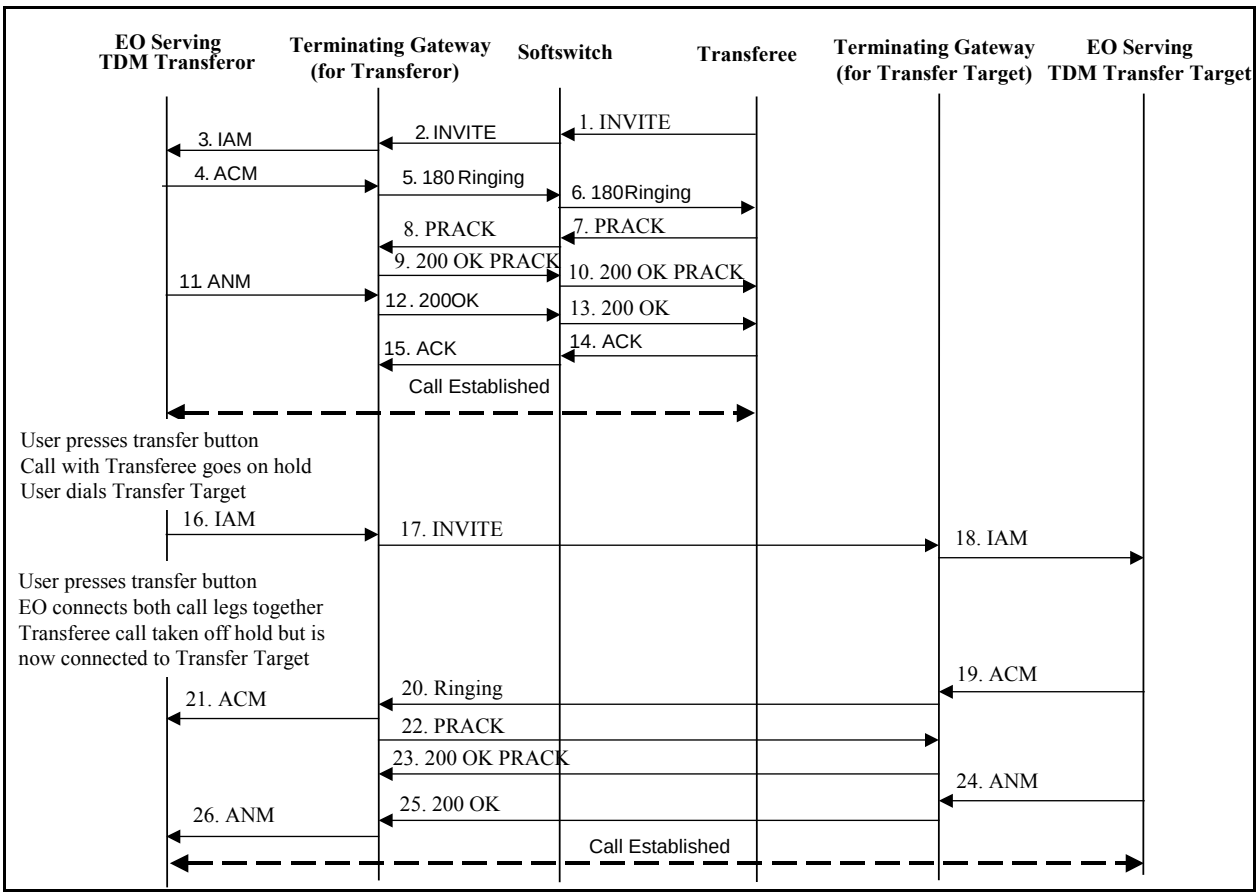


Figure 5.3.4-68. Unattended Call Transfer (Transferor –TDM)

The call Transferor decides to transfer this call to another TDM phone served by a TDM end office. The Transferor user presses the transfer button (or equivalent) thereby signaling the local EO to place the call with the Transferee on hold while the Transferor user dials the Transfer Target. The Transferor then initiates a call with the Transfer Target (Steps 16, 17, 18).

The Transferor user again presses the transfer button (or equivalent) and the local EO switch connects the two (2) call legs and takes the Transferee off call hold.

Steps 19-26 detail the standard SIP and ISUP signaling for completing the establishment of the call between the Transferor switch and Transfer Target however the bearer traffic from the Transfer Target is being forwarded by the Transferor switch to the Transferee and the bearer traffic from the Transferee is being forwarded by the Transferor switch to the Transfer Target.

5.3.4.19.8.3 Attended Transfer Call Transferor: TDM

As shown in Figure 5.3.4-69, the Transferor establishes a standard TDM-IP call with the Transferee in Steps 1-11.

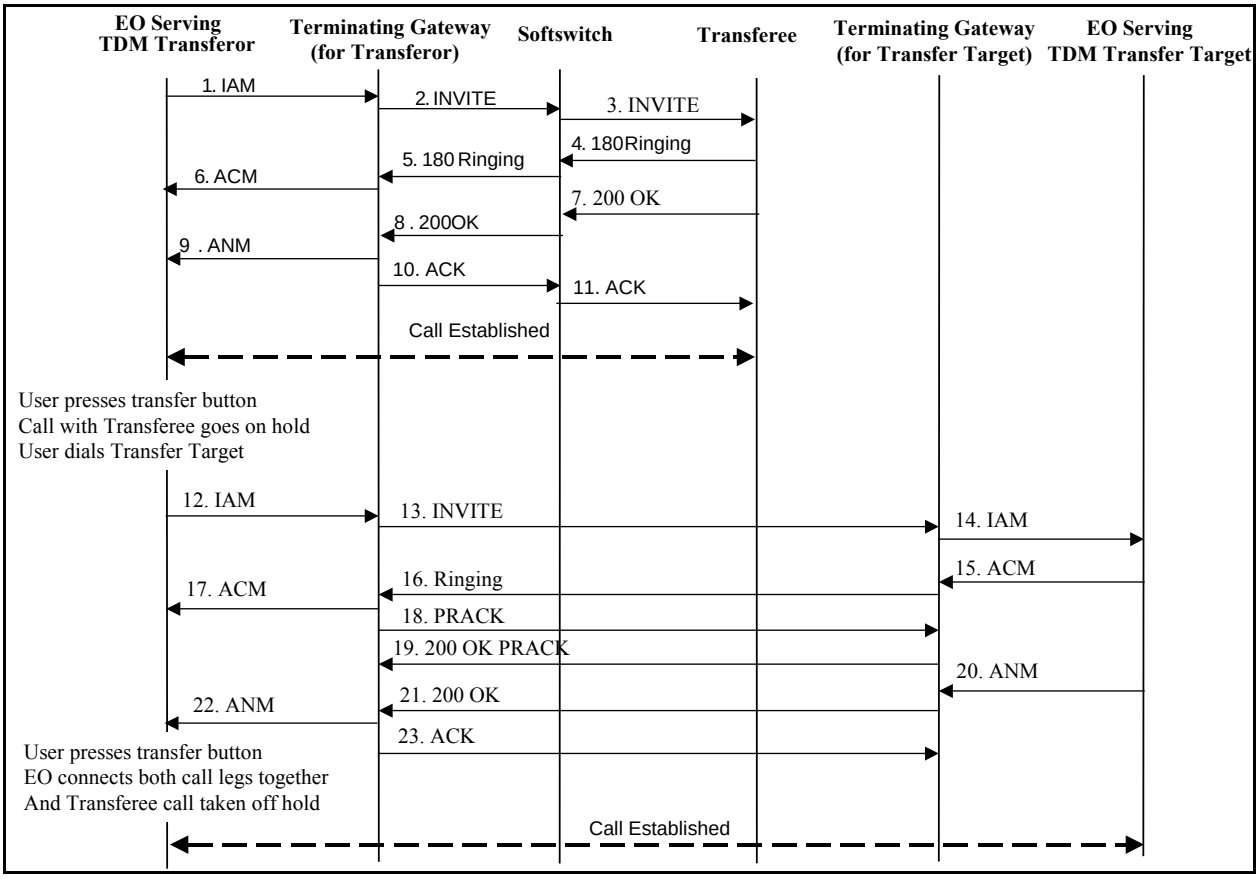


Figure 5.3.4-69. Attended Call Transfer Transferor – TDM

The Transferor user then presses the Transfer button (or equivalent) which places the call between the Transferor and Transferee on hold after which the Transferor user dials the Transfer Target.

The Transferor establishes a standard TDM bridging call with the Transfer Target in Steps 12-23.

The Transferor user again presses the Transfer button (or equivalent) and the local EO switch connects the two (2) call legs and takes the Transferee off call hold. At this point, the bearer traffic from the Transfer Target is being forwarded by the Transferor switch to the Transferee and the bearer traffic from the Transferee is being forwarded by the Transferor switch to the Transfer Target.

THIS PAGE INTENTIONALLY LEFT BLANK

TABLE OF CONTENTS

SECTION **PAGE**

5.3.5 IPv6 Requirements....1165
5.3.5.1 Introduction....1165
5.3.5.2 Characteristics....1166
5.3.5.3 System Requirements....1168
5.3.5.3.1 MTU....1168
5.3.5.3.2 Flow Label....1169
5.3.5.3.3 Address....1169
5.3.5.3.4 DHCP....1170
5.3.5.3.5 Neighbor Discovery....1171
5.3.5.3.5.1 Redirect Mesages....1172
5.3.5.3.5.2 Router Advertisements....1172
5.3.5.3.6 Stateless Address Autoconfiguration and Manual Address Assignment....1173
5.3.5.3.7 Internet Control Message Protocol (ICMP)....1174
5.3.5.3.8 Routing Functions....1175
5.3.5.3.9 IP Security....1176
5.3.5.3.10 Network Management (NM)....1181
5.3.5.3.11 Traffic Engineering....1182
5.3.5.3.12 IP Version Negotiation....1183
5.3.5.3.13 AS-SIP IPv6 Unique Requirements....1183
5.3.5.3.14 Miscellaneous Requirements....1185
5.3.5.4 Mapping of RFCs to DoD IPv6 Profile Categories....1186

5.3.5 IPv6 Requirements

Section 5.3.5 describes the IPv6 requirements for Sensitive But Unclassified (SBU) Unified Capabilities subsets provided by the DSN, DISN Video Services (DVS), circuit emulation, and/or short, latency sensitive command and control (C2) messages. This section addresses a wired network, but does not address wireless networks or mobile environments. Future revisions of this section may address these voids based on the customer and industry feedback.

Beginning on 1 January 2009, no DSN VoIP Lineside system that is IPv4 only will be accepted for APL testing. All systems submitted for testing must be IPv6 capable. Dual Stack solutions are preferred and tunneling solutions are unacceptable. The definitions of IPv6 capable and IPv6 enabled products are provided in UCR 2008 Section 4.3.1.3, Internet protocol Version 6 Requirement.

Exception: Products participating in the DISN UC Spiral One deployment as IPv4 E2E solution will be given APL status at the end of their spiral testing with at least one other vendor and will then be required to complete all IPv6 capable testing requirements at JITC by 1 April 2010 and will be expected to participate in the IPv6 DISN UC Spiral Two deployment.

5.3.5.1 Introduction

The terms used within UCR 2008 are defined in Appendix A, Definitions, Abbreviations and Acronyms, and References. The requirements defined in UCR 2008 Section 5.3.2, Assured Services Requirements, are associated with the external interfaces of the UC products or Network Appliances (NAs). For the purpose of defining each requirement, the terms UC products and NAs are shortened to 'system'. The external interfaces for a NA are generally considered to be interfaces that connect to and interact with the ASLAN or the non-ASLAN. The primary interfaces associated with the IPv6 requirements are the signaling, AS-SIP, and bearer, Secure Real-Time Transport Protocol (SRTP), interfaces. In addition, any interfaces that transmit packets external to the enclave (i.e., to the WAN) shall meet the IPv6 requirements. However, some interfaces may remain internal to the enclave, although they are external to the UC product, and may remain Internet Protocol version 4 (IPv4) only. For example, if the EI can send and receive signaling and bearer packets using IPv6, it is acceptable for it to send and receive IPv4 configuration information from the LSC. Internal interfaces shall be evaluated for information assurance (IA), but will not be evaluated for interoperability as they are considered internal to the UC product.

The DoD memorandum, subject: Department of Defense Information Technology Standards Registry Baseline Release 07-3.0, dated Nov 6, 2007, approved "DoD IPv6 Standard Profiles For IPv6 Capable Products- Supplemental Guidance" Version 2.0, dated 01 August 2007.

The UCR 2008, IPv6 requirements are based on the DoD IPv6 Profile version 2.0, with four exceptions as noted below:

1. If the DoD IPv6 Profile version 3.0 [Ref: DoD memorandum, sub: Department of Defense Information Technology Standards Registry Baseline Release 08-2.0, dated July 14, 2008] has identified an IA risk that must be mitigated with a new requirement.

2. If the DoD IPv6 Profile 3.0 has deleted or relieved requirements.

3. If the DoD IPv6 Profile 3.0 has identified an IO issue that needs to be corrected.

4. If there is an UCR 2008 unique requirement that is levied on the UCR system and is not included in the DoD IPv6 Profile version 2.0.

For some cases DoD IPv6 Profile version 3.0 requirements differ from DoD IPv6 Profile 2.0 where RFCs have been deprecated. For example, in DoD IPv6 Profile version 3.0, RFC 2462 is replaced by RFC 4862. In the text of UCR 2008, this case is denoted by: "RFC 2462 and RFC 4862 (FY2010)." This is to be interpreted to mean that:

1. Under UCR 2008 the requirement for RFC 4862 is optional.

2. Under UCR 2010 the requirement for RFC 4862 will be mandatory.

5.3.5.2 Characteristics

The system requirements specified in UCR 2008, Section 5.3.2, Assured Services Requirement, are the minimum set of requirements necessary for the system to be IPv6 capable for VVoIP. An implementer may choose to specify additional IPv6 requirements based on their non-VVoIP or unique VVoIP requirements. A vendor may choose to implement additional IPv6 functions based on their commercial market. This section focuses on the deltas between an IPv6 implementation and an IPv4 implementation, and does not address consistencies or inconsistencies between IPv4 and IPv6. The requirements are Fiscal Year (FY) 2008 requirements unless specifically stated that the requirement applies to a different time frame. In addition, requirements may be designated as "Required," "Conditional, or "Objective" requirements, the terms are defined in UCR 2008, Appendix A, Definitions, Abbreviations and Acronyms, and References. In addition, several requirements are levied explicitly on EI that are classified as softphones (EI [Softphone only]) due to the dual use of the appliance for data and voice applications. Unless the requirement is levied on all EIs, it not a requirement associated with voice and is intended to apply to the data applications that reside on the softphone. All EIs IPv6 requirements are the same and for the purposes of this section of UCR 2008, the term EI

includes secure EIs. Finally, whenever a reference to a specific RFC appears in an UCR 2008 requirement, the specific language of the UCR 2008 requirement and its subtended requirements should be understood within the context of the RFC. The acronyms used for designating the appliances that a requirement pertains to are shown in Table 5.3.5-1, Mapping of UC products or Functions to DoD IPv6 Profile Categories.

Table 5.3.5-1. Mapping of UC Products or Functions to DoD IPv6 Profile Categories

UC PRODUCT OR FUNCTION	APPLIANCE	DOD IPV6 STANDARD PROFILES CATEGORY
MFSS	Multifunction Softswitch	Simple Server (SS)
LSC	Local Session Controller	Simple Server (SS)
MG	Media Gateway	Network Appliance (NA)
EBC	Edge Boundary Controller	IA Device
EI	End Instrument	Network Appliance (NA)
LS	LAN Switch	Layer 3 Switch (LS)
R	Router	Router (R)
MFS/Tandem Switch	Multifunction Switch	Simple Server (SS)
EOS	End office Switch	Simple Server (SS)
SOME	Small End Office	Simple Server (SS)
DVX	Deployed Voice Exchange	Simple Server (SS)
PBX1	Private Branch Exchange 1	Simple Server (SS)
PBX2	Private Branch Exchange 2	Simple Server (SS)
CPE	Customer Premise Equipment	Network Appliance (NA)
NE	Network Element	Network Appliance (NA)
EC	Echo Canceller	Network Appliance (NA)
IAS	Integrated Access Switch	Network Appliance (NA)
CB	Conference Bridge (external)	Network Appliance (NA)
MCU	Multipoint Control Unit	Network Appliance (NA)
VTU	Video Telephony Unit	Network Appliance (NA)
H.323/H.320 GW	H.323/H.320 Gateway	Network Appliance (NA)
NOTE: There are differences between this UCR and the DoD IPv6 Standard Profiles For IPv6 Capable Products Version 2.0. Where those differences occur, this UCR takes precedence over the DoD IPv6 Standards Profile Version 2.0. DoD IPv6 Standards Profile Version 2.0 categories are included to assist the reader in mapping between the DoD IPv6 Standards Profile Version 2.0 and this UCR.		

NOTE: Legacy TDM based devices (e.g., MFS, PBX1, CPE etc.) are mapped in the requirements section based on their equivalent IPv6 Profile Category. All IP centric appliances (MFSS, LSC etc.) are mapped based on their function category. Even though an EI is associated with the DoD IPv6 Standard Profile network appliance, it is listed as individually as an EI on a requirement basis to avoid confusion.

The acronyms used within the subsequent requirements paragraphs reflect those used in both columns 1 and 3 in Table 5.3.5-1.

5.3.5.3 System Requirements

1. **[Required: SS, NA, EBC, R, LS, – Conditional: EI]** The system shall support dual IPv4 and IPv6 stacks as described in RFC 4213.

   NOTE: The tunnel requirements are only associated with appliances that provide IP routing functions (e.g., routers). The primary intent of these requirements is to (1) require dual stacks on all UC appliances and (2) allow dual stacks and tunneling on routers.

   [Conditional: EI FY 08-12] The EIs are allowed to use alternative mechanisms (e.g., translation and tunneling) between FY2008 and FY2012 as long as performance, interoperability, and IA requirements are met.

   1.1 **[Conditional: R, LS]** If the system supports routing functions, the system shall support the manual tunnel requirements as described in RFC 4213.

2. **[Required: SS, NA, EBC, R, LS, EI]** The system shall support the IPv6 format as described in RFC 2460 and updated by RFC 5095.

3. **[Required: SS, EBC, R, LS, EI]** The system shall support the transmission of IPv6 packets over Ethernet networks using the frame format defined in RFC 2464.

   NOTE: This requirement does not mandate that the remaining sections of RFC 2464 have to be implemented.

5.3.5.3.1 MTU

4. **[Required: EBC, R, LS, EI (Softphone only)]** The system shall support Path Maximum Transmission Unit (MTU) Discovery (RFC 1981).

5. **[Required: SS, NA, EBC, R, LS, EI]** The system shall support a minimum MTU of 1280 bytes (RFC 2460 and updated by RFC 5095).

   NOTE: Guidance on MTU requirements and settings can be found in UCR 2008, Section 5.3.3.10.1.2 Layer 2- Data Link Layer.

6. **[Conditional: SS, NA, EBC, R, LS, EI]** If Path MTU Discovery is used and a "Packet Too Big" message is received requesting a next-hop MTU that is less than the IPv6 minimum link MTU, the system shall ignore the request for the smaller MTU and shall include a fragment header in the packet.

   NOTE: This is to mitigate an attack where the path MTU is adequate, but the Packet Too Big messages are used to make the packet so small it is inefficient.

5.3.5.3.2 Flow Label

7. **[Required: SS, NA, EBC, EI]** The system shall not use the Flow Label field as described in RFC 2460.

   7.1. **[Required: SS, NA, EBC, EI]** The system shall be capable of setting the Flow Label field to zero when originating a packet.

   7.2. **[Required: SS, NA, EBC]** The system shall not modify the Flow Label field when forwarding packets.

   7.3. **[Required: SS, NA, EBC, EI]** The system shall be capable of ignoring the Flow Label field when receiving packets.

5.3.5.3.3 Address

8. **[Required: SS, NA, EBC, R, LS, EI]** The system shall support the IPv6 Addressing Architecture as described in RFC 4291.

   NOTE: The use of "IPv4 Mapped" addresses "on-the-wire" is discouraged due to security risks raised by inherent ambiguities.

9. **[Required: SS, NA, EBC, R, LS, EI]** The system shall support the IPv6 Scoped Address Architecture as described in RFC 4007.

   9.1. **[Conditional: SS, NA, EBC, R, LS, EI]** If a scoped address (RFC 4007) is used, the system shall use a scope index value of zero (0) when the default zone is intended.

   9.2. **[Conditional: SS, NA, EBC, R, LS, EI]** If a scoped address (RFC 4007) is used, the system shall use the syntax of <address>%<zone_id>/<prefix_length> when specifying an IPv6 nonglobal address.

NOTE: Address is the IPv6 address and % and / are delimiters. If the zone id is zero (0) or default, the % and zone id may be omitted.

5.3.5.3.4 DHCP

10. **[Conditional: SS, NA EI, R, LS]** If Dynamic Host Configuration Protocol (DHCP) is supported within an IPv6 system, it shall be implemented in accordance with the DHCP for IPv6 (DHCPv6) as described in RFC 3315.

NOTE 1: UCR 2008, Section 5.4, Information Assurance, requires that the voice or video DHCP servers are not to be located on the same physical appliance as the voice or video LAN switches and routers in accordance with the Security Technical Implementation Guides (STIGs). Also, the VoIP STIG requires (in VoIP 0082) separate DHCP servers for (1) the phone system in the phone VLAN(s) and (2) the data devices (PCs) in the data VLAN(s).

NOTE 2: There is no requirement that separate DHCP servers be used for IPv4 and for IPv6.

10.1. **[Conditional: SS, NA, EI]** If the system is a DHCPv6 client, the system shall discard any messages that contain options that are not allowed to appear in the received message type (e.g., an Identity Association option in an Information-Request message).

10.2. **[Required: EI]** The system shall support DHCPv6 as described in RFC 3315.
NOTE: The following subtended requirements are predicated upon an implementation of DHCPv6 for the end instrument. It is not expected that other UC appliances will use DHCPv6.

10.2.1. **[Required: EI Conditional: SS, NA]** If the system is a DHCPv6 client, and the first Retransmission Timeout has elapsed since the client sent the Solicit message and the client has received an Advertise message(s), but the Advertise message(s) does not have a preference value of 255, the client shall continue with a client-initiated message exchange by sending a Request message.

10.2.2. **[Required: EI Conditional: SS, NA]** If the system is a DHCPv6 client and the DHCPv6 message exchange fails, it shall restart the reconfiguration process after receiving user input, system restart, attachment to a new link, a system configurable timer, or a user defined external event occurs.

NOTE: The intent is to ensure that the DHCP client continues to restart the configuration process periodically until it succeeds.

10.2.3. **[Required: EI Conditional: SS, NA]** If the system is a DHCPv6 client and it sends an Information-Request message, it shall include a Client Identifier option to allow it to be authenticated to the DHCPv6 server.

10.2.4. **[Required: EI Conditional: SS, NA]** If the system is a DHCPv6 client, it shall perform duplicate address detection upon receipt of an address from the DHCPv6 server prior to transmitting packets using that address for itself.

10.2.5. **[Required: EI Conditional: SS, NA]** If the system is a DHCPv6 client, it shall log all reconfigure events.

10.3. **[Conditional: SS, NA, EI, R, LS]** If the system supports DHCPv6 and uses authentication, it shall discard unauthenticated DHCPv6 messages from UC systems and log the event.

NOTE: This requirement assumes authentication is used as described in RFC 3118 (and extended in RFC 3315) but does not require authentication.

5.3.5.3.5 Neighbor Discovery

11. **[Required: SS, NA, EBC, R, LS, EI]** The system shall support Neighbor Discovery for IPv6 as described in RFC 2461 and RFC 4861 (FY2010).

11.1. **[Required: SS, NA, EBC, R, LS]** The system shall not set the override flag bit in the neighbor advertisement message for solicited advertisements for anycast addresses or solicited proxy advertisements.

11.2. **[Required: SS, NA, EBC, R, LS]** The system shall set the override flag bit in the neighbor advertisement message to “1” if the message is not an anycast address or a unicast address for which the system is providing proxy service.

11.3. **[Conditional: SS, NA, EBC, R, LS, EI]** If a valid neighbor advertisement is received by the system and the system neighbor cache does not contain the target’s entry, the advertisement shall be silently discarded.

11.4. **[Conditional: SS, NA, EBC, R, LS, EI]** If a valid neighbor advertisement is received by the system and the system neighbor cache entry is in the INCOMPLETE

state when the advertisement is received and the link layer has addresses and no target link-layer option is included, the system shall silently discard the received advertisement.

11.5. **[Conditional: SS, NA, EBC, R, LS, EI]** If address resolution fails on a neighboring address, the entry shall be deleted from the system's neighbor cache.

5.3.5.3.5.1 Redirect Mesages

11.6. **[Required: SS, NA, EBC, EI]** The system shall support the ability to configure the system to ignore redirect messages.

11.7. **[Required: SS, NA, EBC, R, LS, EI]** The system shall only accept redirect messages from the same router as is currently being used for that destination.

NOTE: The intent of this requirement is that if a node is sending its packets destined for location A to router X, that it can only accept a redirect message from router X for packets destined for location A to be sent to router Z.

11.7.1. **[Conditional: SS, NA, EBC, R, LS, EI]** If redirect messages are allowed, the system shall update its destination cache in accordance with the validated redirect message.

11.7.2. **[Conditional: SS, NA, EBC, R, LS, EI]** If the valid redirect message is allowed and no entry exists in the destination cache, the system shall create an entry.

5.3.5.3.5.2 Router Advertisements

11.8. **[Required: R Conditional: LS, EBC]** If the system supports routing functions, the system shall inspect valid router advertisements sent by other routers and verify that the routers are advertising consistent information on a link and shall log any inconsistent router advertisements.

11.8.1. **[Required: SS, NA, EBC, EI]** The system shall prefer routers that are reachable over routers whose reachability is suspect or unknown.

11.8.2 Reserved.

11.9. **[Required: R] [Conditional: LS, EBC]** If the system supports routing functions, the system shall include the MTU value in the router advertisement message for all links in accordance with RFC 2461 and RFC 4861 (FY2010).

5.3.5.3.6 Stateless Address Autoconfiguration and Manual Address Assignment

12. **[Required: R, LS, EI (Softphone only)] [Conditional: SS, NA, EBC, EI]** If the system supports stateless IP address autoconfiguration, the system shall support IPv6 Stateless Address Auto-Configuration (SLAAC) for interfaces supporting UC functions in accordance with RFC 2462 and RFC 4862 (FY2010).

12.1. **[Required: SS, NA, EBC, R, LS, EI]** The system shall have a configurable parameter that allows the "managed address configuration" flag and the "other stateful configuration" flag to always be set and not perform stateless autoconfiguration.

NOTE: The objective of this requirement is to prevent a system from using stateless auto configuration.

12.2. **[Required: SS, NA, EBC, R, LS, EI]** The system shall support manual assignment of IPv6 addresses.

12.3. **[Required: EI]** The system shall support stateful autoconfiguration (i.e., ManagedFlag=TRUE).

NOTE: This requirement is associated with the earlier requirement for the EI to support DHCPv6.

12.3.1. **[Required: R] [Conditional: LS, EBC]** If the system provides routing functions, the system shall default to using the "managed address configuration" flag and the "other stateful flag" set to TRUE in their router advertisements when stateful autoconfiguration is implemented.

12.4. **[Conditional: EI]** If the system supports a subtended appliance behind it, the system shall ensure that the IP address assignment process of the subtended appliance is transparent to the UC components of the system and does not cause the system to attempt to change its IP address.

NOTE: An example is a PC that is connected to the LAN through the hub or switch interface on a phone. The address assignment process of the PC should be

transparent to the EI and should not cause the phone to attempt to change its IP address.

12.5. **[Conditional: SS, NA, EBC, EI]** If the system supports IPv6 SLAAC, the system shall have a configurable parameter that allows the function to be enabled and disabled.

12.6. **[Conditional: EI (Softphones only)]** If the system supports SLAAC and security constraints prohibit the use of hardware identifiers as part of interface addresses generated using SLAAC, IPsec capable systems shall support privacy extensions for stateless address autoconfiguration as defined in RFC 3041 and RFC 4941 (FY2010).

12.7. **[Required: R, LS, EI (Softphone only)] [Conditional: SS, NA, EBC, EI]** If the system supports stateless IP address autoconfiguration, the system shall support a configurable parameter to enable or disable manual configuration of the site-local and Global addresses (i.e., disable the "Creation of Global and Site-Local Addresses" as described in Section 5.5 of RFC 2462).

12.8 **[Required: SS, NA, EBC, R, LS, EI]** All IPv6 nodes shall support link-local address configuration, and the Duplicate Address Detection (DAD) shall not be disabled in accordance with RFC 2462 and RFC 4862 (FY2010).

13. Reserved.

5.3.5.3.7 Internet Control Message Protocol (ICMP)

14. **[Required: SS, NA, EBC, R, LS, EI]** The system shall support the Internet Control Message Protocol for IPv6 (ICMPv6) as described in RFC 4443.

14.1. **[Required: SS, NA, EBC, R, LS, EI]** The system shall have a configurable rate limiting parameter for rate limiting the forwarding of ICMP messages.

14.2. **[Required: SS, NA, EBC, R, LS]** The system shall support the capability to enable or disable the ability of the system to generate a Destination Unreachable message in response to a packet that cannot be delivered to its destination for reasons other than congestion.

14.3. **[Required: SS, NA, EBC, R, LS, EI]** The system shall support the enabling or disabling of the ability to send an Echo Reply message in response to an Echo Request message sent to an IPv6 multicast or anycast address.

NOTE: The number of responses may be traffic conditioned to limit the effect of a denial of service attack.

14.4. **[Required: SS, NA, EBC, R, LS, EI]** The system shall validate ICMPv6 messages, using the information contained in the payload, prior to acting on them.

5.3.5.3.8 Routing Functions

15. **[Required: R] [Conditional: LS]** If the system supports routing functions, the system shall support the Open Shortest Path First (OSPF) for IPv6 as described in RFC 2740.

15.1. **[Required: R] [Conditional: LS]** If the system supports routing functions, the system shall support securing OSPF with Internet Protocol Security (IPSec) as described for other IPSec instances in UCR 2008, Section 5.4, Information Assurance.

15.2. **[Required: R] [Conditional: LS]** If the system supports routing functions, the system shall support router-to-router integrity using the IP Authentication Header with HMAC-SHA1-128 as described in RFC 4302.

16 **[Conditional: R]** If the system acts as a CE router, the system shall support the use of Border Gateway Protocol (BGP) as described in RFC 1772 and 4271.

16.1 **[Conditional: R]** If the system acts as a customer edge router, the system shall support the use of BGP-4 multiprotocol extensions for IPv6 Inter-Domain routing (RFC 2545).

NOTE: The requirement to support BGP-4 is in UCR 2008, Section 5.3.3, Wide Area Network General System Requirements.

17. [**Conditional: R, LS]** If the system acts as a CE router, the system shall support multiprotocol extensions for BGP-4 RFC 2858 and RFC 4760 (FY2010).

NOTE: The requirement to support BGP-4 is in UCR 2008, Section 5.3.3, Wide Area Network General System Requirements.

18. [**Conditional: R]** If the system acts as a CE router, the system shall support the Generic Routing Encapsulation (GRE) as described in RFC 2784.

19. [**Conditional: R]** If the system acts as a CE router, the system shall support the Generic Packet Tunneling in IPv6 Specification as described in RFC 2473.

    NOTE: Tunneling is provided for data applications and is not needed as part of the VVoIP architecture.

20. **[Required: R, EI (Softphone Only)] [Conditional: LS]** If the system supports routing functions, the system shall support the Multicast Listener Discovery (MLD) process as described in RFC 2710 and extended in RFC 3810.

    NOTE: The FY 2008 VVoIP design does not utilize multicast, but routers supporting VVoIP also support data applications that may utilize multicast. A softphone will have non-routing functions that require MLDv2.

21. **[Required: SS, NA, EBC, EI, LS]** The system shall support MLD as described in RFC 2710.

    NOTE: This requirement was added in order to ensure that Neighbor Discovery multicast requirements are met. Routers are not included in this requirement since they have to meet RFC 2710 in the preceding requirement.

5.3.5.3.9 IP Security

22. **[Required: R, EI (Softphone Only)] [Conditional: SS, NA, EBC, LS, EI]** If the system uses IPSec, the system shall support the Security Architecture for the IP RFC 2401 and RFC 4301 (FY2010).

    In FY2008, RFC 2401 (and its related RFCs) is the Threshold requirement as described in UCR 2008, Section 5.4, Information Assurance. In addition, the interfaces required to use IPSec are defined in UCR 2008, Section 5.4, Information Assurance.

    22.1. **[Required: R, EI (Softphone Only)] [Conditional: SS, NA, EBC, LS, EI]** If RFC 4301 is supported, the system shall support binding of a security association (SA) with a particular context.

    22.2. **[Required: R, EI (Softphone Only)] [Conditional: SS, NA, EBC, LS, EI]** If RFC 4301 is supported, the system shall be capable of disabling the BYPASS IPSec **processing** choice.

NOTE: The intent of this requirement is to ensure that no packets are transmitted unless they are protected by IPSec.

22.3. **[Required: R, EI (Softphone Only)] [Conditional: SS, NA, EBC, LS, EI]** If RFC 4301 is supported, the system shall not support the mixing of IPv4 and IPv6 in a security association.

22.4. **[Required: R, EI (Softphone Only)] [Conditional: SS, NA, EBC, LS, EI]** If RFC 4301 is supported, the system's security association database (SAD) cache shall have a method to uniquely identify a SAD entry. NOTE: The concern is that a single SAD **entry** will be associated with multiple security associations. RFC 4301, Section 4.4.2, describes a scenario where this could occur.

22.5. **[Required: R, EI (Softphone Only)] [Conditional: SS, NA, EBC, LS, EI]** If RFC 4301 is supported, the system shall be capable of correlating the Differentiated **Services** Code Point (DSCP) for a VVoIP stream to the security association in accordance with UCR 2008, Section 5.3.2, Assured Services Requirements and Section 5.3.3, Network Infrastructure End-to-End Performance Requirements, plain text DSCP plan.

22.6. **[Required: R, EI (Softphone Only)] [Conditional: SS, NA, EBC, LS, EI]** If RFC **4301** is supported, the system shall implement IPSec to operate with both integrity and confidentiality.

22.7. **[Required: R, EI (Softphone Only)] [Conditional: SS, NA, EBC, LS, EI]** If RFC 4301 is supported, the system shall be capable of enabling and disabling the ability of the **system** to send an ICMP message informing the sender that an outbound packet was discarded.

22.7.1. **[Required: R, EI (Softphone Only)] [Conditional: SS, NA, EBC, LS, EI]** If an ICMP outbound packet message is allowed, the system shall be capable of rate **limiting** the transmission of ICMP responses.

22.8. **[Required: R, EI (Softphone Only)] [Conditional: SS, NA, EBC, LS, EI**] If RFC 4301 is supported, the system shall be capable of enabling or disabling the **propagation** of the Explicit Congestion Notification (ECN) bits.

22.9. **[Required: R, EI (Softphone Only)] [Conditional: SS, NA, EBC, LS, EI]** If RFC 4301 is supported, the system's Security Policy Database (SPD) shall have a nominal, final entry that discards anything unmatched.

22.10. **[Required: R, EI (Softphone Only)] [Conditional: SS, NA, EBC, LS, EI]** If RFC 4301 is supported, and the system receives a packet that does not match any SPD cache entries and the system determines it should be discarded, the system shall log the event and include the date/time, Security Parameter Index (SPI) if available, IPSec protocol if available, source and destination of the packet, and any other selector values of the packet.

22.11. **[Required: R, EI (Softphone Only)] [Conditional: SS, NA, EBC, LS, EI]** If RFC 4301 is supported, the system should include a management control to allow an **administrator** to enable or disable the ability of the system to send an Internet Key Exchange (IKE) notification of an INVALID_SELECTORS.

22.12. **[Required: R, EI (Softphone Only)] [Conditional: SS, NA, EBC, LS, EI]** If RFC 4301 is supported, the system shall support the Encapsulating Security Payload (ESP) Protocol in accordance with RFC 4303.

22.12.1. **[Required: R, EI (Softphone Only)] [Conditional: SS, NA, EBC, LS, EI]** If RFC 4303 is supported, the system shall be capable of enabling anti-replay.

22.12.2. **[Required: R, EI (Softphone Only)] [Conditional: SS, NA, EBC, LS, EI]** If RFC 4303 is supported, the system shall check as its first check after a packet has been matched to its SA whether the packet contains a Sequence Number that does not duplicate the Sequence Number of any other packet received during the life of the security association.

22.13 **[Required: R, EI (Softphone Only)] [Conditional: SS, NA, EBC, LS, EI]** If RFC 4301 is supported, the system shall support the cryptographic algorithms as defined in RFC 4308 for Suite Virtual Private Network (VPN)-B.

22.13.1. **[Required: R, EI (Softphone Only)] [Conditional: SS, NA, EBC, LS, EI]** If RFC 4301 is supported, the system shall support the use of AES-CBC with 128-bits keys for encryption.

22.13.2. **[Required: R, EI (Softphone Only)] [Conditional: SS, NA, EBC, LS, EI]** If RFC 4301 is supported, the system shall support the use of HMAC-SHA1-96 for (Threshold) and AES-XCBC-MAC-96 (FY2010).

22.14. **[Required: R, EI (Softphone Only)] [Conditional: SS, NA, EBC, LS, EI]** If RFC 4301 is supported, the system shall support IKE Version 1 (IKEv1) (Threshold) as defined in RFC 2409, and IKE Version 2 (IKEv2) (FY2010) as defined in RFC 4306.

NOTE: Internet Key Exchange version 1 (IKEv1) requirements are found in UCR 2008, Section 5.4, Information Assurance.

22.14.1. **[Conditional: SS, NA, EBC, R, LS, EI]** If the system supports IKEv2, it shall be capable of configuring the maximum User Datagram Protocol (UDP) message size.

22.14.2. **[Conditional: SS, NA, EBC, R, LS, EI]** If IKEv2 is supported, the system shall support the use of the ID_IPv6_ADDR and ID_IPV4_ADDR Identification Type.

22.14.3. **[Conditional: SS, NA, EBC, R, LS, EI]** If the system supports IKEv2, the system shall be capable of ignoring subsequent SA setup response messages after the receipt of a valid response.

22.14.4. **[Conditional: SS, NA, EBC, R, LS, EI]** If the system supports IKEv2, the system shall be capable of sending a Delete payload to the other end of the security association.

22.14.5. **[Conditional: SS, NA, EBC, R, LS, EI]** If the system supports IKEv2, the system shall reject initial IKE messages unless they contain a Notify payload of type COOKIE.

22.14.6. **[Conditional: SS, NA, EBC, R, LS, EI]** If the system supports IKEv2, the system shall close a SA instead of rekeying when its lifetime expires if there has been no traffic since the last rekey.

22.14.7. **[Conditional: SS, NA, EBC, R, LS, EI]** If the system supports IKEv2, the system shall not use the Extensible Authentication Protocol (EAP) method for IKE authentication.

22.14.8. **[Conditional: SS, NA, EBC, R, LS, EI]** If the system supports IKEv2, the system shall limit the frequency to which it responds to messages on UDP port 500 or 4500 when outside the context of a security association known to it.

22.14.9. **[Conditional: SS, NA, EBC, R, LS, EI]** If the system supports IKEv2, the system shall not support temporary IP addresses or respond to such requests.

22.14.10. **[Conditional: SS, NA, EBC, R, LS, EI]** If the system supports IKEv2, the system shall support the IKEv2 cryptographic algorithms defined in RFC 4307.

22.14.11. **[Conditional: SS, NA, EBC, R, LS, EI]** If the system supports IKEv2, the system shall support the VPN-B Suite as defined in RFC 4308 and RFC 4869 (FY2010).

- Encryption - AES with 128-bit keys in CBC Mode
- Pseudo-random function – AES-XCBC-PRF-128
- Integrity – AES-XCBC-MAC-96
- Diffie-Hellman Group – 2048-bit MODP
- Rekeying of Phase 2 or the CREATE_CHILD_SA shall be supported by both parties. The initiator of the exchange may include a Diffie-Hellman key; if included, it shall be a type 2048 – bit MODP. If the initiator of the exchange includes a Diffie-Hellman key, the responder shall include a Diffie-Hellman key and it shall also be a type 2048-bit MODP.

NOTE: RFC 4869 Suite B Cryptographic Suites for IPsec identifies four new cryptographic user interface suites based on implementations of the U.S. NSA's Suite B algorithms.

22.15. **[Required: R, EI (Softphone Only)] [Conditional: SS, NA, EBC, LS, EI]** If RFC 4301 is supported, the system shall support extensions to the Internet IP Security Domain of Interpretation for the Internet Security Association and Key Management Protocol (ISAKMP) as defined in RFC 2407.

22.16. **[Required: R, EI (Softphone Only)] [Conditional: SS, NA, EBC, LS, EI]** If RFC 4301 is supported, the system shall support the ISAKMP as defined in RFC 2408.

22.17. **[Required: R] [Conditional: SS, NA, EBC, LS, EI]** If the system supports the IPsec Authentication Header Mode, the system shall support the IP Authentication Header (AH) as defined in RFC 4302.

22.18. **[Required: R, EI (Softphone Only)] [Conditional: SS, NA, EBC, LS, EI]** If RFC 4301 is supported, the system shall support manual keying of IPSec.

22.19. **[Required: R, EI (Softphone Only)] [Conditional: SS, NA, EBC, LS, EI]** If RFC 4301 is supported, the system shall support the ESP and AH cryptographic algorithm implementation requirements as defined in RFC 4305 and RFC 4835 (FY2010).

22.20. Reserved.

22.21. **[Required: R, EI (Softphone Only)] [Conditional: SS, NA, EBC, LS, EI]** If RFC 4301 is supported, the system shall support the IKEv1 security algorithms as defined in RFC 4109.

5.3.5.3.10 Network Management (NM)

23. **[Required: SS, NA, EBC, R, LS]** The system shall comply with the Management Information Base (MIB) for IPv6 textual conventions and general group as defined in RFC 4293. NOTE: The requirements to support SNMPv3 are found in UCR 2008, Section 5.3.2.17.3.1.5, SNMP Version 2 and Version 3 Format Alarm messages, and UCR 2008, Section 5.4, Information Assurance.

    23.1 **[Required: R] [Conditional: LS]** If the system performs routing functions, the system shall support the SNMP management framework as described in RFC 3411.

    23.2 **[Required: R] [Conditional: LS]** If the system performs routing functions, the system shall support SNMP message processing and dispatching as described in RFC 3412.

    23.3 **[Required: R] [Conditional: LS]** If the system performs routing functions, the system shall support the SNMP applications as described in RFC 3413.

24. **[Required: SS, NA, EBC, R, LS]** The system shall support the ICMPv6 MIBs as defined in RFC 4293.

25. **[Required: SS, NA, EBC, R, LS]** The system shall support the Transmission Control Protocol (TCP) MIBs as defined in RFC 4022.

26. **[Required: SS, NA, EBC, R, LS]** The system shall support the UDP MIBs as defined in RFC 4113.

27. **[Required: R] [Conditional: LS]** If the system performs routing functions, the system shall support IP tunnel MIBs as described in RFC 4087.

28. **[Required: R] [Conditional: LS]** If the system performs routing functions, the system shall support the IP Forwarding MIB as defined in RFC 4292.

29. **[Conditional: R, LS]** If the system supports mobile users, the system shall support the Mobile IP Management MIBs as described in RFC 4295.

30. **[Required: R] [Conditional: LS]** If the system supports SNMP and supports routing functions, the system shall support the textual conventions for IPv6 flow labels as described in RFC 3595.

31. **[Required: R] [Conditional: LS]** If the system supports SNMP and IPsec, the system shall support the IPsec security policy database as described in RFC 4807.

32. **[Required: EI (Softphone only)] [Conditional: SS, NA, EBC, R, LS, EI]** If the system uses Uniform Resource Identifiers (URIs), the system shall use the URI syntax described in RFC 3986.

33. **[Conditional: SS, NA, EBC, R, LS, EI]** If the system uses the Domain Name System (DNS), the system shall conform to RFC 3596 for DNS queries.

    NOTE: DNS is primarily used for NM applications.

5.3.5.3.11 Traffic Engineering

34. **[Required: R, LS, EBC, SS]** For traffic engineering purposes, the bandwidth required per voice subscriber is calculated to be 110.0 kbps (each direction) for each IPv6 call. This is based on G.711 (20 ms codec) with IP overhead (100 kbps) resulting in a 250 byte bearer packet plus 10 kbps for signaling, Ethernet Interframe Gap, and the SRTCP overhead. Based on overhead bits included in the bandwidth calculations, vendor implementations may use different calculations and hence arrive at slightly different numbers.

35. **[Required: R, LS]** The number of VoIP subscribers per link size for IPv6 is the same as for IPv4 and is defined in UCR 2008, Section 5.3.1, Assured Services Local Area Network Infrastructure Product Requirements.

36. **[Required: R, LS]** The number of video subscribers per link size for IPv6 is the same as for IPv4 and is defined in UCR 2008, Section 5.3.1, Assured Services Local Area Network Infrastructure Product Requirements.

5.3.5.3.12 IP Version Negotiation

37. **[Required: SS, EBC]** The system shall forward packets using the same IP version as the version in the received packet.

    NOTE: If the packet was received as an IPv6 packet, the appliance will forward it as an IPv6 packet. If the packet was received as an IPv4 packet, the appliance will forward the packet as an IPv4 packet. This requirement is primarily associated with the signaling packets to ensure that translation does not occur. This requirement may be waived from FY2008 to FY12 in order to support IPv4 or IPv6 only EIs.

38. **[Required: SS, NA, EI]** The system shall use the Alternative Network Address Types (ANAT) semantics for the Session Description Protocol (SDP) in accordance with RFC 4091 when establishing media streams from dual stacked appliances for AS-SIP signaled sessions.

    38.1. **[Required: SS, NA, EI]** The system shall prefer any IPv4 address to any IPv6 address when using ANAT semantics.

    38.2. **[Required: SS, NA, EI]** The system shall place the SDP-ANAT option-tag in a required header field when using ANAT semantics in accordance with RFC 4092.

    38.3. **[Required: EI]** Dual stacked systems shall include the IPv4 and IPv6 addresses within the SDP of the SIP INVITE message when the INVITE contains the SDP.

5.3.5.3.13 AS-SIP IPv6 Unique Requirements

39. **[Conditional: SS, NA, EBC, EI]** If the system is using AS-SIP and the <addrtype> is IPv6 and the <connection-address> is a unicast address, the system shall support generation and processing of unicast IPv6 addresses having the following formats:

- x:x:x:x:x:x:x:x (where *x* is the hexadecimal values of the eight 16-bit pieces of the address). Example: 1080:0:0:0:8:800:200C:417A

- x:x:x:x:x:x:d.d.d.d (where *x* is the hexadecimal values of the six high-order 16-bit pieces of the address, and *d* is the decimal values of the four low-order 8-bit pieces of the address (standard IPv4 representation). Example: 1080:0:0:0:8:800:116.23.135.22

40. **[Conditional: SS, NA, EBC, EI]** If the system is using AS-SIP, the system shall support the generation and processing of IPv6 unicast addresses using compressed zeros consistent with one of the following formats:

    - x:x:x:x:x:x:x:x format: 1080:0:0:0:8:800:200C:417A
    - x:x:x:x:x:x:d.d.d.d format: 1080:0:0:0:8:800:116.23.135.22
    - compressed zeros: 1080::8:800:200C:417A

41. **[Conditional: SS, NA, EBC, EI]** If the system is using AS-SIP and the <addrtype> is IPv6 and the <connection-address> is a multicast group address (i.e., the two most significant hexadecimal digits are FF), the system shall support the generation and processing of multicast IPv6 addresses having the same formats as the unicast IPv6 addresses.

42. Reserved.

43. **[Conditional: SS, NA, EBC, EI]** If the system is using AS-SIP and the <addrtype> is IPv6 and the <connection-address> is an IPv6 multicast group address, the multicast connection address shall not have a TTL value appended to the address as IPv6 multicast does not use TTL scoping.

44. **[Conditional: SS, NA, EBC, EI]** If the system is using AS-SIP, the system shall support the processing of IPv6 multicast group addresses having the <number of address> field and may support generating the <number of address> field. This field has the identical format and operation as the IPv4 multicast group addresses.

45. **[Required: EBC]** The system shall be able to provide topology hiding (e.g., NAT) for IPv6 packets in the manner described in UCR 2008 Section 5.4, Information Assurance.

46. **[Required: EI (Softphone)]** The system shall support default address selection for IPv6 as defined in RFC 3484 (except for Section 2.1).

NOTE: It assumed that an IPv6 appliance will have as a minimum an IPv6 link local and an IPv4 address and will have at least two addresses.

5.3.5.3.14 Miscellaneous Requirements

47. **[Conditional: EBC, R, LS]** If the system supports Remote Authentication Dial In User Service (RADIUS) authentication, the system shall support RADIUS in the manner defined in RFC 3162.

    NOTE: RFC 3162 only defines the additional attributes of RADIUS that are unique to IPv6 implementations. For the base RADIUS requirements, other RFCs are required, such as RFC 2865.

48. **[Conditional: EI (Softphone)]** If the system supports Mobile IP version 6 (MIPv6), the system shall provide mobility support as defined in RFC 3775.

    48.1. **[Conditional: R]** If the system acts as a home agent, the system shall provide mobility support as defined in RFC 3775.

49. **[Conditional: R, EI (Softphone)]** If the system supports Mobile IP version 6 (MIPv6), the system shall provide a secure manner to signal between mobile nodes and home agents in manner described in RFC 3776 and RFC 4877 (FY2010).

50. Reserved.

51. **[Conditional: R, LS]** If the system supports network mobility (NEMO), the system shall support the function as defined in RFC 3963.

52. **[Required: SS, NA, EBC, R, LS, EI]** The systems shall support Differentiated Services as Described in RFC 2474 and RFC 5072 (FY 2010) for a voice and video stream to the security association in accordance with UCR 2008, Section 5.3.2, Assured Services Requirements and UCR 2008, Section 5.3.3, Network Infrastructure End-to-End Performance Requirements, plain text DSCP plan.
53. **[Conditional: EI (Softphone), R]** If the system acts as an IPv6 tunnel broker, the system shall support the function in the manner defined in RFC 3053.

54. **[Conditional: R]** If the system supports roaming (as defined within RFC 4282), the system shall support this function as described by RFC 4282.

55. **[Conditional: R]** If the system supports the Point-to-Point Protocol (PPP), the system shall support PPP as described in RFC 2472.

5.3.5.4 Mapping of RFCs to DoD IPv6 Profile Categories

Table 5.3.5-2. UC Network Appliance (EI, MG)

RFC NUMBER	RFC TITLE	REQUIRED – R CONDITIONAL – C
2407	The Internet IP Security Domain of Interpretation for ISAKMP	C*
2408	Internet Security Association and Key Management Protocol (ISAKMP)	C*
2409	The Internet Key Exchange (IKE)	C*
2460	Internet Protocol, Version 6 (v6) Specification	R-2
2461	Neighbor Discovery for IP Version 6 (IPv6)	R
2462	IPv6 Stateless Address Autoconfiguration	C
2464	Transmission of IPv6 Packets over Ethernet Networks	R-3
2474	Definition of the Differentiated Services Field (DS Field) in the IPv4 and IPv6 Headers	R-4*
2710	Multicast Listener Discovery (MLD) for IPv6	R
3315	Dynamic Host Configuration Protocol for IPv6 (DHCPv6)	C
3596	DNS Extensions to Support IP Version 6	C*
3986	Uniform Resource Identifier (URI): Generic Syntax	C-6*
4007	IPv6 Scoped Address Architecture	R
4022	Management Information Base for the Transmission Control Protocol (TCP)	R
4091	The Alternative Network Address Types (ANAT) Semantics for the Session Description Protocol (SDP) Grouping Framework	R*
4092	Usage of the Session Description Protocol (SDP) Alternative Network Address Types (ANAT) Semantics in the Session Initiation Protocol (SIP)	R*
4109	Algorithms for Internet Key Exchange version 1 (IKEv1)	C*
4113	Management Information Base for the User Datagram Protocol (UDP)	R
4213	Basic Transition Mechanisms for IPv6 Hosts and Routers	R-1*
4291	IP Version 6 Addressing Architecture	R
4293	Management Information Base for the Internet Protocol (IP)	R
4301	Security Architecture for the Internet Protocol	C*
4302	IP Authentication Header	C*
4303	IP Encapsulating Security Payload (ESP)	C*
4305	Cryptographic Algorithm Implementation Requirements for Encapsulating Security Payload (ESP) and Authentication Header (AH)	C*

RFC NUMBER	RFC TITLE	REQUIRED – R CONDITIONAL – C
4306	Internet Key Exchange (IKEv2) Protocol	C-10*
4307	Cryptographic Algorithms for Use in the Internet Key Exchange Version 2 (IKEv2)	C*
4308	Cryptographic Suites for IPSec	C*
4443	Internet Control Message Protocol (ICMPv6) for the Internet Protocol Version 6 (IPv6) Specification	R
4835	Cryptographic Algorithm Implementation Requirements for Encapsulating Security Payload (ESP) and Authentication Header (AH)	C-10*
4861	Neighbor Discovery for IP version 6 (IPv6)	R-10*
4862	IPv6 Stateless Address Autoconfiguration	C-10
4941	Privacy Extensions for Stateless Address Autoconfiguration in IPv6	R-10*
5095	Deprecation of Type 0 Routing Headers in IPv6	R*

NOTES:
R-1: Only meets the dual stack requirements of this RFC
R-2: Only meets IPv6 formatting requirements of this RFC
R-3: Only meets framing format aspects of RFC
R-4: Requirement covered in Section 5.3.3, Wide Area Network General System Requirements, of this UCR 2008.
C/R-10: Conditional/Objective Requirement for FY2010
C-5: Condition is that system acts as a router
C-6: Only applies to MG
*: Deviation from DoD IPv6 version 2 Profile Appendix C

Table 5.3.5-3. UC Host/Workstation (EI (Softphone))

RFC NUMBER	RFC TITLE	REQUIRED – R CONDITIONAL – C
1981	Path MTU Discovery for IPv6	R
2407	The Internet IP Security Domain of Interpretation for ISAKMP	R*
2408	Internet Security Association and Key Management Protocol (ISAKMP)	R*
2409	The Internet Key Exchange (IKE)	R*
2460	Internet Protocol, Version 6 (v6) Specification	R-2
2461	Neighbor Discovery for IP Version 6 (IPv6)	R
2462	IPv6 Stateless Address Autoconfiguration	R
2464	Transmission of IPv6 Packets over Ethernet Networks	R-3
2474	Definition of the Differentiated Services Field (DS Field) in the IPv4 and IPv6 Headers	R-4*
2710	Multicast Listener Discovery (MLD) for IPv6	R
3041	Privacy Extensions for Stateless Address Autoconfiguration in IPv6	C
3053	IPv6 Tunnel Broker	C

RFC NUMBER	RFC TITLE	REQUIRED – R CONDITIONAL – C
3315	Dynamic Host Configuration Protocol for IPv6 (DHCPv6)	R*
3484	Default Address Selection for Internet Protocol version 6 (IPv6)	R*
3596	DNS Extensions to Support IP Version 6	R*
3775	Mobility Support in IPv6	C*
3776	Using IPSec to Protect Mobile IPv6 Signaling Between Mobile Nodes and Home Agents	C
3810	Multicast Listener Discovery Version 2 (MLDv2) for IPv6	R
3986	Uniform Resource Identifier (URI): Generic Syntax	R
4007	IPv6 Scoped Address Architecture	R
4091	The Alternative Network Address Types (ANAT) Semantics for the Session Description Protocol (SDP) Grouping Framework	R*
4092	Usage of the Session Description Protocol (SDP) Alternative Network Address Types (ANAT) Semantics in the Session Initiation Protocol (SIP)	R*
4109	Algorithms for Internet Key Exchange version 1 (IKEv1)	R*
4213	Basic Transition Mechanisms for IPv6 Hosts and Routers	R-1
4291	IP Version 6 Addressing Architecture	R
4301	Security Architecture for the Internet Protocol	R
4302	IP Authentication Header	C*
4303	IP Encapsulating Security Payload (ESP)	R
4305	Cryptographic Algorithm Implementation Requirements for Encapsulating Security Payload (ESP) and Authentication Header (AH)	R
4306	Internet Key Exchange (IKEv2) Protocol	R-10
4307	Cryptographic Algorithms for Use in the Internet Key Exchange Version 2 (IKEv2)	C
4308	Cryptographic Suites for IPSec	R*
4443	Internet Control Message Protocol (ICMPv6) for the Internet Protocol Version 6 (IPv6) Specification	R
4835	Cryptographic Algorithm Implementation Requirements for Encapsulating Security Payload (ESP) and Authentication Header (AH)	R-10*
4861	Neighbor Discovery for IP Version 6 (IPv6)	R-10*
4862	IPv6 Stateless Address Autoconfiguration	R-10*
4941	Privacy Extensions for Stateless Address Autoconfiguration in IPv6	R-10*
5095	Deprecation of Type 0 Routing Headers in IPv6	R*

RFC NUMBER	RFC TITLE	REQUIRED – R CONDITIONAL – C
NOTES: R-1: Only meets the dual stack requirements of this RFC R-2: Only meets IPv6 formatting requirements of this RFC R-3: Only meets framing format aspects of RFC R-4: Requirement covered in UCR 2008, Section 5.3.3, Wide Area Network General System Requirements C/R-10: Conditional/Objective Requirement for FY2010 C-5: Condition is that system acts as a router C-6: Only applies to MG *: Deviation from DoD IPv6 version 2 Profile Appendix C		

Table 5.3.5-4. UC Simple Server (LSC, MFSS)

RFC NUMBER	RFC TITLE	REQUIRED – R CONDITIONAL – C
2407	The Internet IP Security Domain of Interpretation for ISAKMP	C*
2408	Internet Security Association and Key Management Protocol (ISAKMP)	C*
2409	The Internet Key Exchange (IKE)	C*
2460	Internet Protocol, Version 6 (v6) Specification	R-2
2461	Neighbor Discovery for IP Version 6 (IPv6)	R
2462	IPv6 Stateless Address Autoconfiguration	C
2464	Transmission of IPv6 Packets over Ethernet Networks	R-3
2474	Definition of the Differentiated Services Field (DS Field) in the IPv4 and IPv6 Headers	R-4*
2710	Multicast Listener Discovery (MLD) for IPv6	R
3315	Dynamic Host Configuration Protocol for IPv6 (DHCPv6)	C
3986	Uniform Resource Identifier (URI): Generic Syntax	C*
4007	IPv6 Scoped Address Architecture	R
4022	Management Information Base for the Transmission Control Protocol (TCP)	R*
4091	The Alternative Network Address Types (ANAT) Semantics for the Session Description Protocol (SDP) Grouping Framework	R*
4092	Usage of the Session Description Protocol (SDP) Alternative Network Address Types (ANAT) Semantics in the Session Initiation Protocol (SIP)	R*
4109	Algorithms for Internet Key Exchange version 1 (IKEv1)	C*
4113	Management Information Base for the User Datagram Protocol (UDP)	R
4213	Basic Transition Mechanisms for IPv6 Hosts and Routers	R-1*
4291	IP Version 6 Addressing Architecture	R
4293	Management Information Base for the Internet Protocol (IP)	R
4301	Security Architecture for the Internet Protocol	C*

RFC NUMBER	RFC TITLE	REQUIRED – R CONDITIONAL – C
4302	IP Authentication Header	C*
4303	IP Encapsulating Security Payload (ESP)	C*
4305	Cryptographic Algorithm Implementation Requirements for Encapsulating Security Payload (ESP) and Authentication Header (AH)	C*
4306	Internet Key Exchange (IKEv2) Protocol	C-10*
4307	Cryptographic Algorithms for Use in the Internet Key Exchange Version 2 (IKEv2)	C*
4308	Cryptographic Suites for IPSec	C*
4443	Internet Control Message Protocol (ICMPv6) for the Internet Protocol Version 6 (IPv6) Specification	R
4835	Cryptographic Algorithm Implementation Requirements for Encapsulating Security Payload (ESP) and Authentication Header (AH)	C-10*
4861	Neighbor Discovery for IP Version 6 (IPv6)	R-10*
4862	IPv6 Stateless Address Autoconfiguration	C-10*
5095	Deprecation of Type 0 Routing Headers in IPv6	R*

NOTES:
R-1: Only meets the dual stack requirements of this RFC
R-2: Only meets IPv6 formatting requirements of this RFC
R-3: Only meets framing format aspects of RFC
R-4: Requirement covered in UCR 2008, Section 5.3.3, Wide Area Network General System Requirements.
C/R-10: Conditional/Objective Requirement for FY2010
C-5: Condition is that system acts as a router
C-6: Only applies to MG
*: Deviation from DoD IPv6 version 2 Profile Appendix C

Table 5.3.5-5. UC Information Assurance Device (EBC)

RFC NUMBER	RFC TITLE	REQUIRED – R CONDITIONAL – C
1981	Path MTU Discovery for IPv6	R
2407	The Internet IP Security Domain of Interpretation for ISAKMP	C*
2408	Internet Security Association and Key Management Protocol (ISAKMP)	C*
2409	The Internet Key Exchange (IKE)	C*
2460	Internet Protocol, Version 6 (v6) Specification	R-2
2461	Neighbor Discovery for IP Version 6 (IPv6)	R, C-5
2462	IPv6 Stateless Address Autoconfiguration	C
2464	Transmission of IPv6 Packets over Ethernet Networks	R-3
2473	Generic Packet Tunneling in IPv6 Specification	C-5
2474	Definition of the Differentiated Services Field (DS Field) in the IPv4 and IPv6 Headers	R-4*

RFC NUMBER	RFC TITLE	REQUIRED – R CONDITIONAL – C
2710	Multicast Listener Discovery (MLD) for IPv6	R
3162	RADIUS and IPv6	C
3315	Dynamic Host Configuration Protocol for IPv6 (DHCPv6)	C*
3986	Uniform Resource Identifier (URI): Generic Syntax	C
4007	IPv6 Scoped Address Architecture	R*
4022	Management Information Base for the Transmission Control Protocol (TCP)	R*
4109	Algorithms for Internet Key Exchange version 1 (IKEv1)	C*
4113	Management Information Base for the User Datagram Protocol (UDP)	R*
4213	Basic Transition Mechanisms for IPv6 Hosts and Routers	R-1*
4291	IP Version 6 Addressing Architecture	R
4293	Management Information Base for the Internet Protocol (IP)	R*
4301	Security Architecture for the Internet Protocol	C
4302	IP Authentication Header	C*
4303	IP Encapsulating Security Payload (ESP)	C
4305	Cryptographic Algorithm Implementation Requirements for Encapsulating Security Payload (ESP) and Authentication Header (AH)	C
4306	Internet Key Exchange (IKEv2) Protocol	C-10
4307	Cryptographic Algorithms for Use in the Internet Key Exchange Version 2 (IKEv2)	C-10
4308	Cryptographic Suites for IPSec	C*
4443	Internet Control Message Protocol (ICMPv6) for the Internet Protocol Version 6 (IPv6) Specification	R
4835	Cryptographic Algorithm Implementation Requirements for Encapsulating Security Payload (ESP) and Authentication Header (AH)	C-10*
4861	Neighbor Discovery for IP Version 6 (IPv6)	R-10*
4862	IPv6 Stateless Address Autoconfiguration	R-10*
5095	Deprecation of Type 0 Routing Headers in IPv6	R*

NOTES:
R-1: Only meets the dual stack requirements of this RFC
R-2: Only meets IPv6 formatting requirements of this RFC
R-3: Only meets framing format aspects of RFC
R-4: Requirement covered in Section 5.3.3, Wide Area Network General System Requirements, of this UCR 2008.
C/R-10: Conditional/Objective Requirement for FY2010
C-5: Condition is that system acts as a router
C-6: Only applies to MG
*: Deviation from DoD IPv6 version 2 Profile Appendix C

Table 5.3.5-6. UC Router (R)

RFC NUMBER	RFC TITLE	REQUIRED – R CONDITIONAL – C
1772	Application of the Border Gateway Protocol in the Internet	C-7
1981	Path MTU Discovery for IPv6	R
2407	The Internet IP Security Domain of Interpretation for ISAKMP	R
2408	Internet Security Association and Key Management Protocol (ISAKMP)	R
2409	The Internet Key Exchange (IKE)	R
2460	Internet Protocol, Version 6 (v6) Specification	R-2
2461	Neighbor Discovery for IP Version 6 (IPv6)	R
2462	IPv6 Stateless Address Autoconfiguration	R
2464	Transmission of IPv6 Packets over Ethernet Networks	R-3
2472	IP Version 6 over PPP	C
2473	Generic Packet Tunneling in IPv6 Specification	C-7
2474	Definition of the Differentiated Services Field (DS Field) in the IPv4 and IPv6 Headers	R-4
2545	Use of BGP-4 Multiprotocol Extensions for IPv6 Inter-Domain Routing	C-5
2710	Multicast Listener Discovery (MLD) for IPv6	R
2740	OSPF for IPv6	R
2784	Generic Router Encapsulation	C-7
2858	Multiprotocol Extensions for BGP-4	R-5
3053	IPv6 Tunnel Broker	C
3162	RADIUS and IPv6	C*
3315	Dynamic Host Configuration Protocol for IPv6 (DHCPv6)	C
3411	An Architecture for Describing Simple Network Management Protocol (SNMP) Management Frameworks	R
3412	Message Processing and Dispatching for the Simple Network Management Protocol (SNMP)	R
3413	Simple Network Management Protocol (SNMP) Applications	R
3595	Textual Conventions for IPv6 Flow Label	R
3775	Mobility Support in IPv6	C*
3776	Using IPSec to Protect Mobile IPv6 Signaling Between Mobile Nodes and Home Agents	C*
3810	Multicast Listener Discovery Version 2 (MLDv2) for IPv6	R
3963	Network Mobility (NEMO) Basic Support Protocol	C
3986	Uniform Resource Identifier (URI): Generic Syntax	C*
4007	IPv6 Scoped Address Architecture	R
4022	Management Information Base for the Transmission Control Protocol (TCP)	R
4087	IP Tunnel MIB	R
4109	Algorithms for Internet Key Exchange version 1 (IKEv1)	R*
4113	Management Information Base for the User Datagram Protocol (UDP)	R

RFC NUMBER	RFC TITLE	REQUIRED – R CONDITIONAL – C
4213	Basic Transition Mechanisms for IPv6 Hosts and Routers	R-1
4271	A Border Gateway Protocol 4 (BGP-4)	R-4, R-5
4291	IP Version 6 Addressing Architecture	R
4282	The Network Access Identifier	C*
4292	IP Forwarding MIB	R
4293	Management Information Base for the Internet Protocol (IP)	R
4295	Mobile IP Management MIB	C
4301	Security Architecture for the Internet Protocol	R
4302	IP Authentication Header	R
4303	IP Encapsulating Security Payload (ESP)	R
4305	Cryptographic Algorithm Implementation Requirements for Encapsulating Security Payload (ESP) and Authentication Header (AH)	R
4306	Internet Key Exchange (IKEv2) Protocol	R-10
4307	Cryptographic Algorithms for Use in the Internet Key Exchange Version 2 (IKEv2)	R
4308	Cryptographic Suites for IPSec	R*
4443	Internet Control Message Protocol (ICMPv6) for the Internet Protocol Version 6 (IPv6) Specification	R
4760	Multiprotocol Extensions for BGP-4	R-5, R-10*
4807	IPsec Security Policy Database Configuration MIB	R
4835	Cryptographic Algorithm Implementation Requirements for Encapsulating Security Payload (ESP) and Authentication Header (AH)	R-10*
4861	Neighbor Discovery for IP Version 6 (IPv6)	R-10*
4862	IPv6 Stateless Address Autoconfiguration	R-10*
4941	Privacy Extensions for Stateless Address Autoconfiguration in IPv6	R-10*
5095	Deprecation of Type 0 Routing Headers in IPv6	R*

NOTES:
R-1: Only meets the dual stack requirements of this RFC
R-2: Only meets IPv6 formatting requirements of this RFC
R-3: Only meets framing format aspects of RFC
R-4: Requirement covered in Section 5.3.3, Wide Area Network General System Requirements, of this UCR 2008.
C/R-10: Conditional/Objective Requirement for FY2010
C-5: Condition is that system acts as a router
C-6: Only applies to MG
C-7: Requirements only applied if system acts as a customer edge router
*: Deviation from DoD IPv6 version 2 Profile Appendix C

Table 5.3.5-7. LAN Switch (LS)

RFC NUMBER	RFC TITLE	REQUIRED – R CONDITIONAL – C
1981	Path MTU Discovery for IPv6	R
2407	The Internet IP Security Domain of Interpretation for ISAKMP	C*
2408	Internet Security Association and Key Management Protocol (ISAKMP)	C*
2409	The Internet Key Exchange (IKE)	C*
2460	Internet Protocol, Version 6 (v6) Specification	R-2, C-5
2461	Neighbor Discovery for IP Version 6 (IPv6)	R
2462	IPv6 Stateless Address Autoconfiguration	R
2464	Transmission of IPv6 Packets over Ethernet Networks	R-3
2474	Definition of the Differentiated Services Field (DS Field) in the IPv4 and IPv6 Headers	R-4*
2710	Multicast Listener Discovery (MLD) for IPv6	R
2740	OSPF for IPv6	C-5*
2858	Multiprotocol Extensions for BGP-4	C-5
3162	RADIUS and IPv6	C*
3315	Dynamic Host Configuration Protocol for IPv6 (DHCPv6)	C
3411	An Architecture for Describing Simple Network Management Protocol (SNMP) Management Frameworks	C-5
3412	Message Processing and Dispatching for the Simple Network Management Protocol (SNMP)	C-5
3413	Simple Network Management Protocol (SNMP) Applications	C-5
3595	Textual Conventions for IPv6 Flow Label	C-5
3810	Multicast Listener Discovery Version 2 (MLDv2) for IPv6	C-5
3963	Network Mobility (NEMO) Basic Support Protocol	C*
3986	Uniform Resource Identifier (URI): Generic Syntax	C*
4007	IPv6 Scoped Address Architecture	R
4022	Management Information Base for the Transmission Control Protocol (TCP)	R
4087	IP Tunnel MIB	C-5
4109	Algorithms for Internet Key Exchange version 1 (IKEv1)	C*
4113	Management Information Base for the User Datagram Protocol (UDP)	R
4213	Basic Transition Mechanisms for IPv6 Hosts and Routers	R-1*
4291	IP Version 6 Addressing Architecture	R
4292	IP Forwarding MIB	C-5
4293	Management Information Base for the Internet Protocol (IP)	R
4295	Mobile IP Management MIB	C
4301	Security Architecture for the Internet Protocol	C*
4302	IP Authentication Header	C*
4303	IP Encapsulating Security Payload (ESP)	C*

RFC NUMBER	RFC TITLE	REQUIRED – R CONDITIONAL – C
4305	Cryptographic Algorithm Implementation Requirements for Encapsulating Security Payload (ESP) and Authentication Header (AH)	C*
4306	Internet Key Exchange (IKEv2) Protocol	C-10*
4307	Cryptographic Algorithms for Use in the Internet Key Exchange Version 2 (IKEv2)	C*
4308	Cryptographic Suites for IPSec	C*
4443	Internet Control Message Protocol (ICMPv6) for the Internet Protocol Version 6 (IPv6) Specification	R
4760	Multiprotocol Extensions for BGP-4	C-5, C-10*
4807	IPsec Security Policy Database Configuration MIB	R
4835	Cryptographic Algorithm Implementation Requirements for Encapsulating Security Payload (ESP) and Authentication Header (AH)	C-10*
4861	Neighbor Discovery for IP Version 6 (IPv6)	R-10*
4862	IPv6 Stateless Address Autoconfiguration	R-10*
4941	Privacy Extensions for Stateless Address Autoconfiguration in IPv6	R-10*
5095	Deprecation of Type 0 Routing Headers in IPv6	R*

NOTES:
R-1: Only meets the dual stack requirements of this RFC
R-2: Only meets IPv6 formatting requirements of this RFC
R-3: Only meets framing format aspects of RFC
C/R-4: Requirement covered in Section 5.3.3, Wide Area Network General System Requirements, of this UCR 2008.
R-5: Requirements only applied if system acts as a customer edge router.
C/R-10: Conditional/Objective Requirement for FY2010
C-5: Condition is that system acts as a router
C-6: Only applies to MG
*: Deviation from DoD IPv6 version 2 Profile Appendix C

Table 3.1-1 provides the IPv6 Rules of Engagement for Products. **Note that Network Management (NM) is not included in this list, since NM at this time is not required to be IPv6 capable.**

Table 5.3.5-8 IPv6 Rules of Engagement for Products

DSN Product (Appliance)	IPv6 Profile Category	IPv6 Product Rules of Engagement
Multifunction Switch	Simple Server (SS)	MFS in conjunction with the End Instrument must be IPv6 capable
End Office Switch	Simple Server (SS)	EO in conjunction with the End Instrument must be IPv6 capable
Small End Office	Simple Server (SS)	SMEO in conjunction with the End Instrument must be IPv6 capable
Deployed Voice Exchange	Simple Server (SS)	DVX in conjunction with the End Instrument must be IPv6 capable
Private Branch Exchange 1	Simple Server (SS)	PBX1in conjunction with the End Instrument must be IPv6 capable
Private Branch Exchange 2	Simple Server (SS)	PBX2 in conjunction with the End Instrument must be IPv6 capable
Customer Premise Equipment	Network Appliance (NA)	Need not be IPv6 capable at this time. Exception: IP End Instruments must be IPv6 capable via Dual Stack or Translation
Network Element	Network Appliance (NA)	Must be IPv6 capable
LAN Switch	Layer 3 Switch (LS)	Must be Dual Stack IPv6 and IPv4
Router	Router (R)	Must be Dual Stack IPv6 and IPv4
Echo Canceller	Network Appliance (NA)	Need not be IPv6 capable at this time
Integrated Access Switch	Network Appliance (NA)	Must be IPv6 capable via Dual Stack or Translation if supporting an IP End Instrument.
Conference Bridge (external)	Network Appliance (NA)	Need not be IPv6 capable at this time
Multipoint Control Unit	Network Appliance (NA)	Need not be IPv6 capable at this time
Video Telephony Unit	Network Appliance (NA)	Need not be IPv6 capable at this time
H.323/H.320 Gateway	Network Appliance (NA)	Need not be IPv6 capable at this time

TABLE OF CONTENTS

SECTION **PAGE**

5.4 Information Assurance Requirements....1197
5.4.1 Section Overview and Scope....1197
5.4.2 VVoIP IA Requirements Structured Process....1197
5.4.3 Non-Mitigated Risks....1200
5.4.4 VVoIP Generic Countermeasures....1211
5.4.4.1 Recommended Countermeasures....1211
5.4.4.2. Access Control Countermeasures....1213
5.4.4.3 Authentication Countermeasures....1213
5.4.4.4 Non-Repudiation Countermeasures....1214
5.4.4.5 Data Confidentiality Countermeasures....1215
5.4.4.6 Data Integrity Countermeasures....1215
5.4.4.7 Survivability/Availability Countermeasures....1216
5.4.4.8 Miscellaneous Countermeasures....1216
5.4.4.9 Privacy Countermeasures....1216
5.4.4.10 Network Management Countermeasures....1217
5.4.5 VVoIP IA Design....1217
5.4.5.1 Physical Security....1217
5.4.5.2 VVoIP Appliance Security Design....1218
5.4.5.2.1 User Roles....1218
5.4.5.2.2 Hardened Operating Systems....1220
5.4.5.2.3 Auditing....1220
5.4.5.2.4 Application Security....1224
5.4.5.2.5 Redundant Systems....1224
5.4.5.3 VVoIP Component Interactions....1225
5.4.5.4 VVoIP Protocol Design....1230
5.4.5.4.1 Overview....1230
5.4.5.4.2 End Instrument Authentication and Registration....1231
5.4.5.4.3 User Authentication and Authorization....1232
5.4.5.4.4 Signaling Appliance Authentication and Authorization....1233
5.4.5.4.5 Network Management....1236
5.4.5.4.6 Secure VVoIP End Instruments....1239
5.4.5.4.7 Edge Boundary Control Appliances....1239
5.4.5.5 VVoIP IA Design Items Outstanding....1245
5.4.6 Requirements....1246

5.4.6.1 Introduction....1246
5.4.6.2 General Requirements....1246
5.4.6.2.1 Authentication (Includes Authorization and Access Control)....1249
5.4.6.2.2 Integrity....1286
5.4.6.2.3 Confidentiality....1289
5.4.6.2.4 Non-Repudiation....1300
5.4.6.2.5 Availability....1304
5.4.6.3 Time Division Multiplexing (TDM) Unique....1304
5.4.7 Quality Assurance Provisions....1305
5.4.7.1 Responsibility for Inspection....1305
5.4.8 Mitigated Risks....1306

5.4 INFORMATION ASSURANCE REQUIREMENTS

5.4.1 Section Overview and Scope

This UCR 2008 section consolidated the TDM and IP Voice and Video over IP (VVoIP) IA requirements from the Unified Capabilities Requirements 2007 (UCR 2007), Section 13, and the Real-Time Services (RTS) IA Generic System Requirements (GSR). Future updates to this section will expand on the Voice TDM IA architectural aspects to the same extent that VVoIP IA design aspects are discussed.

5.4.2 VVoIP IA Requirements Structured Process

This UCR 2008 section provides an overview of the VVoIP IA design and specifies the VVoIP IA requirements using a defined, structured process in order to secure the VVoIP system. The process is called the IA Process, shown in Figure 5.4.2-1, because it applies to any IA design. A basic tenet of this process is that threats are the primary driver for all stages of the IA Process. However, it is recognized that architectures may be influenced by other drivers, such as political, time, and technical motivators. This section is structured to follow the IA Process in the development of the VVoIP IA design and requirements.

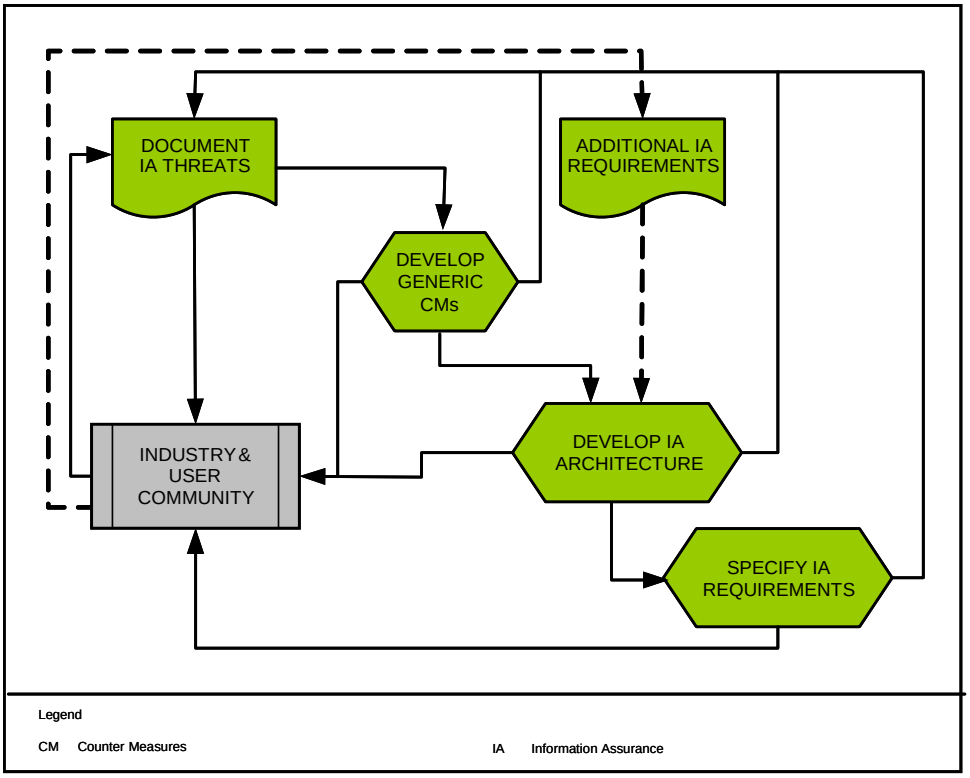


Figure 5.4.2-1. IA Process

The first step in the IA process is to document the threats based on a preliminary understanding of how the system will be deployed and in conformance with the DoD high-level IA requirements. A summary of the threats is provided in this UCR 2008 section, but the details of the threats are found in the "Analysis of Information Assurance Requirements and Threats for the DoD Real-Time Services Environment," Version 3.4, DoD RTS IA Working Group, 23 May 2006. In creating the IA section of the UCR, the threats were vetted with industry and the user community in order to get user buy-in and to ensure that all known threats were documented. An example of a threat is eavesdropping on the media stream of a telephone call to hear the contents of a conversation. After the threats were documented, the risks associated with each threat were classified based on the likelihood of a successful attack and the impact of a successful attack. The classification of the risks permitted the prioritization of resources to mitigate the risks during the development of the IA design.

Based on the threats, a set of generic countermeasures (CMs) was developed. A summary of the countermeasures is discussed in the main body of UCR 2008, but the details of the countermeasures are found in "DoD RTS IA Countermeasures," Version 0.7, DoD RTS IA Working Group, 29 March 2006. The reason generic countermeasures were developed, instead of specific countermeasures, is that it allows for maximum flexibility in selecting an approach to implement the countermeasure. Encryption of the media stream is an example of a generic countermeasure, which would mitigate the threat associated with eavesdropping on the media stream. In defining the generic countermeasures, it is important to understand the interdependence of the countermeasures and document those interdependencies.

For example, confidentiality without authentication and authorization diminishes its benefit. In addition, it is important to map threats to countermeasures to ensure all threats are addressed. As with the threats, the generic countermeasures were vetted with industry and the user community to determine if they were feasible and to get user buy-in.

The next step was to develop an IA design based on the generic countermeasures and threats. The first step in the development of the IA design was to identify candidate mechanisms that satisfy the countermeasures and mitigate the threats. For example, confidentiality of the bearer stream could be achieved by implementing the Secure Real Time Transport Protocol (SRTP), Internet Protocol Security (IPSec), or Type 1 point-to-point bulk encryption. The candidates were vetted with the user community and industry prior to selecting the default solution(s) for the IA design. Alternative solutions were allowed in specific cases, but a default solution was specified to ensure multivendor interoperability. In addition, although the threats and generic countermeasures were the primary driver of the IA design, political, time, and technical motivators also influenced the IA design and requirements and were incorporated into the IA design.

After the design was completed, the final step in the IA Process involved documenting the requirements necessary to achieve the IA design in a multivendor interoperable integrated environment that could be tested. An example of a requirement is that the system shall use SRTP for encrypting the media stream. As with the threats and countermeasures, the requirements were vetted with industry and the user community to ensure that the requirements were clear, concise, and achievable within the time frame allocated.

The requirements are loosely grouped by their IA category. The IA categories are defined in DoD Directive (DoDD) 8500.1. The IA categories are similar to the IA services described in the "Analysis of Information Assurance Requirements and Threats for the DoD Real-Time Services Environment," which was developed prior to UCR 2008, with one exception. The one exception is that unlike the "Analysis of Information Assurance Requirements and Threats for the DoD Real-Time Services Environment," DoDD 8500.1 does not have a separate category for authorization and includes the functions associated with authorization and access control in the authentication category. The "Analysis of Information Assurance Requirements and Threats for the DoD Real-Time Services Environment" is a reference document for the UCR 2008 and provides an IA analysis of the protocols, traceability of the DoD IA requirements, and a threat analysis of the VVoIP design. This document does not provide that background information and instead focuses on the requirements with an overview of the threats.

Table 5.4.2-1, Mapping of Security Services to Security Categories and Goals, shows a mapping of the security services in the "Analysis of Information Assurance Requirements and Threats for the DoD Real-Time Services Environment," and the security categories in DoDD 8500.1. For completeness, the table also maps the security services to the European Telecommunications Standards Institute (ETSI) Telecommunications and Internet Protocol Harmonization Over Networks (TIPHON); Protocols Framework Definition; Methods and Protocols for Security; Part 1: Threat Analysis, which provides a basis for the threat analysis used in this UCR 2008 section and is discussed later.

Table 5.4.2-1. Mapping of Security Services to Security Categories and Goals

"ANALYSIS OF IA REQUIREMENTS AND THREATS FOR THE DoD VVoIP ENVIRONMENT" SECURITY SERVICES	DoDD 8500.1 CATEGORIES	ETSI TS 102 165-1 GOALS
Authorization	Authentication (Includes Authorization and Access Control)	Accountability (Includes Non-Repudiation)
Authentication		
Non-Repudiation	Non-Repudiation	
Confidentiality	Confidentiality	Confidentiality
Integrity	Integrity	Integrity
Availability	Availability	Availability

This UCR 2008 section concludes with a discussion of the threats and the extent to which they have been mitigated by enforcing the requirements and implementing the countermeasures. In addition, a brief discussion of the outstanding IA design issues is discussed. This UCR 2008 section is a companion document to the STIGs, which are produced by the DISA FSO, and the intent is for this UCR 2008 section to complement the STIGs. For instance, UCR 2008 specifies the IA requirements that a VVoIP product must meet to be sold to DoD users. The STIGs specify the configurations that a DoD user must implement to ensure that the system is deployed in a secure manner.

5.4.3 Non-Mitigated Risks

The threat matrix used by the DISN IP VVoIP is based on the one developed by the ETSI TS 165-1. Where necessary it has been modified to reflect the threats that are unique to the DoD environment due to the issues raised in "Analysis of Information Assurance Requirements and Threats for the DoD Real-Time Services Environment," which also provides a complete discussion of the threats associated with each protocol. The threat matrix was developed to permit a prioritization of the risks associated with those threats in order to target the most urgent threats. It was developed with the knowledge that it is impossible to prevent all attacks, but it is possible to limit the avenues of attack and to react to an attack in an expeditious manner.

The threats identified by the ETSI TIPHON work are focused on the nonphysical threats and do not address the physical threats to the system or all the threats that might arise from the interaction with ancillary equipment (i.e., equipment external to the system such as an external DHCP server). Currently, TDM threats are not fully addressed in this document. Future updates to this section will address those deficiencies. These threats are summarized in Table 5.4.3-1, TIPHON Threats. The "Xs" in Table 5.4.3-1 indicate that the threat impacts the IA goal and must be mitigated to achieve that goal. The TIPHON Threats are extracted from ETSI TS 101 165-1 and additional detail is provided in the following paragraphs.

Masquerading or spoofing is the act of pretending to be someone you are not. This threat is often used to get information, deny a service, pervert a service, or misdirect a call. As shown in Table 5.4.3-1, masquerading is a system threat to confidentiality, integrity, accountability, and availability. It is also used as a means to introduce other threats to the system, such as unauthorized access or forgery, eavesdropping, and denial of service.

Table 5.4.3-1. TIPHON Threats

THREAT	GOALS			
	CONFIDENTIALITY	INTEGRITY	ACCOUNTABILITY	AVAILABILITY
Masquerade	X	X	X	X
Unauthorized Access	X (within a system)	X (within a system)	X	X
Eavesdropping	X (on the line)			
Loss or corruption of information		X (on the line)	X	X
Repudiation			X	
Forgery		X	X	
Denial of Service				X
NOTE: The Xs indicate that the threat impacts the IA goal and must be mitigated to achieve that goal.				

Unauthorized access is the act of someone accessing data or services in violation of the security policy. The threat with unauthorized access is that an attacker may access personal or classified information in a database or may be able to make precedence calls causing unnecessary network preemptions. As shown in Table 5.4.3-1, TIPHON Threats, unauthorized access is a threat to both confidentiality and integrity if the action is from within a system. In addition, it is a threat to accountability and availability regardless of where the attacker is located. The principal resultant threats associated with unauthorized access are denial of service, masquerading as a real user, and eavesdropping on other users.

Eavesdropping is a breach of confidentiality caused by the unauthorized monitoring of a communication. It is typically associated with the monitoring of a phone call. Eavesdropping is often used to determine call patterns, gain knowledge of personal information, and to acquire the information necessary to masquerade as another authorized user.

Loss or corruption of data is an attack that compromises the integrity of data. Typically, it involves unauthorized deletion, insertion, modification, reordering, replay, or delay. The goals that are impacted by loss or corruption of data are integrity, accountability, and availability. The loss or corruption of data on a call will affect the integrity of the call and may make the call unintelligible. If the call detail records are destroyed, the accountability for the call will be impacted. Finally, if the loss or corruption of data is significant enough, it could result in a denial of service, which would impact the availability of the system.

Repudiation is when a user involved in a session subsequently denies that the session took place. Non-repudiation is required by the DISN to prevent subscription fraud and to determine

responsibility for network management actions. The security service associated with this threat is accountability. In the DoD environment, this threat is not as significant as some of the other threats, but is still a concern.

Forgery is the act of fabricating information and then claiming that the information was received from or sent to another caller. The security goals impacted by this threat are integrity and accountability. One possible scenario for forgery is that an attacker may pretend to be a subscriber and receive calls intended for a legitimate subscriber with no intent to alert the caller, although they may falsely acknowledge that the request was completed. A different situation would involve a subscriber pretending to be the forged subscriber for issuing orders that may negatively impact the operational capabilities of the callee.

The final threat is a denial of service attack, which is typically associated with an attacker causing enough congestion on the network that a subscriber's calls cannot be completed or are degraded. In the converged networks planned for the DoD, this may involve either data or VVoIP type attacks. Of particular concern is a VVoIP attack that involves a high number of illegitimate above ROUTINE precedence calls preventing access to the network for legitimate above ROUTINE precedence VVoIP calls. A denial of service attack can occur at all three layers: signaling, bearer, or network management. The principal security goal affected by this type of attack is availability and this vulnerability is more likely to occur in a converged network.

The next step after identifying the threats is to perform a risk analysis of the threats. The method used in the ETSI TIPHON risk model is to score each threat in terms of its likelihood of occurrence and its potential impact. The Threat Risk Score is the product of the likelihood of occurrence and the impact scores. Table 5.4.3-2, ETSI TIPHON Threat Likelihood Scoring Criteria, and Table 5.4.3-3, ETSI TIPHON Threat Impact Scoring Criteria, are extracted from ETSI TS 102 165-1 and designate the scores that should be used for assessing the system risks.

Table 5.4.3-2 describes the scores that should be used for the likelihood of a particular threat.

Table 5.4.3-2. ETSI TIPHON Threat Likelihood Scoring Criteria

SCORE	LIKELIHOOD	DESCRIPTION
1	Unlikely	According to up-to-date knowledge, a possible attacker needs to solve strong technical difficulties to start the threat, or the motivation for an attacker is very low.
2	Possible	The technical requirements necessary to state this threat are not too high and seem to be solvable without big effort; furthermore, there must be a reasonable motivation for an attacker to perform the threat.
3	Likely	There are no sufficient mechanisms installed to counteract this threat, and the motivation for an attacker is quite high.

Table 5.4.3-3 describes the scores that should be used for the impact of a particular threat.

Table 5.4.3-3. ETSI TIPHON Threat Impact Scoring Criteria

SCORE	IMPACT	DESCRIPTION
1	Low	The concerned party is not harmed very strongly; the possible damage is low.
2	Medium	The threat addresses the interests of providers and subscribers, and cannot be neglected.
3	High	A basis of business is threatened and severe damage might occur in this context.

Following the ETSI TIPHON model, the risk associated with each threat is divided into three categories and all risks scoring a six or nine require countermeasures. Although risks scoring four do not require countermeasures, they are still considered major risks and the risk should be mitigated. It should be noted that the risk cannot score five, seven, or eight due to basic mathematics. Figure 5.4.3-1, ETSI TIPHON Threat Risk Score, shows the result of likelihood and impact scores on the overall risk score.

The UC IA team developed the initial scores and vetted the scores with the user community and industry. The scores are an average based on the feedback since every vendor's IA solution and every user's implementation is different.

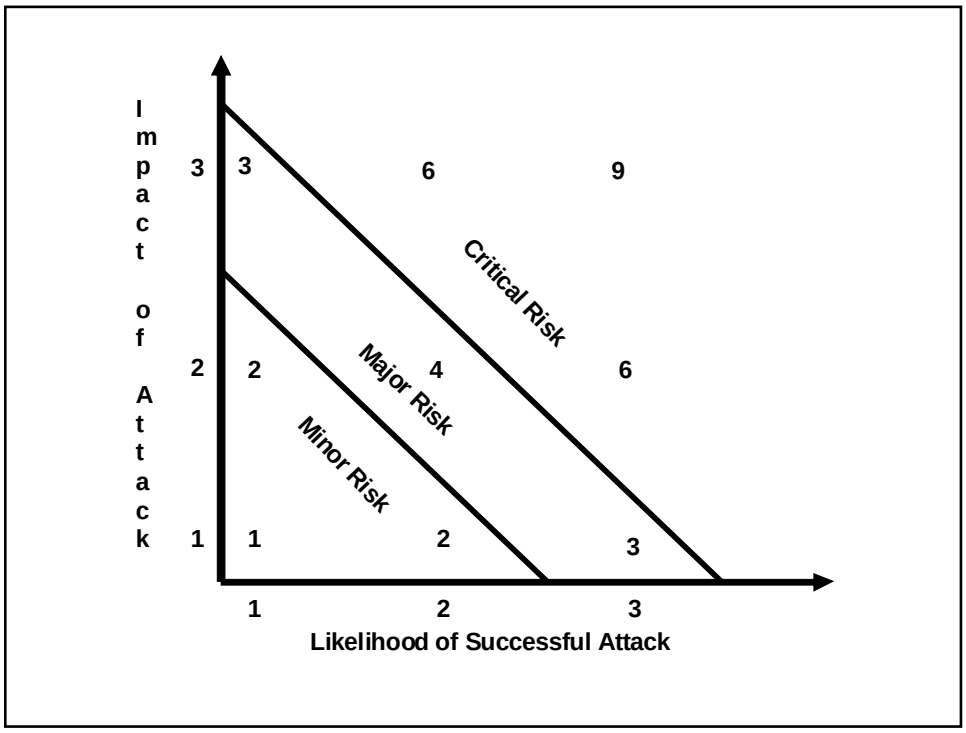


Figure 5.4.3-1. ETSI TIPHON Threat Risk Score

Tables 5.4.3-4 through 5.4.3-12 are extracted from the "Analysis of Information Assurance Requirements and Threats for the DoD Real-Time Services Environment," and summarize the risk assessments associated with the threats.

Table 5.4.3-4. General Threat Risk Assessment

ITEM	THREAT	LIKELIHOOD	IMPACT	RISK	COMMENT
G1	Eavesdropping on VVoIP subscriber transport data	2	2	4	Although the SBU voice service is a distinct network from the PSTN, most attacks do occur from inside the network. However, the impact is reduced due to the use of STU/STEs for classified conversations and the use of encryption for all calls.
G2	Corruption of transport data	2	3	6	A user who can eavesdrop on the transport data can manipulate the data stream to issue false orders or to make the communication unintelligible.
G3	Eavesdropping on a valid telephone number to determine its location or to masquerade	2	3	6	Encrypting all layers of the communication should reduce the likelihood. The ability to masquerade the telephone number makes the impact higher.
G4	Eavesdropping on the signaling data	3	3	9	SIP increases the likelihood of this attack and the information gained in this attack can be used to derive other attacks.
G5	Corruption of signaling data	2	3	6	SIP increases the likelihood of this occurrence and the modification of the signaling data could be used to derive other types of attacks or for a DoS attack.
G6	Eavesdropping on network management traffic	2	1	2	The large number of tools available on the Internet makes this task easier, but the impact is minimal.
G7	Corruption of network management data	3	3	9	The closed loop approach to signaling involving the routers would make the impact of this attack high to the voice or video.

ITEM	THREAT	LIKELIHOOD	IMPACT	RISK	COMMENT
G8	Obtaining telephone number from VVoIP end instrument	3	2	6	This information could be used to discern the origination of calls, which can be used by enemies as intelligence.
G9	Denial of service	3	3	9	This is particularly important to voice or video due to the need for assured service for precedence calls.
G10	Unauthorized access to data	1	3	3	The primary concern is unauthorized access to CDR. Nevertheless, the security in-depth approach employed minimizes the likelihood of this occurring.
G11	Flooding the network	3	3	9	Similar reasons to DoS attacks.
G12	Stolen terminals	3	3	9	In wartime and peacetime scenarios, it is likely that a terminal may be acquired by an enemy agent.
G13	Subscription fraud	3	1	3	Since the DoD is a military organization, this is not as critical since the profit is not the only factor in the solution. This does not mean that it is not important as relates to PSTN charges.
G14	Unauthorized access to network management or subscriber database	2	3	6	The prevention of the dissemination of the locations and sizes of units is critical to the safety of our forces.
G15	Unauthorized access to data in end instruments	2	1	2	The end instruments in the voice or video have limited usable data stored in them. If the end instrument stores private keys, then a possible threat is unauthorized access to the private key and additional related threats become possible.
G16	Masquerading as one legitimate subscriber or signaling device to another	3	3	9	In wartime and peacetime scenarios, it is likely that an enemy agent who gains access to the network will masquerade as a legitimate subscriber.

ITEM	THREAT	LIKELIHOOD	IMPACT	RISK	COMMENT
G17	Man-in-the-middle attack	3	3	9	Although this is an internal threat, the numerous shareware tools available to execute this attack make it likely and the impact is high due to the ability to redirect voice traffic and get access to user data.
G18	Repudiation of actions	2	2	4	The threat depends on the action taken and ability of the system to detect the action rapidly.
G19	Replay attack	1	2	2	This type of attack could be associated with command related actions, such as "launch all aircraft." These attacks apply to NM, signaling, and bearer streams.
G20	SIP Parser Attack	2	2	4	This attack could occur if an unauthenticated EI or SIP signaling appliance was allowed to connect to the network. Another avenue would include the manipulation of the SIP application to create a poorly organized SIP message that is difficult to parse
G21	SIP Registration or INVITE Flooding or DoS Attack	3	2	6	This attack could occur if an unauthenticated EI or SIP signaling appliance was allowed to connect to the network. Another avenue would include the manipulation of the SIP application to generate repetitive registration or INVITEs.
G22	Buffer Overflow Attack	1	3	3	The likelihood of this attack is small due to the requirement to mutually authenticate all signaling appliances. This attack is associated with malformed SIP messages causing the buffer to overflow.
G23	SIP INVITE	2	1	2	The SIP timers should clear this issue within approximately 32 seconds. In addition, this attack would only affect one phone at a time.
G24	SPAM over Internet Telephony (SPIT)	1	2	2	This attack would have to originate within the SBU voice due to the TDM constraint to the PSTN.

ITEM	THREAT	LIKELIHOOD	IMPACT	RISK	COMMENT
G25	Worms, Viruses, and Trojans	1	3	3	Remove applications that are not VVoIP related from VVoIP appliances. Install anti-virus software on appliances that have applications.

Table 5.4.3-5. Data Deletion Threat Risk Assessment

ITEM	THREAT	LIKELIHOOD	IMPACT	RISK	COMMENT
D1	Eavesdropping of old address	3	1	3	The likelihood is high due to the mobile nature of DoD subscribers. The risk is reduced by using non-global addressing.
D2	Masquerading as a subscriber to delete data	2	3	6	Once enemy agents gain access to the network they may, in addition to calling people, attempt to access the signaling data to disrupt the ability to place calls. However, the likelihood of this action is less than calling another subscriber.

Table 5.4.3-6. Subscriber Registration Threat Risk Assessment

ITEM	THREAT	LIKELIHOOD	IMPACT	RISK	COMMENT
SR1	Illegal registration by an attacker masquerading as a voice or video switch/appliance	1	1	1	Due to the use of TDM for the interface to the PSTN and other networks, the likelihood of this attack is minimal. The impact is also minimal since this would likely be detected very rapidly.

Table 5.4.3-7. Subscriber Registration Threat Risk Assessment

ITEM	THREAT	LIKELIHOOD	IMPACT	RISK	COMMENT
SD1	Illegal de-registration by an attacker masquerading as a voice or video switch/appliance	1	1	1	Due to the use of TDM for the interface to the PSTN and other networks, the likelihood of this attack is minimal. The impact is also minimal since this would likely be detected very rapidly.
SD2	Subscriber does not allow de-registration by manipulating the end instrument	2	1	2	The impact is minimal since the subscriber should be easily isolated using firewalls and other security mechanisms.

ITEM	THREAT	LIKELIHOOD	IMPACT	RISK	COMMENT
SD3	Subscriber does not allow de-registration by manipulating VVoIP server	2	3	6	This can inhibit the ability of the network to disable illegitimate users and is part of a DoS or flooding attack. SIP manipulation is possible using virus infection.

Table 5.4.3-8. Incoming Call Threat Risk Assessment

ITEM	THREAT	LIKELIHOOD	IMPACT	RISK	COMMENT
I1	Masquerading by using someone's ID	2	2	4	Since authentication is mandatory, the likelihood is low.
I2	Masquerading by using someone's ID and authentication	1	3	3	The design of the authentication mechanism should be sufficient to minimize the likelihood of an attack. However, if the mechanism is broken it makes a large segment of the network vulnerable.
I3	Eavesdropping of the communication on the access interface by use of a session key	1	2	2	Session keys have a shorter lifespan than the time it should take to break the key. The key is not sent in the clear, making it difficult to obtain.
I4	Eavesdropping at the start of a communication on the end instrument	2	1	2	This is possible if call setup is performed before the authentication is completed. Call transfers are also vulnerable to this due to the interval between a call transfer and the rekey.
I5	Modification of routing data	1	3	3	The impact is that data may be routed to bogus or enemy networks. The likelihood is low due to the defense in depth strategy required.

Table 5.4.3-9. Outgoing Call Threat Risk Assessment

ITEM	THREAT	LIKELIHOOD	IMPACT	RISK	COMMENT
O1	Masquerading using a subscriber's ID	1	2	2	This attack is associated with outgoing calls and the likelihood is minimized if authentication is required.
O2	Masquerading using a subscriber's ID and authentication	1	3	3	Authentication would be obtained by methods described elsewhere in this UCR 2008.
O3	Eavesdropping on the access interface by using a session key	1	2	2	Session keys have a shorter lifespan than the time it should take to break the key. The key is not sent in the clear making it difficult to obtain.
O4	Eavesdropping on the network	1	3	3	The use of encryption for all layers should minimize the likelihood of this event occurring.
O5	Eavesdropping on the start of a communication on the end instrument	2	1	2	This is possible if call setup is performed before the authentication is completed. Call transfers are also vulnerable to this due to the interval between a call transfer and the rekey.
O6	Eavesdropping on the phone number of a called party	2	1	2	This is possible if call setup is performed before the authentication is completed.
O7	Modification of the dialed number	2	3	6	This attack could result in a precedence call being forwarded to the wrong location.
O8	Masquerading using someone's ID	2	1	2	This is accomplished for the purpose of placing a short call prior to authentication.

Table 5.4.3-10. Emergency and Precedence Call Threat Risk Assessment

ITEM	THREAT	LIKELIHOOD	IMPACT	RISK	COMMENT
E1	Misuse of emergency call	3	1	3	An attacker would place a 911 or emergency call without reason to cause chaos during a crisis or attack. This is important if the authentication mechanisms are compromised or are not implemented for emergency calls. Normally, it would be associated with single sessions.
E2	Misuse of precedence calls	3	3	9	An attacker would place a precedence call without reason to a particular phone to deny that phones access to other calls. This is important if the authentication mechanisms are compromised.
E3	Manipulation of emergency database information	2	3	6	This could cause calls to be improperly sent to emergency numbers thereby tying up the circuits or sending the emergency calls to invalid destinations.
E4	Manipulation of precedence database information	2	3	6	The likelihood of this attack occurring is higher since this is a critical point of attack for an enemy agent.

Table 5.4.3-11. Survivability Threat Risk Assessment

ITEM	THREAT	LIKELIHOOD	IMPACT	RISK	COMMENT
S1	A node in the network is destroyed or disabled	3	3	9	This is a situation very likely in the DoD environment
S2	A device in the network is disabled or destroyed	3	3	9	Many times an attacker will be able to disable one device before the attacker is detected

Table 5.4.3-12. Risk Summary

RISK LEVEL	NUMBER OF RISKS	RISK SCORE
Critical Risks	22	6,9
Major Risks	13	3,4
Minor Risks	16	1,2
Total	**51**	

As seen in Table 5.4.3-12, Risk Summary, approximately half of the risks are categorized as critical and require countermeasures. Thirteen risks were categorized as major risks and the risk should be minimized. Although the other risks are minor, they are still risks that require mitigation and will need to be addressed in the IA design. The Risk Summary Table is repeated at the end of this section, and it shows the mitigated scores based on the full implementation of the VVoIP IA design.

5.4.4 VVoIP Generic Countermeasures

In "Analysis of Information Assurance Requirements and Threats for the DoD Real-Time Services Environment," a set of threats and requirements for the DoD VVoIP environment, was identified and these threats were summarized in the preceding paragraphs. A complete discussion of the countermeasures is provided in "DoD RTS IA Countermeasures." This section describes the process used to develop the countermeasures required of the DoD VVoIP environments based on those threats and requirements and summarizes the generic countermeasures developed to mitigate the threats. The first step in the process is to develop an initial set of recommended countermeasures that tentatively mitigate the threat to an acceptable level.

5.4.4.1 Recommended Countermeasures

The recommended countermeasures were developed using an iterative process involving the vendor and DoD communities to mitigate the threats associated with a DoD VVoIP environment. The countermeasures are presented in a generic manner to ensure they do not mandate a technical solution, and are provided as part of the systems engineering process for developing the IA design. There is no intent to mandate a countermeasure on an appliance or system and they should not be considered requirements. The system design, and its associated requirements, will define the technical solution for the system and its appliances and a specific countermeasure may or may not be used dependent on the design. As mentioned previously, the threats associated with ancillary services and TDM technologies have not been addressed completely. Therefore, the countermeasures described below do not address the threats associated with ancillary equipment and TDM technologies completely. An update to UCR 2008 will address those deficiencies. Prior to discussing the countermeasures, it is important to define the terms used in the discussion.

1. Registrant. An appliance, which is used to register with the network to seek and gain authority to invoke services or resources from the network. Registrants are typically associated with primary and alternate registrars. Examples of registrants are EIs, EOs, PCs, and LSCs.

2. Registrar. The appliance that stores the location of a registrant and its profile. The profile is used to define the services to which a registrant is authorized (or a user via the registrant). In the DoD VVoIP environment, examples of the registrar include LSCs and DoD Public Key Infrastructure (PKI) servers. A registrar may reside on the same appliance and be integrated with a Service Point of Attachment (SpoA).

3. Service Point of Attachment . A SpoA is an appliance to which a registrant establishes a session over the IP network or TDM network. The session may be established to pass signaling or network management traffic. In the DoD VVoIP environment, examples of a SpoA are LSCs, MFSSs, softswitches (SSs), directory servers, or gateways.

4. Transport Point of Attachment (TpoA). A TpoA is an appliance that is used to provide transport of a session over a network. Examples of transport appliances in the DoD VVoIP environment include routers, LAN switches, firewalls, EBCs, MFSS, and gateways.

Figure 5.4.4-1, Interaction between VVoIP IA Components, shows the interactions between the different countermeasure elements.

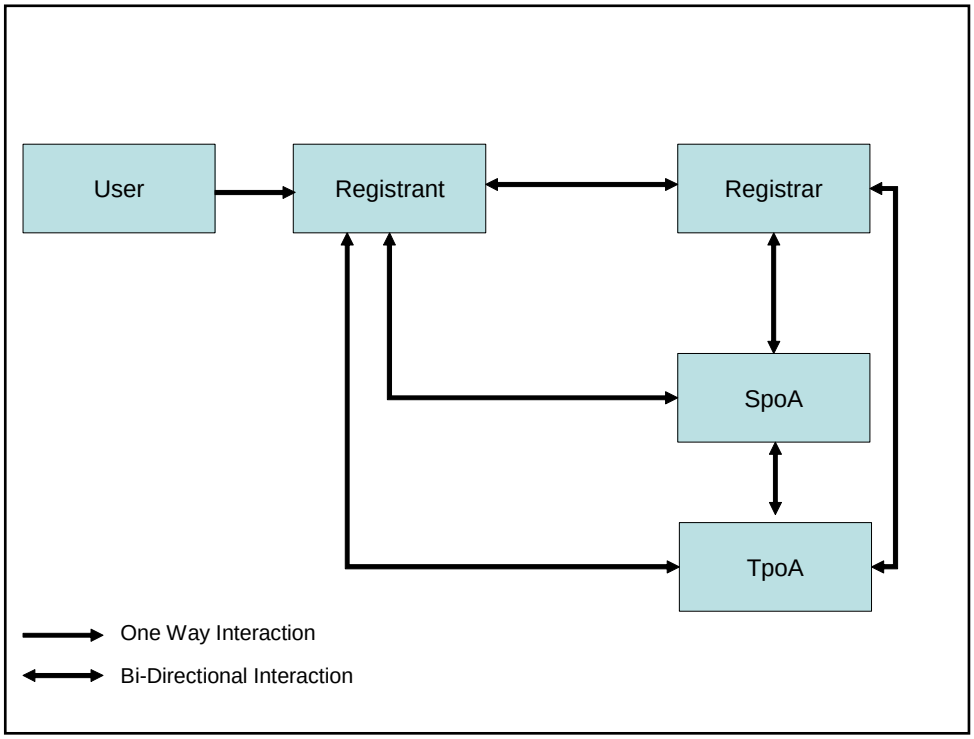


Figure 5.4.4-1. Interaction between VVoIP IA Components

5.4.4.2. Access Control Countermeasures

1. C1 – Access Control to Services. The system should validate, based on prior authentication, the privileges to which a user has authorization before granting access to services.

2. C2 – Access Control to Database. The system should validate, based on prior authentication, the privileges to which a user has authorization before granting access to a database.

3. C3 – Access Control to Sensitive Information in EI. The system should validate, based on prior authentication, the privileges to which a user has authorization before granting access to sensitive information stored on an EI.

4. C4 – Access Control to System Software. The system should validate, based on prior authentication, the privileges to which a user has authorization before granting access to the system software. This software includes the software needed to provide VVoIP as well as the operating system software.

5. C5 – Access Control to System Hardware. The system should control access to the use of system hardware from users who are not authenticated.

6. C6 – Access Control to System Resources. The system should protect system resources from users who are not authenticated.

7. C7 – Access Control between Network Resources. The system should protect one network resource from another network resource unless there is a defined requirement for those resources to interact.

5.4.4.3 Authentication Countermeasures

1. A1 – Authentication of the EI by the Registrar. The EI should contain a unique identity that identifies the EI to the registrar and authentication should confirm this identity through proof of knowledge of a secret shared by the registrar and the EI or by the use of a public key cryptosystem. This countermeasure is the corollary of A2.

2. A2 – Authentication of the Registrar by the EI. The Registrar should contain a unique identity that identifies the registrar to the EI and authentication should confirm this identity through proof of knowledge of a secret shared by the registrar and the EI or by the use of a public key cryptosystem. This countermeasure is the corollary of A1.

3. A3 – Authentication of the EI by the SpoA. Prior to providing service to the SpoA, the SpoA should authenticate the EI. This countermeasure is the corollary of A4.

4. A4 – Authentication of the SpoA by the EI. Prior to transmitting to a SpoA, the EI should authenticate the SpoA to ensure that it is the actual SpoA assigned by the registrar. This countermeasure is the corollary of A3.

5. A5 – Authentication of the SpoA by the Registrar. The registrar should authenticate the SpoA prior to directing an EI to use that SpoA. This authentication should be based upon a secret shared by the registrar and the SpoA. This countermeasure is the corollary of A6.

6. A6 – Authentication of the Registrar by the SpoA. The SpoA should authenticate the registrar requesting service prior to granting that service. The authentication should be based upon a secret shared by the registrar and the SpoA. This countermeasure is a corollary to A5.

7. A7 – Authentication of the User to the Appliance. The user should authenticate to the appliance to protect against misuse. This countermeasure does not have a corollary.

8. A8 – Authentication of the SpoA by the TpoA. Prior to transmitting to a SpoA, the TpoA should authenticate the SpoA to ensure that it is the actual SpoA to which it is assigned. This countermeasure is the corollary of A9.

9. A9 – Authentication of the TpoA by the SpoA. Prior to transmitting to a TpoA, the SpoA should authenticate the TpoA to ensure that it is the actual TpoA to which it intends to transmit. This countermeasure is the corollary of A8.

10. A10 – Authentication between SpoAs. Prior to transmitting to a SpoA, the SpoA should authenticate the other SpoA to ensure that it is the actual SpoA to which intends to transmit. This countermeasure does not have a corollary.

11. A11 – Authentication between TpoAs. Prior to transmitting to a TpoA, the TpoA should authenticate the other TpoA to ensure that it is the actual TpoA to which intends to transmit. This countermeasure does not have a corollary.

5.4.4.4 Non-Repudiation Countermeasures

N1 – Non-Repudiation of User Modifications to Appliance Resources. The appliances should ensure that non-repudiation is associated with any modifications made to an appliance's resources to include the operating system, files, applications, or databases.

5.4.4.5 Data Confidentiality Countermeasures

1. E1 – Confidentiality of User Communication on the EI. The system should provide confidentiality for bearer stream at the EI for originating and terminating sessions.

2. E2 – Confidentiality of Signaling on the EI. The system should provide confidentiality for the signaling stream at the EI for all originating and terminating sessions.

3. E3 – Confidentiality of Signaling between SpoAs. The system should provide confidentiality for the signaling between SpoAs. Signaling may include session keys, call-forwarding numbers, network management traffic, and personal data.

4. E4 – Confidentiality of Signaling between SpoA and TpoA. The system should provide confidentiality for sessions between the SpoA and the TpoA. The signaling may consist of signaling or network management traffic. This may be accomplished using physical protection or cryptographic protections.

5. E5 – Confidentiality of Communication between TpoAs. The system should provide confidentiality for sessions between TpoAs. The communication between TpoAs may consist of signaling or network management traffic. This may be accomplished using physical protection or cryptographic protections.

6. E6 – Confidentiality of Communication between SpoA and Registrar. The system should provide confidentiality for sessions between SpoAs and registrars. The communication may consist of signaling or network management traffic. This may be accomplished using physical protection or cryptographic protections.

7. E7 – Confidentiality between User and Appliance. The system should provide confidentiality for sessions between an authenticated and authorized user and an appliance for network management purposes.

8. E8 – Confidentiality of Data at Rest. The system should provide confidentiality for data at rest. The data may be stored in a file or a database.

5.4.4.6 Data Integrity Countermeasures

1. I1 – Signaling Integrity. The system should ensure integrity for signaling messages. Types of signaling messages include SIP, H.323, and routing updates.

2. I2 – Bulk Data Transfer Data Integrity. The system should ensure integrity for bulk data transfers. Bulk data transfers include call detail records (CDRs).

3. I3 – Appliance Data Integrity. The system should ensure the integrity of data written, read, or stored on an appliance.

4. I4 – Appliance System Integrity. The system should ensure the integrity of the operating system and the applications on the appliance. This shall include unauthorized operating system or application modifications.

5. I5 – End Instrument Transport Integrity. The system should ensure the integrity of the bearer packets transmitted between the end instruments.

5.4.4.7 Survivability/Availability Countermeasures

1. S1 – Diversity of Network Connections. The system should ensure high availability using diverse geographical distinct connections for designated locations throughout the network. In addition, the connections should be diverse from both physical and logical perspectives. Sites that require diverse geographic distinct connections are typically C2 sites. However, non-C2 sites sometimes require diverse connectivity dependent on the mission and network topology.

2. S2 – Redundancy of Hardware and Software. The system should have sufficient redundancy in hardware and software to ensure that the required availability is achievable based on the computed failure rates for the hardware and software.

3. S3 – Out-of-Band Network Management Capability. The system should have an out-of-band network management capability for use during network outages or for when network resources are not reachable during IA attacks.

4. S4 – System Power Redundancy. The system should have sufficient backup power for use during power failures based on its usage and user requirements

5.4.4.8 Miscellaneous Countermeasures

Some countermeasures overlap many assurance categories and they are classified as miscellaneous countermeasures.

5.4.4.9 Privacy Countermeasures

1. P1 – Physical Security. The system infrastructure should be placed in a secure facility that only permits access by authenticated and authorized personnel.

2. P2 – Personal Data Security. Personally Identifiable information (PII), especially Social Security Numbers, in the system infrastructure should be minimized to the maximum extent possible. Where present, the PII should be protected in accordance with DOD information assurance and privacy policy and guidelines.

5.4.4.10 Network Management Countermeasures

M1 – Threshold Exception Management System Notification. The system should notify a designated network management system when predefined thresholds are exceeded. A threshold may consist of a single event (e.g., an audit log failure) or multiple events (e.g., multiple failed login attempts).

After developing the countermeasures, the next step in the IA Process was to develop an VVoIP IA design that implements these countermeasures. Based on that design a set of requirements was derived. An iterative process was used due to the many interdependencies involved.

5.4.5 VVoIP IA Design

5.4.5.1 Physical Security

Physical security for a VVoIP system is the responsibility of the installing B/P/C/S. There are essentially two sets of requirements associated with a complete VVoIP system. The EIs have one set of physical security requirements while the network (LAN switches and routers) and signaling products (i.e., LSC, MFSS, SS, MG, etc.) require another set of requirements. A full definition of physical security requirements is beyond the scope of this section of the UCR 2008.

The EIs of a VVoIP product are located in many different types of facilities. Their physical security is dependant upon the physical security afforded by the facility in which they are housed. The physical security of the facility is dependant upon the sensitivity and/or classification of the information that it contains or processes.

The physical security for the VVoIP product network infrastructure and signaling appliances must limit physical access to all the associated appliances and cable terminations. Sensitivity and/or classification of the product have no bearing on this requirement. This means that the supporting infrastructure for the total product must reside, minimally, behind locked doors. Again, as with the EIs, this is typically afforded by the facility in which the equipment/ infrastructure is housed (e.g., locks and/or access control on doors of rooms and closets housing the equipment). This may, however, be minimally provided by a lock on a cabinet housing a LAN switch in the open (i.e., unsecured area).

Facility security requirements fall under the purview of "DoD Traditional Security." These requirements are well beyond the scope of the UCR 2008. A subset of these requirements will be included in a future release of the RTS STIG.

Vendors must support their customer's need to comply with the DoD system physical security requirements for VVoIP products. This support is to be provided in the form of locking kits for any equipment that the vendor normally provides in a cabinet. If a cabinet lock is not provided normally in the vendor's commercial offering, optional locking kits must be made available that work well with the vendor's cabinet. All cabinet locking mechanisms must be robust enough to resist prying the cabinet open.

5.4.5.2 VVoIP Appliance Security Design

The VVoIP product security design uses a defense in-depth approach that is based on best commercial practices. The product security defenses are categorized as follows and discussed in the following paragraphs:

- User Roles
- Hardened Operating Systems
- Auditing
- Application Security
- Redundant Systems

Additional defenses may be added dependent on the specific threats associated with a product.

5.4.5.2.1 User Roles

There are three types of users related to a VVoIP product, which are segmented into two different categories; users of the system services and administrative users of the product. This becomes confusing due to the unqualified and repeated use of the word "user." One must be aware of, and remember what area of the product is being discussed (i.e., its services or its administration, configuration, or maintenance) in order to be sure of the context of the word.

Essentially, a user of product services has one role. He or she uses the services that the product provides and they are referred to in this UCR 2008 section as application users. Such a user may be a "privileged application user" who has permission to use certain restricted services, such as the ability to initiate a FLASH precedence session. Such a user may be required to authenticate to the product in some fashion (such as entering a PIN code to identify the user (called User-ID) and a different PIN (called password) to authenticate the user) in order to receive access to their "privileged" service. There may be multiple levels of privileged service, which might be considered "service user roles" by some readers.

Administrative users are those users that are tasked with the configuration, operation, or maintenance of the system. These users are usually referred to as system administrators. System administrators fulfill different roles based on their duties, responsibilities, or job description/ function. DoD policy requires that system administrators receive only those system privileges or access to commands that are required to perform their duties (i.e., fulfill their role). System administrators who are limited to selected applications on the system are designated application administrators.

System administrators receive their privileges or access to commands based upon Discretionary Access Control (DAC), which provides authorization control. Discretionary Access Control is a role-based feature that grants a system administrator specific permission to perform various functions when accessing the product. Such permissions are established in accordance with the job functions and responsibilities (role) of the individual. Permissions are established by the responsible security officer (i.e., the Information Assurance Officer (IAO) or system security administrator), and stored in the system memory or its configuration files. The security officer also establishes the relationship in the system between authorized command class(es) or group(s).

Products that are developed with various levels of authorization or command access must support DAC requirements. This can be achieved by user privileges or group privileges. The methods to access resources may vary depending on hardware and software products.

Examples of system administration roles are as follows:

1. Tier 3 Engineer (Troubleshooter – Initial Support). This role may only have privileges and access to commands that allow him/her to view operational statistics, alarms, and some specific level of appliance or system configuration. This role may not have the ability to change any configuration settings. This could be considered Tier 3 support.

2. Tier 2 Engineer. This role would have all the capabilities of the troubleshooter role with the added privileges and access to certain commands that allow him or her to make some but not all configuration changes.

3. Tier 1 Engineer. This role would have privileges and access to all commands for troubleshooting and system configuration.

4. Provisioner/Administrator. This role may only have privileges and access to commands that allow him/her to provision circuits, configure end instruments and/or features. This role may have the ability to troubleshoot some aspects of the system.

Another scenario is the case of a database administrator or application administrator role that only has rights to access the database or application that they manage but does not have rights to access the administration of the operating system on the platform that support one or more databases or applications.

Similar roles or levels of privilege and DAC to those described above are required for DoD information systems. These equate to the normal system administrator roles. The granularity of DAC provided is dependent on the capabilities of the specific system being managed.

The third type of user required for DoD systems is the Auditor, which is short for Security Auditor. This role has none of the normal system administrator privileges or access. The normal system administrator role does not have access to auditor level commands. The auditor role only has access to commands related to the security or audit logs, and is associated with the system security administrator.

5.4.5.2.2 Hardened Operating Systems

Multipurpose or general-use operating systems are delivered with none, or a minimal number, of security features enabled. Access to critical areas of the operating system as well as application and data files is sometimes unrestricted. Additionally, some of these operating systems are delivered with inherent security vulnerabilities, both known and undiscovered. The process of "hardening" an operating system is the process of restricting access to those system areas and functions that could be detrimental to the security of the system and mitigating the known and/or discovered security vulnerabilities. The implementation guidelines associated with common operating systems are found in the STIGs developed for the operating system and are different for every operating system.

5.4.5.2.3 Auditing

In this UCR 2008 section, auditing refers to the logging and analysis of security related events. Auditing and recording the events occurring to or within a appliance of the APL product is critical to maintaining accountability. This is accomplished by tracking security and configuration related changes, which provides the system security administrator or IA manager vital information to reconstruct what may have occurred prior to a system crash or other situation. Security auditing is necessary for the reconstruction of system events that have led to a security incident in support of disciplinary action or prosecution. This information may also allow the system manager to restore a system to its correct configuration and to determine the cause of the problem. The term "history file" may or may not relate only to security. Some systems such as telecommunications appliances record every transaction performed by the appliance. History files may or may not contain auditable security events. A determination must be made for each appliance regarding the location of the security audits. Appropriate security

record events must be captured, recorded, retrieved, protected, reviewed, and archived on a regular basis.

The DoDI 8500.2 is the primary driver of auditing requirements. The DoDI 8500.2 IA control Enclave and Computing Environment Audit Trail Protection-1 (ECTP-1) states:

> "The contents of audit trails are protected against unauthorized access, modification or deletion."

DoD requirements also state that all system and network devices perform security auditing and that auditing records are placed in an unalterable audit or history file that is available only to those individuals authorized to analyze system or network appliance access and configuration activity. This implies that the audit log must be separate from any other system logs.

The DoDI 8500.2 states the following regarding audit record content:

Audit records include:

Enclave and Computing Environment Audit Record Content-1 (ECAR-1); Base level for information sensitivity = public

- User ID.
- Successful and unsuccessful attempts to access security files
- Date and time of the event.
- Type of event.

Enclave and Computing Environment Audit Record Content -2 (ECAR-2); Adds items for information sensitivity = sensitive

- Success or failure of event.
- Successful and unsuccessful logons.
- Denial of access resulting from excessive number of logon attempts.
- Blocking or blacklisting a user ID, terminal or access port, and the reason for the action.
- Activities that might modify, bypass, or negate safeguards controlled by the system.

ECAR-3; Adds items for information sensitivity = classified

- Data required to audit the possible use of covert channel mechanisms.
- Privileged activities and other system-level access.
- Starting and ending time for access to the system.
- Security relevant actions associated with periods processing or the changing of security labels or categories of information.

The above DoD 8500.2 requirements are mapped, interpreted, and augmented with best practice, as shown below.

At a minimum, the following events are to be audited on the system and network devices:

- Logons and logouts
  - Starting and ending time for access to the system.
- Excessive logon attempts/failures
  - Denial of access resulting from excessive number of logon attempts.
  - Blocking or blacklisting a user ID, terminal or access port, and the reason for the action.
- Remote system access
- Change in privileges or security attributes
  - Activities that might modify, bypass, or negate safeguards controlled by the system.
- Change of security levels or categories of information
  - Security relevant actions associated with periods processing or the changing of security labels or categories of information.
- Failed attempts to access restricted system privilege levels or data files

- Audit file access
- Password changes (not the passwords)
- Device configuration changes
  - Privileged activities and other system-level access.
- Other
  - Data required to audit the possible use of covert channel mechanisms."

At a minimum, the following information is recorded in the audit log for each event that is audited:

1. Date and time of the event
2. Origin of the request (e.g., terminal/workstation ID, port ID, IP address, etc.)
3. Unique ID of the user who initiated the event
4. Type of event
5. Success or failure
   a. Success or failure of event.
   b. Successful and unsuccessful logons.
   c. Successful and unsuccessful attempts to access security files
6. Description of modification to configurations

NOTE: A vendor's system, appliance, or product should support the audit requirements for classified products so that they can be purchased for use in classified systems. There may be additional requirements that it will need to meet.

DoD 8500.2 also requires that audit logs be:

> "…regularly reviewed for indications of inappropriate or unusual activity" (ECAT-1) on MAC-3 and/or systems processing sensitive and public information. Additionally, for MAC 1 and 2 and/or systems processing classified information it states, "An automated, continuous on-line monitoring and audit trail creation

> capability is deployed with the capability to immediately alert personnel of any unusual or inappropriate activity with potential IA implications, and with a user-configurable capability to automatically disable the system if serious IA violations are detected (ECAT-2). These requirements indicate that they are to be reviewed regularly and additionally for classified and/or mission critical systems, auditing should generate alarms to 'immediately alert personnel' of security issues."

The process of auditing security events can generate large volumes of data on busy systems. For this reason, audit logs are to be retrieved or removed from the system on a regular basis. Since audit logs contain information that may be required in support of administrative or prosecutorial actions, they must be protected. In some cases (i.e., Windows based systems), audit log protection is provided by halting the system operation if the audit capability fails.

DoD 8500.2 ECRG-1 states:

> "Tools are available for the review of audit records and for report generation from audit records."

The tools that are referenced are software tools provided by the vendor that can interpret the vendor's audit log file format to allow offline viewing and analysis of the logs, as well as the generation of report VVoIP from the data contained therein.

5.4.5.2.4 Application Security

DoD application security requirements are based on and are implemented in accordance with DoD IA policy requirements. These requirements are detailed in the DoD Application Security Checklist and DoD Application Development STIG. Basic application security requires that the application must not alter the security posture of the supporting operating system or other applications on the platform. In addition, applications must not change operating system files. Applications may rely on the operating system for some IA functions or may include some or all IA enablement features in the application. Applications that provide management capabilities of a system should be IA enabled. These applications should provide, at a minimum, for identification, authorization, roles/command classes, and auditing in accordance with the documents mentioned previously in this section.

5.4.5.2.5 Redundant Systems

Products that support critical services, such as voice communications, should be designed with enough redundancy to prevent single point of failure issues that could affect more than a threshold number of endpoints. This is partially driven by the percentage of "uptime" that is targeted for the overall system. Every critical product function should have a backup. This

includes power distribution, signaling appliances, other critical servers, core LAN hardware (routers and switches), boundary hardware (EBCs and CE Routers), and data links. A certain level of redundancy is appropriate. The core and distribution segments of a LAN, for example, should be redundant. The uplinks to the access segment switches should be redundant also. Redundancy for access segment switches and the distribution cabling to the endpoints does not make sense. One design concern is that if the access segment switch supports more than the threshold number of voice endpoints, which is typically driven by the Telcordia Technologies GR-815-CORE reliability requirements, then it is recommended that the endpoints be split among different switches. If this cannot be done, the switch should have redundant processors and power supplies.

It is beyond the scope of this section to define every item that needs to be redundant. This determination must be made based on good design criteria and best commercial practices. Nevertheless, UCR 2008, System Quality Factors section specifies many requirements associated with redundancy, and these should be used as a requirement baseline for the systems to which the documents apply.

5.4.5.3 VVoIP Component Interactions

One of the principal tenets of any IA Design is the separation of components (i.e., traffic, appliances, and users) and/or services from each other based on their characteristics. Still, a converged network requires the opposite in that appliances within a converged network may service the voice, data, and video applications. As a result of this conflict, the interactions between the various component segments must be controlled to ensure that an attacker that gains access to one segment does not gain access to, nor can affect, the other segments. In addition, interaction control between various segments is also used to prevent configuration or user errors in one segment from impacting other segments. The actions of normal users of converged network services must not affect the other services, more specifically the voice service. The principal mechanisms that are used within this design for segmenting the network are Virtual LANs (VLANs), segmented IP address space or subnets, and Virtual Private Networks (VPNs) and are used in combination with filters, access control lists (ACLs), and stateful packet inspection firewalls (VVoIP Stateful Firewalls) to control the flow of traffic between the VLANs and VPNs.

Figure 5.4.5-1, Notional Example of Voice and Data ASLAN Segmentation, presents the simplest type of converged LAN with only voice and data applications. Separate VLANs are established between voice and data applications and the Layer 3 switches are responsible for providing access control between the different VLANs using filtering techniques, such as ACLs. In this type of deployment, appliances are classified as VVoIP appliances or data appliances and it may be possible to avoid deploying appliances that service both VVoIP and data appliances. At the CE Router, separate VPNs may be established, if necessary, to segment the voice traffic

from the data traffic as the packets transit the DISN WAN. In addition, VPNs may be used to extend the local enclave to remote offices of the same organization, telecommuters, and travelers. Also, the VVoIP traffic is routed from the CE Router to the PE Router along the same path as the non-VVoIP traffic. The only connection to the PSTN is through a TDM interface using PRI or CAS signaling so that there is not interaction between the VVoIP system and commercial VVoIP IP networks. Moreover, it is important to note that the LSC has two separate interfaces; one for local network management and a second for the VoIP end-to-end network management traffic.

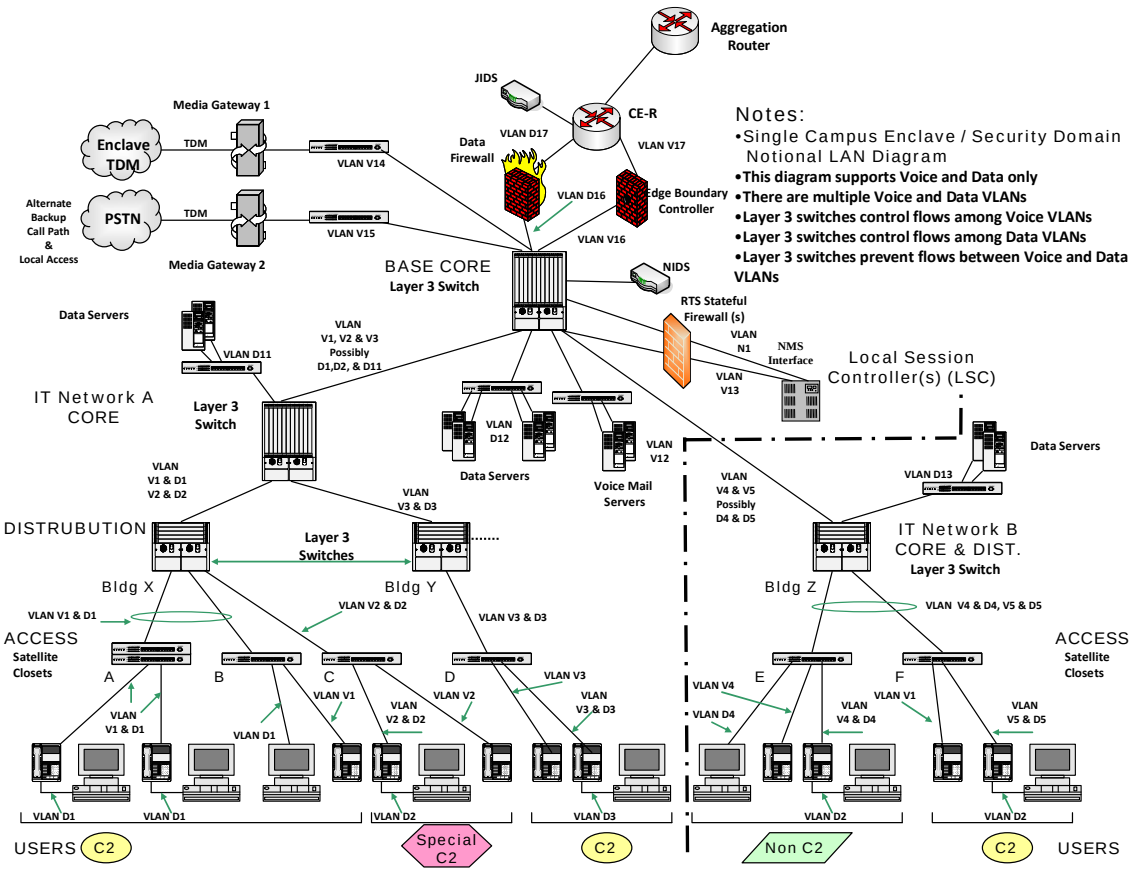


Figure 5.4.5-1. Notional Example of Voice and Data ASLAN Segmentation

The 802.1Q VLAN tagging of the packet for the appropriate VLAN should occur at the appliance, but may occur at the first LAN switch if the appliance is not capable of 802.1Q VLAN tagging. To comply with this, the ASLAN permits port-based and MAC-based VLAN tagging. If the EI supports a subtended data computer/workstation, it must perform several unique functions. The first function is that it should be capable of VLAN tagging the data traffic with a different VLAN tag than the voice traffic. In addition, it must be capable of routing the VVoIP traffic and the data traffic to the appropriate VLAN. The objective of this function is to

ensure that the data applications on the workstation do not have visibility to the voice related packets.

A more complex design involves appliances that support multiple types of applications like softphones and videophones. Figure 5.4.5-2, Notional Example of Voice, Video, Softphone, Videophone, and Data ASLAN Segmentation, shows the VLAN segmentation associated with this complex design. To simplify the design, all voice, video, and data sessions associated with a VTC are VLAN tagged (and DSCP marked) as a video session. In the case of videophones, the videophone may be used for voice or video applications. In this case, the audio and video traffic from the videophone may reside in the voice VLAN(s). The VTC only systems, desktop or room size, should have their own VLAN and addressing structure.

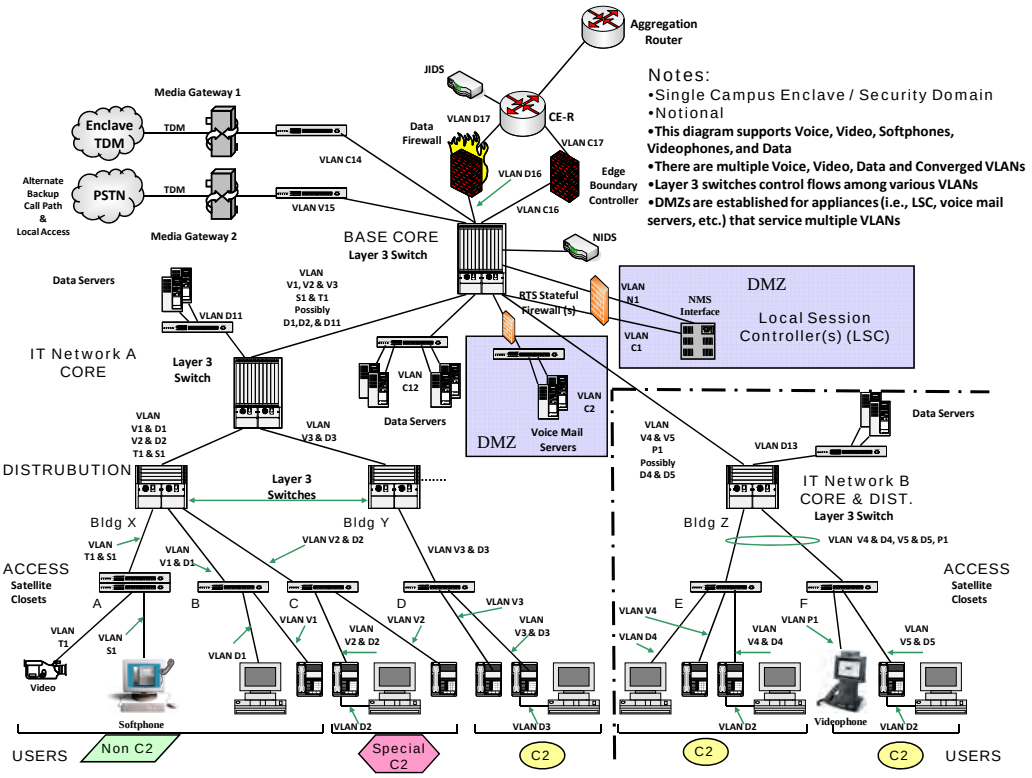


Figure 5.4.5-2. Notional Example of Voice, Video, Softphone, Videophone, and Data ASLAN Segmentation

Demilitarized zones are created for appliances that must service multiple segments of the converged network. An example is the LSC, which must service voice, video, videophone, and softphone appliances. Since access control between the various VLANs is significantly more complex, filtering is not adequate to achieve this goal and VVoIP stateful firewalls are needed to ensure that only authorized packets are able to transit the VLAN boundaries. The stateful firewall may have the complete functionality of an EBC, but this is not required.

In addition, if the softphones are used in remote connectivity situations, such as for a long local for a tactical deployed system, the system must be capable of supporting a VPN for VVoIP traffic from the PC to the LSC. It is essential that the data and VVoIP traffic must be separated into the appropriate VLAN at the earliest point in the path. In the long local scenario for a tactical user, this separation would likely occur at the Teleport facility.

Finally, an alternative not shown in the diagrams involves an LSC that has separate interfaces for the H.323, AS-SIP, and network management traffic. In this scenario, the ASLAN should have an H.323 VLAN, an AS-SIP VLAN, a data VLAN, and a network management VLAN as a minimum. Each network will typically have unique requirements and topology, and the VLANs implemented will depend on the local network needs.

Each of the following represents a separate VLAN:

1. VoIP EIs (multiple VLANs recommended for large sites)*

2. VoIP LSCs, SSs, and configuration servers*

3. Separate VLANs for other voice/VVoIP related servers

    a. Voice mail or unified messaging (voice mail and e-mail)*
    b. Computer Telephony Integration (CTI)
    c. Automatic Attendant/Call Director (ACD)
    d. Call center or operator's systems
    e. Emergency messaging system servers
    f. Multipoint controllers for conferencing: VTC and/or audio only
    g. Streaming video servers (video streams share the data VLANs)

4. Media Gateways*

    a. VoIP EIs that are part of a CTI, ACD, or call center/operator's system

5. VoIP EIs that have an integrated VTC capability

    a. VoIP and VTC video can share the same VLAN
    b. Multiple VLANs recommended for larger sites

6. Stand-alone desktop VTC units

    a. Units associated with and/or controlled by the VoIP LSC can reside in the VoIP EI VLAN(s).

b. Workstations running softphone applications (DAA Approved)*

c. Workstations running Desktop VTC applications (DAA Approved)

7. Collaboration tools: The VTC portion should use the appropriate VVoIP VLAN(s) if technically feasible while the data applications (e.g., whiteboard, file sharing, etc.) must use the data VLAN(s).

NOTE: Items marked with an asterisk (*) are currently required in the VoIP STIG.

Figure 5.4.5-3, Component Interaction Flow Diagram, provides a different depiction of the interactions between various VLANs within a B/P/C/S. The illustrations in this section are notional and address the scenario where ancillary services are internal to the system. The information is only provided as reference material and each B/P/C/S will determine its VLAN needs and boundaries based on its tailored requirements and security profile.

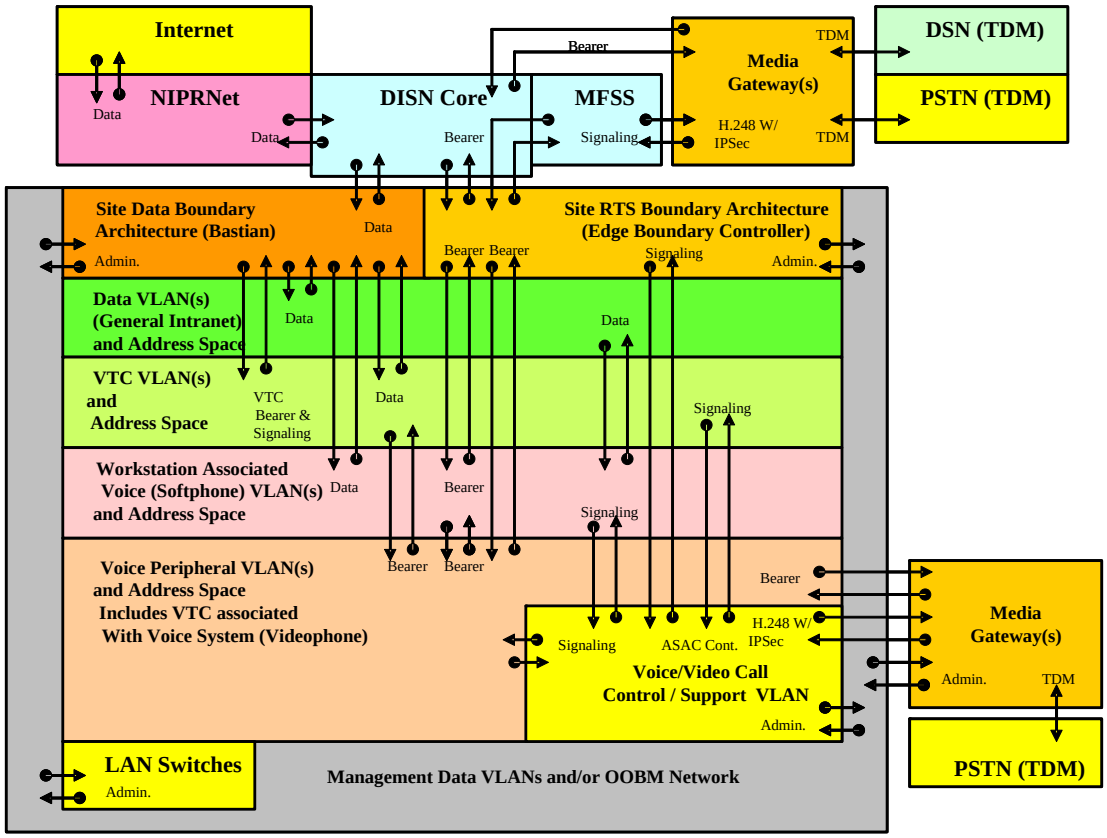


Figure 5.4.5-3. Component Interaction Flow Diagram

5.4.5.4 VVoIP Protocol Design

5.4.5.4.1 Overview

The VVoIP protocol Design consists of a combination of standards based protocols and proprietary based protocols. Within an APL Product the vendor is allowed to implement proprietary protocols for signaling (e.g., between the End Instrument and the LSC or between the LSC and the Media Gateway), but standards-based protocols are required for interfaces to external network management, signaling and transport appliances. Every proprietary protocol must be secured in a manner that is at least as secure as can be achieved using a standardized protocol. For instance, the VVoIP design mandates the use of Transport Layer Security (TLS) with Assured Services Session Initiation Protocol (AS-SIP) to provide confidentiality and integrity. AS-SIP, in combination with TLS, could be used for the signaling between the EI and the LSC, but is not required. Since every proprietary protocol must be secured in a manner that is at least as secure as can be achieved using a standardized protocol, if a vendor chooses to use a proprietary protocol for that interface, it must be as secure as that which can be achieved by using AS-SIP with TLS. Figure 5.4.5-4 presents the different protocols that are allowed in the VVoIP system and discriminates between interfaces that permit proprietary protocols and ones that require standardized protocols.

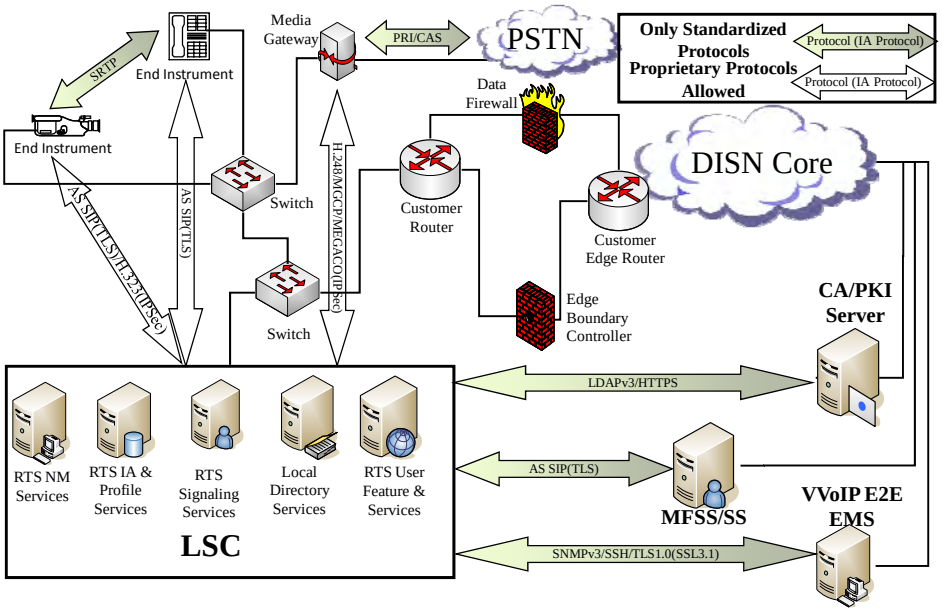


Figure 5.4.5-4. VVoIP Proprietary and Standards Based Protocols

Independent of the protocol or cryptographic algorithm used, many common IA mechanisms are required of all appliances. For example, every VVoIP signaling appliance that performs a cryptographic function must use a cryptographic module that is FIPS 140-2 level 1 compliant. In addition, the default encryption algorithm for the VVoIP system is the Advanced Encryption Standard (AES) algorithm with 128-bit encryption unless the protocol does not support AES, in which case the encryption algorithm selected must use 128-bit encryption as a minimum. The default hash is the Secure Hash Algorithm (SHA) – 1, which is supported on every protocol used in this system. In compliance with DoD requirements and policies, most VVoIP appliances will also be Public Key Enabled (PKE) so that they may interoperate with the DoD PKI with the exception of the EI for which the PKE requirement is an objective requirement for FY08 and will become required in FY12.

5.4.5.4.2 End Instrument Authentication and Registration

The first step in the VVoIP protocol design is the registration of the appliance to the network and its receipt of an E.164 telephone number if it is an EI. During the initial installation of an appliance either it will be configured with a static IP address (i.e., LSC, SS, MG, MFSS, and EI) or will receive its (EI) IP address from a Dynamic Host Configuration Protocol (DHCP) server. If DHCP is used, the EI shall also authenticate itself to the LAN switch to which it is physically connected using the 802.1X protocol. The DHCP server will be physically separate from the routers and LAN switches. The EI will then authenticate itself to the LSC so that it may obtain its E.164 number and the LSC shall update its user database and local directory to reflect the active status of the EI with its associated profile. In addition, the LSC shall authenticate itself to the EI. The mutual authentication between the EI and the LSC shall use TLS or its equivalent for authentication as a minimum and more sophisticated authentication mechanisms, such as a PKI certificate, are encouraged. At this point, the EI is able to support VVoIP sessions at the ROUTINE precedence level. Figure 5.4.5-5, EI Registration Process (DHCP), shows the EI registration process if DHCP is used for obtaining its IP address. The figure simplifies the TLS authentication process for ease of understanding the sequence, but Figure 5.4.5-7, AS-SIP TLS Authentication Process, provides a detailed description of the process.

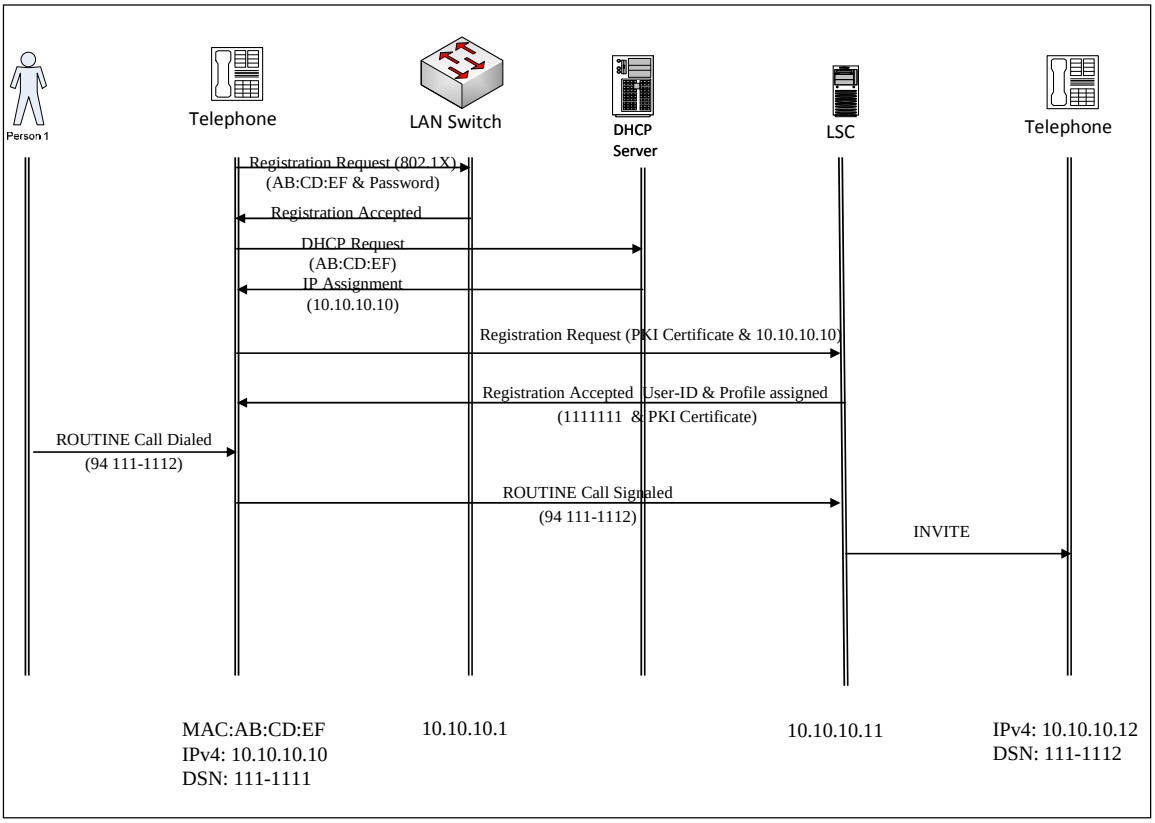


Figure 5.4.5-5. EI Registration Process (DHCP)

5.4.5.4.3 User Authentication and Authorization

For a ROUTINE precedence VVoIP session, the system does not require user authentication. However, VVoIP sessions above ROUTINE precedence may require user authentication and that authentication may be provided using a User-ID (PIN) with an associated numeric password (PIN) or using DoD PKI user certificates. If the end instrument is a softphone, the end instrument should be able to pass the user credential provided by the Common Access Card (CAC) to the LSC for user authentication. If a DoD PKI certificate is used, then the certificate path should be authenticated up to the trust point (or anchor point). If no other trust point is established, the certificate path shall be authenticated to the root certificate or certification authority (CA). Limiting the authentication of a user to sessions with precedence above ROUTINE also limits the impact that authentication has on the post dial delay since the validation of a DoD PKI certificate can take up to four seconds to complete. If the user certificate cannot be validated due to an inaccessibility of the On-Line Status Check (OSC), the session setup shall continue, but the event shall be logged and an alarm shall be sent to the NMS.

Based upon the user authentication and the profile associated with that user, the LSC will make a decision on whether to allow the session setup to continue.

Figure 5.4.5-6, Precedence Session User Authentication and Authorization, shows the PKI user authentication and authorization process for session requests above the ROUTINE precedence level.

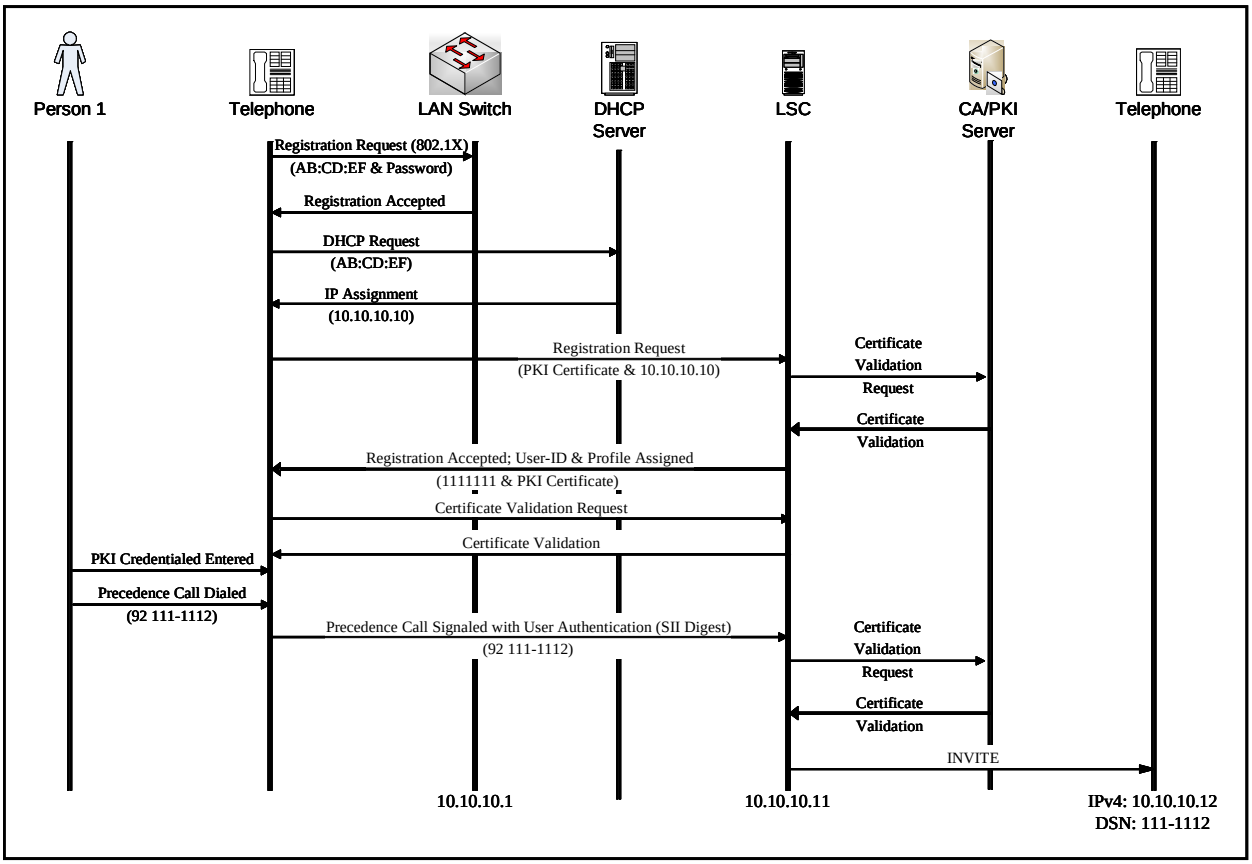


Figure 5.4.5-6. Precedence Session User Authentication and Authorization

5.4.5.4.4 Signaling Appliance Authentication and Authorization

5.4.5.4.4.1 AS-SIP

In addition to user authentication and EI authentication, the signaling appliances must also mutually authenticate to each other using the DoD PKI. Since all signaling appliances support AS-SIP, the authentication mechanisms must be integrated with AS-SIP in order to provide interoperability. Unfortunately, the SIP protocol is not intended to be a secure protocol and must rely on other security protocols for its security. Since the AS-SIP model chosen is a hierarchical signaling model, TLS was chosen as the IA protocol to secure AS-SIP since its hop-by-hop security model integrated nicely with the hierarchical signaling model. Fortunately, all AS-SIP signaling appliances (Objective for an EI) are required to be DoD Public Key Enabled (PKE) and support the DoD PKI. The process for obtaining a DoD PKI certificate is a manual process and

has to be completed prior to or during the initial installation. The DoD PKI in combination with TLS provides a secure process for signaling appliances to authenticate to each other and the process must be completed prior to transmitting an AS-SIP signaling session to the remote AS-SIP signaling appliance.

Figure 5.4.5-7 shows the process that must be completed before AS-SIP signaling is transmitted between AS-SIP signaling appliances.

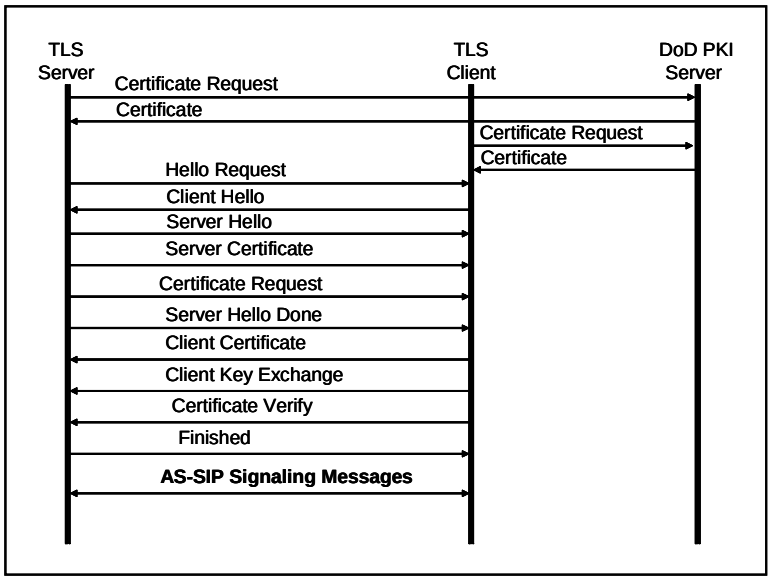


Figure 5.4.5-7. AS-SIP TLS Authentication Process

Once a TLS session is established between the AS-SIP signaling appliances, the AS-SIP signaling messages are allowed to transit between the appliances if the appliance profile permits. Every signaling appliance in the path of a AS-SIP signaling session (with the exception of the EI where it is Conditional) is responsible for receiving the AS-SIP packet, decrypting the packet, verifying the integrity of the packet, processing the packet in accordance with the AS-SIP specification, and then encrypting the packet prior to transmitting it to the next hop. Figure 5.4.5-8, AS-SIP Signaling Appliance Packet Processing, shows this process.

5.4.5.4.4.2 H.323 and H.248

Several legacy protocols must be supported until the Fiscal Year 2012 (FY12) timeframe. They include H.323, which is primarily used to support video sessions, and H.248, which is primarily used to communicate between a media gateway controller and a media gateway. The LSC may interpret H.323 and H.248 for line side connections (within a local domain or to the PSTN), but will translate the signaling to AS-SIP for trunk side (WAN) signaling. If H.323 is used for trunk (WAN) side signaling it will involve a point-to-point signaling session that will bypass the LSC

and extend directly to the remote EI or Multipoint Control Unit (MCU). TLS can be used to secure H.245 channels within the H.323 protocols because it uses TCP. However, H.323 is also composed of H.225.0 and RAS protocols and these protocols are not compatible with TLS if they are implemented with UDP since TLS requires a reliable protocol (TCP or SCTP). As a result, IP Security (IPSec) was chosen as the protocol to secure H.323 and H.248.

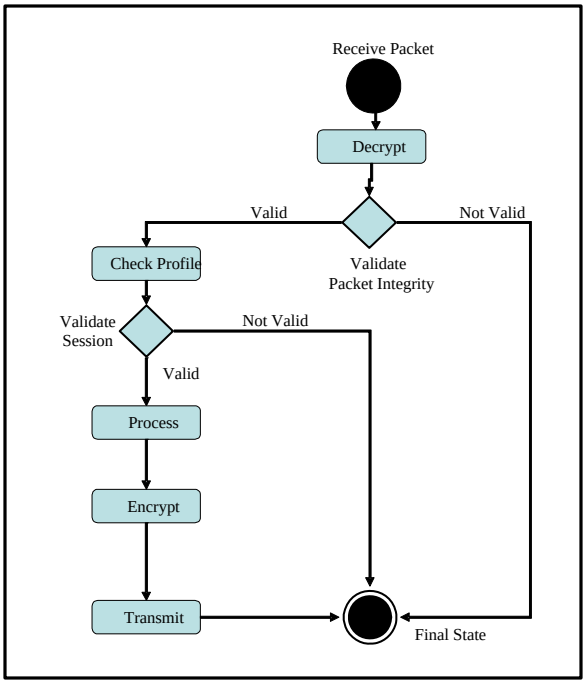


Figure 5.4.5-8. AS-SIP Signaling Appliance Packet Processing

The mechanism used for H.323 authentication and key exchange is the Internet Key Exchange (IKE) protocol. The IKE is a standards-based approach developed by the IETF to support IPSec. The IKE is a method for establishing a security association (SA) that authenticates users, negotiates the encryption method, and exchanges the secret key. The IKE is derived from the ISAKMP framework for key exchange and the Oakley key exchange technique, IKE is designed to support a PKI like infrastructure, such as the DoD PKI, and has mechanisms to provide the secure transmission of the secret key to the recipient so that the encrypted data may be decrypted at the other end.

5.4.5.4.4.3 Secure Bearer Path

In addition to securing the VVoIP signaling path, the VVoIP bearer path for EIs is also secured using the Secure Real Time Protocol (SRTP) to provide confidentiality and integrity. Since the end-to-end signaling path was authenticated using TLS and the EIs are the origination and termination points for that path, the EIs authentication will be achieved via that hop-by-hop authentication. It is understood that a limitation of hop-by-hop authentication model is that it is

only as strong as the weakest link. To understand the effect of this approach, an analysis was conducted that weighed the risk of a hop-by-hop security model with the benefit of reducing post dial delay by eliminating the point-to-point authentication process between the EIs using the authentication provided by the TLS process. The result of the analysis was that the benefits outweighed the risks. Given that additional authentication is not required, the next concern is to reduce the delay associated with exchanging encryption keys.

This was accomplished by embedding the SRTP encryption key for the session in the AS-SIP INVITE message as part the Session Description Protocol (SDP) within the AS-SIP packet. H.248 is also capable of distributing the SRTP encryption key in the SDP portion of the H.248 using the same parameter. H.323 distributes the session key in the same manner using the H.235 key distribution mechanisms instead of using SDP. Since the AS-SIP messages are encrypted and checked for integrity, the inclusion of the SRTP encryption key in the AS-SIP message provides a secure method for key exchange. In addition to providing a secure method for transport of the session key, it also allows the encrypted bearer stream to be transmitted as soon as the session setup is complete. The SRTP is used for both confidentiality and integrity of the bearer path. In determining the size of the hash needed to provide SRTP integrity, a cost benefit analysis was conducted that weighed the cost for each SRTP packet to process the hash and the IP overhead associated with the hash with the risk mitigated by a applying a larger secure hash. The analysis showed that a small hash (32-bit) was adequate to mitigate the risk given the large number of packets and the documented threats.

5.4.5.4.5 Network Management

Network management protocols are the final category of protocols that must be secured within the VVoIP environment. Network management protocols for the purposes of this discussion are separated into two categories dependent on whether they support traditional fault-management, configuration, accounting, performance, and security (FCAPS) related functions or directory services type functions. At this time, the VVoIP IA Design has not identified a requirement for XML-based Web services and UCR 2008 does not address the mechanisms that would be used to secure those services. Appliances performing network management functions (i.e., LSC, SS, MFSS, MG, ADIMSS, ARDIMSS, etc.) will use static IP addresses, and they will not be assigned IP addresses by a DHCP server. Since the IP address can be published to the FCAPS personnel in advance, the session initiator will use the appropriate IP address (either IPv6 or IPv4) in their request and IPv4/IPv6 translation is not required between the terminal and the appliance.

The VVoIP IA Design requires that every LSC and MFSS support three interfaces (to include redundancy on each interface). The three interfaces are used to support 1) Signaling and Bearer Traffic, 2) Local Element Management System (EMS), and 3) VVoIP End-to-End EMS. The appliance must ensure that traffic transiting from one interface to a different interface is limited

to authenticated and authorized traffic. For example, the LSC appliance must ensure that a user who has access to the signaling and bearer interface to establish a session is not allowed access to the Local EMS network. Typically, this is implemented by the appliance providing three external Ethernet interfaces. The three external Ethernet interfaces are assigned to three distinct VLANs in accordance with the types of traffic they support. Figure 5.4.5-9, VVoIP Product External Ethernet Interfaces, shows an example of the Ethernet interfaces found on an LSC and the access controls that may be configured to control traffic between the interfaces.

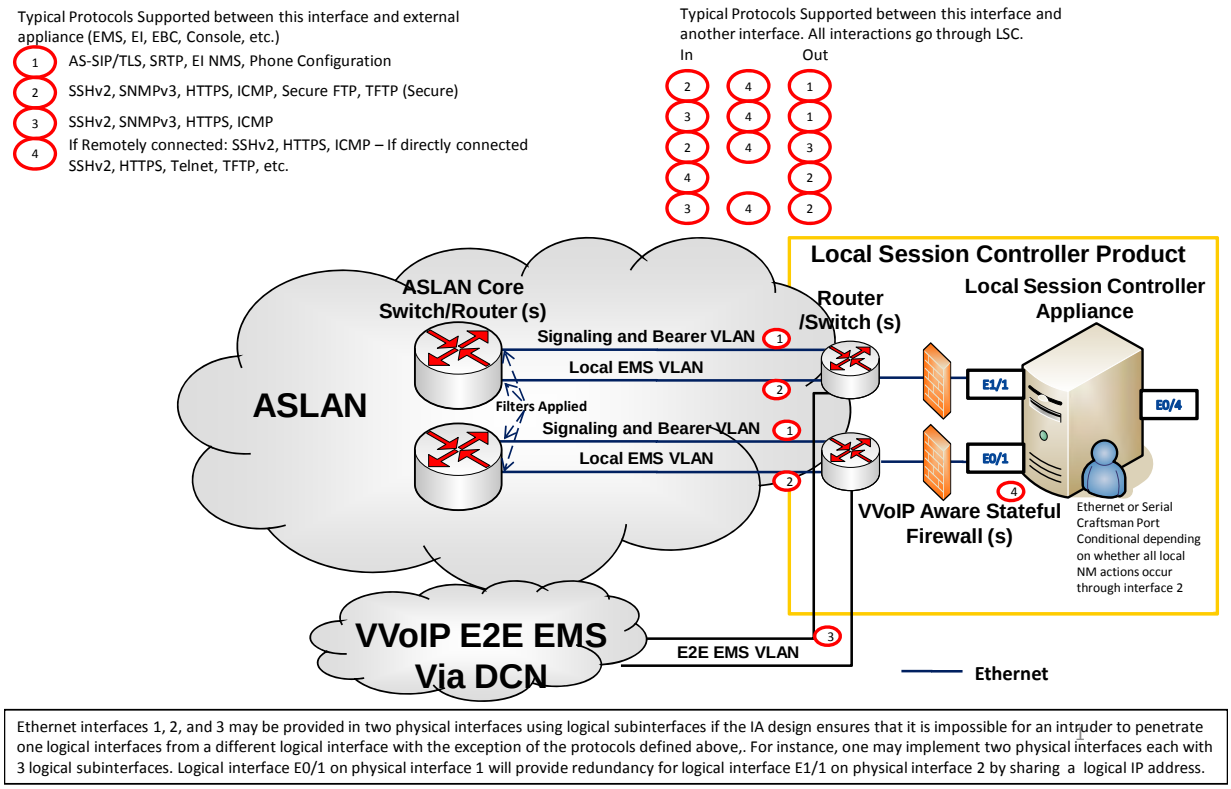


Figure 5.4.5-9. VVoIP Product External Ethernet Interfaces

The first category of protocols is the protocols that support FCAPS. These have been defined as the Simple Network Management Protocol (SNMP) version 3, the Secure Shell Protocol version 2 (SSHv2), and Secure Sockets Layer (SSL) Protocol version 3.1. SNMPv3 builds upon earlier versions of SNMP, but adds additional security mechanisms that are integrated into the protocol. SNMP is primarily used for minor configuration changes and for providing real time status on the VVoIP appliances. The VVoIP IA Design requires the use of SNMPv3 as a threshold requirement due to its significant improvement in the IA area over previous versions. However, it is understood that due to its newness, some solutions may have to use earlier versions of

SNMP with the mitigations of the appropriate patches, IPSec, and a upgrade plan for migrating to SNMPv3 due to their development cycles. The VVoIP IA design will use the SNMPv3 User Based Security Model.

SSHv2 is defined in RFC 4251 as a protocol for secure remote login and other secure network services over an insecure network. Primarily, SSHv2 is in the DoD VVoIP environment as a secure configuration and control protocol used by network engineers to access network elements in order to configure the appliances. It should be noted that EIs will disable remote manual configuration after the initial installation is completed and should not allow remote manual configuration after the initial installation. In addition, all EI non-automatic processes shall be performed locally. The SSH protocol consists of the following three major components: the Transport Layer Protocol, User Authentication Protocol, and Connection Protocol. The Transport Layer Protocol provides server authentication, confidentiality, and integrity. The User Authentication Protocol authenticates the client to the server, and the Connection Protocol multiplexes the encrypted tunnel into several logical channels.

The final protocol is the Transport Layer Security (TLS) version 1.0 or higher, which for the purposes of this design is considered interchangeable with Secure Socket Layer (SSL), version 3.1. The SSL is used within the network management system as an alternative to SSHv2 and is primarily associated with web-based network management GUIs. It provides a secure manner for authorized and authenticated network engineers to access VVoIP appliances to perform network management functions.

The second category of network management protocols is associated with location services. A standard protocol has not yet been selected for location services. The FY2008 design does not support the use of dynamic location services and location services will be provided using a manually populated forwarding table that contains the next hop address for the signaling sessions. It is anticipated that user directory services will be supported in the FY12 timeframe and LDAPv3 is a potential candidate for user directory services. In addition to directory services, this protocol is also used to support the DoD PKI and is designed to provide access to directories supporting the X.500 models, while limiting the resource requirements associated with other protocols. The LDAPv3 is specifically targeted at management applications, such as the DoD PKI and directory services that provide read/write interactive access to directories, including accessing stored PKI certificates and E.164 addresses. When used with a directory supporting the X.500 protocols, it is intended to be a complement to the X.500 Directory Access Protocol (DAP). The LDAP is nothing more than an access protocol and does not require the underlying directory database to be based on any particular technology. The LDAPv3 is designed to integrate with TLS in a similar manner to AS-SIP. The TLS is used with LDAP to provide confidentiality, integrity, and authentication in combination with the use of the DoD PKI certificates. The use of TLS does not provide or ensure confidentiality and/or non-repudiation of the data housed by an LDAP-based directory server, nor does it secure the data from inspection

by the server administrators. Once established, TLS only provides for, and ensures confidentiality and integrity of the operations and data, in transit over the LDAP association and only if the implementations on the client and server support and negotiate it.

5.4.5.4.6 Secure VVoIP End Instruments

The current suite of secure VVoIP EIs consist of legacy appliances and the future version of an IP secure EI is several years away from a wide spread fielding of the systems. The IP secure EI is currently designed to rely on the SCIP standard that was adopted as the replacement for the FNBDT in 2004. The IP secure DSCD currently under development will rely on SCIP to provide classified voice and data across the DoD IP networks.

NSA has directed that IP DSCDs adopt the AS-SIP protocol as the default VVoIP signaling protocol when it is specified to the end instrument. The current version of the DSCD uses a single vendor proprietary VVoIP signaling protocol that only interoperates with single vendor signaling appliances. In addition, the VoIP DSCD under development is not backwards compatible with all legacy secure EIs. However, the VoIP DSCD is designed to interoperate with the TDM STE and STU-III appliances, with the assistance of an IP-TDM Gateway that supports ITU V.150.1.

5.4.5.4.7 Edge Boundary Control Appliances

The VVoIP IA design uses two appliances to defend the boundary between the Customer Edge Segment and the Network Edge Segment. The first appliance is called the EBC its function is to act as a VVoIP aware firewall. The second appliance is called the CE Router, and its primary functions are associated with QoS and perimeter defense. Figure 5.4.5-4, VVoIP Proprietary and Standards Based Protocols, shows the location of the EBC and the CE Router. Both appliances must be highly reliable (i.e., 99.999% available) and IPv6 capable using a dual stack.

The CE Router is responsible for providing traffic conditioning (policing and shaping) on inbound and outbound traffic to ensure that the Service Level Agreements (SLAs) are met for both the Network Edge Segment and the Customer Edge Segment. This is one of the defense-in-depth mechanisms used to prevent a Denial of Service (DoS) attack by ensuring that only a predetermined number of signaling or VVoIP sessions may transit the CE Router at a particular instance of time. It is understood that this only prevents the Customer Edge Network from being impacted by a DoS attack and that the external connectivity may be affected. The granularity of the traffic conditioning is to the level of the granular service class, such as voice or video. In FY2008, configuration changes associated with traffic conditioning will be a manual process. However, the FY2012 Design envisions that traffic conditioning will be dynamic due to the dynamic nature of the closed loop system budgets for the granular service classes. In order to achieve this vision, an interface must be defined for communication between the AS-SIP

signaling appliance (i.e., LSC or SS) and the CE Router in order to ensure that the AS-SIP signaling appliance budgets are consistent with the CE Router traffic conditioning parameters. In addition, the CE Router must also have the capability to provide QoS for VVoIP by supporting the Per Hop Behaviors (PHBs) based on the DiffServ Code Point (DSCP) markings that will be defined by the QoS Working Group.

Primarily, the EBC is focused on perimeter defense. Real time services suffer from certain difficulties with traditional perimeter defense mechanisms, such as NAT and data firewall behavior. Many protocols designed by the IETF used within the VVoIP environment, such as SIP, are designed as end-to-end protocols. The end-to-end model is broken by the presence of firewalls and NAT appliances. In large deployments of VVoIP, such as the DISN, a specialized appliance is needed to facilitate the coexistence of VVoIP and perimeter defense mechanisms. The DoD VVoIP IA design has labeled this specialized appliance as an EBC to distinguish it from similar commercial appliances that do not have unique DoD requirements. Before describing the requirements and functions associated with the EBC, it is important to explain the difficulties that VVoIP protocols experience crossing network boundary devices and to explain the common types of solutions emerging from the standards communities and major vendors. Following this discussion, a general discussion of the requirements associated with an EBC will be provided.

As mentioned previously, the use of NAT introduces several problems to an end-to-end protocol security model. The use of NAT is required at the WAN boundary by the VoIP and Network Infrastructure STIGs. In a traditional NAT employment, the NAT is conducted at the Network Layer (Layer 3) of the OSI model (Network Address Port Translation is conducted at Layer 4). However, the DoD VVoIP environment requires that the EBC perform NAT at a higher layer in order to process the AS-SIP messages properly. The common scenario provided for NAT is the use of private addressing in two remote enclaves, with a public address space in the interconnecting WAN.

During the initial AS-SIP offer/answer exchange, both the originating and terminating AS-SIP User Agents (UAs) will specify in the SDP payload the desired IP address and port combination for the caller and called party to receive the associated media stream and to properly direct the signaling stream. AS-SIP UAs within the Customer Edge segment may use private addressing for topology hiding reasons. A problem occurs when private addressing is used within the SDP payload since the private address is not resolvable from the WAN side of the NAT. A traditional NAT device will change the IP source address and/or port combination at packet header level, but not the IP address within the SDP payload. Consequently, the called party, or User Agent in the remote enclave, will not have the correct IP address to respond to from a signaling perspective and the call setup will fail. Even if the call is established from a signaling perspective, the bearer stream would be sent to the wrong address/port and the session would not be established.

An additional problem is that the signaling and bearer paths are different IP sessions and NAT bindings in a traditional NAT appliance are finite in nature (not correlated). A scenario may result in that a VVoIP session may continue for many minutes with active RTP streams, but no signaling messages. Since there is no signaling, the signaling NAT binding could time out, and the session would not be able to end properly.

Difficulties experienced by AS-SIP signaling and Real Time Protocol / Real Time Control Protocol (RTP/RTCP) media protocols passing through firewalls stem mainly from the fact that bearer stream port numbers are selected dynamically for each call from a large pool of potential port numbers. Allowing this large range of potential port numbers to be open at the enclave boundary is unacceptable. The EBC needs to know which ports to open temporarily, when to open them and when to close them. Placing this functionality (essentially an Application Level Gateway) into data firewalls has not happened yet and carries with it some disadvantages, for example, having the firewall perform actions it is not supposed to handle.

Solutions for these issues have evolved slowly within the standards bodies and major equipment vendors. A myriad of suggestions have been offered from both communities, yet none has attained widespread acceptance. Efforts have included work from the IETF's Middlebox Communication (MIDCOM) Working Group, which closed in March 2008. The envisioned MIDCOM Design provided for a protocol link between the LSC and the boundary device, a firewall or NAT device, called a middlebox, for the purposes of opening and closing pinholes in the middlebox. The MIDCOM Working Group never completely achieved its goal, but certain pre-MIDCOM solutions, such as Simple Tunneling of UDP through NAT (STUN) and Interactive Connectivity Establishment (ICE), have been implemented in freeware projects and in some products. Widespread deployment of technologies such as STUN, Traversal Using Relay NAT (TURN), and ICE has not happened as of this writing. In the interim, some vendors have developed limited solutions for their products to allow functionality, and several have acquired EBC functionality to enhance their product lines, however, no clear solution to achieve multivendor interoperability has come out of the major vendor arena. As a result, interoperability problems often occur between different vendor solutions due to the proprietary nature of the vendor unique solutions.

Some of the difficulty with solutions coming from the standards arena is an aversion to dealing with middleboxes at all. NAT was originally meant to be a short-term solution to the IP address depletion problem. Many Application protocols are designed to be end-to-end in nature, and firewalls and NAT devices break this end-to-end nature of many protocols. There are also arguments that middleboxes prevent application layer protocols from protecting themselves by breaking the end-to-end security model. Standardization of NAT behavior has not occurred and has resulted in NAT implementations that behave differently from vendor to vendor. Another IETF working group, the Behavior Engineering for Hindrance Avoidance (BEHAVE) working

group, was formed to identify, classify, and understand these behaviors in order to bring some standardization to them but the end state of a standardized behavior has not been achieved.

In response to a need for a solution to various problems with VVoIP in the areas of firewall/NAT traversal, topology hiding, and lawful intercept, a large number of startup companies have produced a solution that has come to be known as Session Border Controller (SBC). These products may provide functionality in one or more areas, however there is no standardization among the producers of these products and they currently do not meet the DoD unique requirements associated with the processing of AS-SIP, so it is necessary for the DoD to specify precisely the functionality required in these solutions.

The result of this situation is that the DoD has defined an EBC system that is placed at the boundary between the Edge segment and the Access segment to provide three critical functions; topology hiding, "pinholing," and filtering.

Topology hiding is accomplished by processing the AS-SIP messages and performing the appropriate IP address and port translations within the IP header and the SDP payload. Figure 5.4.5-10, Typical End-to-End AS-SIP Call Flow, shows the typical call flow associated establishing an AS-SIP session. The diagram shows how the media is bi-directionally anchored by the EBC to ensure that topology hiding is provided in accordance with the DoD requirements.

Several issues are encountered by EBCs in attempting to meet the topology hiding requirements due to the VVoIP signaling hierarchy and by the requirement to allow call forwarding and call transfer. The first issue is found in EBCs that front a Softswitch component of an MFSS. Upon receipt of an AS-SIP INVITE, the EBC does not know whether that session terminates within the enclave, or will be forwarded to another enclave (after processing by the Softswitch). Due to the uncertainty, the EBC must anchor the media stream bi-directionally. If the Softswitch returns the INVITE to the EBC for forwarding to the next hop, the EBC must restore the original IP address and port number so that it is no longer involved in the media stream associated with that session.

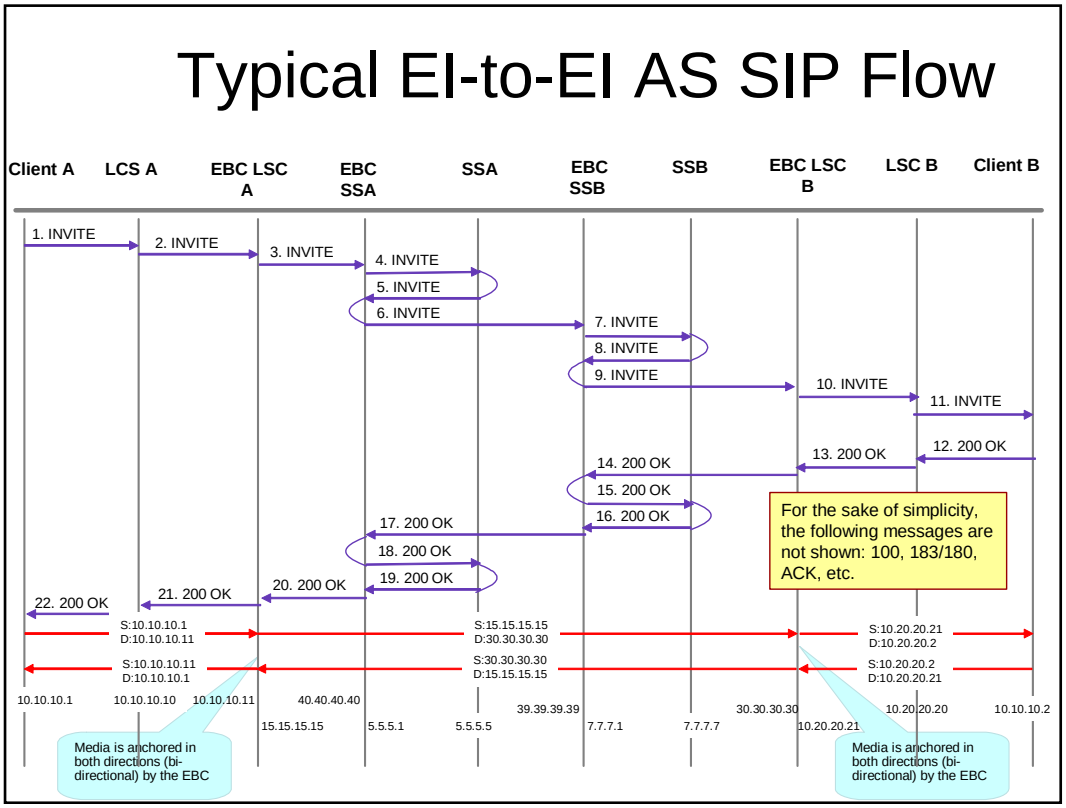


Figure 5.4.5-10. Typical End-to-End AS-SIP Call Flow

Figure 5.4.5-11, Media Anchoring for Transitive SIP Signaling, shows the process associated with transitive SIP signaling for an EBC that fronts the Softswitch component of the MFSS.

The second issue associated with topology hiding is related to call forwarding and call transfer scenarios where the session no longer terminates within the enclave. Upon notification that a session is being forwarded or transferred, the EBC associated with the forwarding or transferring party must restore the original IP address and port number associated with that session to ensure that the media is not improperly anchored at the enclave since the session is no longer associated with the enclave. The process used is similar to the process described in Figure 5.4.5-10, Media Anchoring for Transitive SIP Signaling.

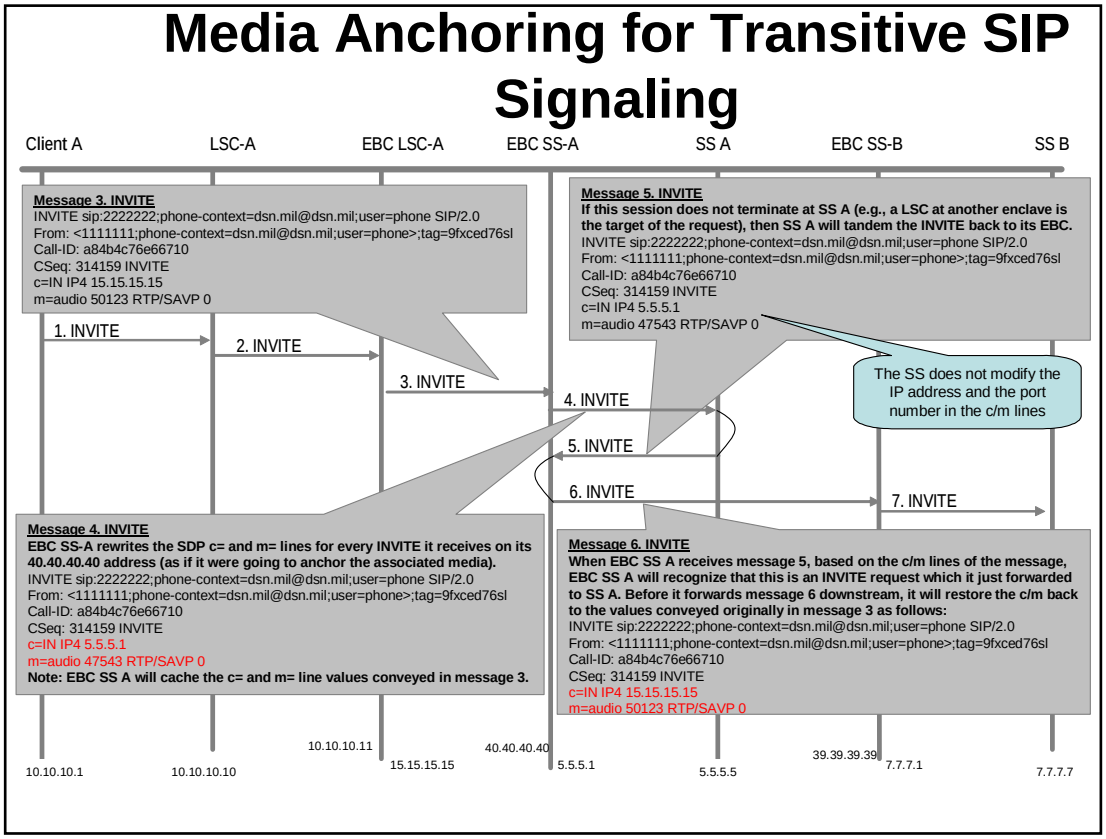


Figure 5.4.5-11. Media Anchoring for Transitive SIP Signaling

The next issue concerns the ability of the EBC to determine the appropriate next hop for signaling. For an EBC fronting an LSC, the EBC has only a primary and secondary TLS path in which to forward the AS-SIP messages. The primary TLS path is to the EBC fronting the primary MFSS for the LSC and the secondary path is to the EBC fronting the secondary MFSS for the LSC. However, for an EBC fronting the Softswitch component of the MFSS, it has numerous TLS sessions associated with the subtended LSCs of the MFSS and with the other Primary and Secondary MFSSs for all the remote LSCs. Since the EBC does not have its own location service, it must rely on the Softswitch component of the MFSS to inform it of the appropriate next hop. The Softswitch informs the EBC of the next hop using the Route Header construct defined in the RFC 3261. It is important to note that this issue is not relevant to INVITEs arriving from the WAN, since the EBC is associated with one and only one AS-SIP signaling system on the line side and always forwards INVITEs arriving from the WAN to its associated AS-SIP signaling system (i.e., LSC or MFSS). In addition to performing topology hiding, the EBC provides several other functions to include "pinholing."

"Pinholing" is accomplished by opening and closing "pinholes" that only allow approved sessions to transit the EBC based on the AS-SIP messages. The coupling of the signaling and bearer stream requires that both streams must transit the EBC. If H.323 video is also transiting

the EBC, the "pinholes" may also be associated with the H.323 messages. In addition, the EBC must have a timer associated with each "pinhole" to ensure that "pinholes" do not remain open indefinitely if a signaling message is not received to close the "pinhole." If the EBC closes the "pinhole," it must send a BYE message in each direction to notify the next hop signaling appliances that the session has been terminated.

Filtering is accomplished by allowing targeted IP flows to transit the EBC based on their "6 tuple," which in VVoIP consists of the:

- Source IP address
- Destination IP address
- Source port number
- Destination port number
- DiffServ Code Point
- Protocol identifier

Compared to "pinholes," filtering is a manual process and is not dynamic in nature. A type of traffic flow associated with filtering is a SNMPv3 session from the EMS to a LSC that is active all the time and is well defined. If the EBC detects an anomalous condition (DoS attack, abnormal number of invalid AS-SIP requests, etc.), it must have the ability to notify the appropriate EMS of the event.

5.4.5.5 VVoIP IA Design Items Outstanding

Several VVoIP IA design items are outstanding and associated with the uncertainty of the final VVoIP design. Some issues that must be resolved prior to the completion of the VVoIP IA design are the finalization of the VVoIP closed loop ASAC solution and the addressing wireless technology IA issues. In addition, the proper design for securing multicast was deemed too difficult to address in this version of the UCR 2008 and may be included in future revisions as the DISN multicast design solidifies.

The VVoIP IA Design team has not developed IA requirements to compliment the Personal Computer Communications Client (PCCC) (Softphone) STIG and future revisions of this section will be updated to correct this omission. It is also assumed that the review process of UCR 2008 will identify several outstanding IA items that will need to be addressed in subsequent revisions of this UCR 2008.

5.4.6 Requirements

5.4.6.1 Introduction

Based on the VVoIP IA design, threats and countermeasures, a set of derived requirements were developed. Different vendors combine different functions into their appliances to meet the requirements of a particular type of product. For the purposes of UCR 2008, the requirements are levied on the individual appliance, as applicable, to secure the entire product. The terms user and customer are used in the same context as GR-815-CORE. It is understood that the IA design provides a high-level description of how the security services are applied to the appliance and how the appliances interact in a secure manner. In addition, the appropriate STIGs will further clarify how the IA design and requirements are implemented on the appliance. UCR 2008, Section 5.4, Information Assurance Requirements, is intended to provide a level of security requirements consistent with the level of security requirements specified in the GR-815-CORE, but adapted for the unique DoD VVoIP environment consistent with the requirements in the UCR. UCR 2008 addresses VVoIP IP requirements and TDM-related IA requirements.

To assist the reader in the origin of the requirements, IA requirements are broken down according to the reference document from which they were derived. The requirement key words (i.e., REQUIRED, CONDITIONAL, etc) are defined elsewhere in the UCR 2008. Failure to satisfy a requirement will result in a Category I, II, or III finding.

Finally, the derived requirements do not include all of the administrative requirements (nontechnical) associated with policy and the STIGs. For instance, if someone is required to administratively document something (e.g. waiver, pilot request, etc.), that requirement is not included. The acronyms and appliances used for specifying the type of component are shown in Table 5.4.6-1, Acronyms and Appliances Specifying Type of Component.

5.4.6.2 General Requirements

1. **[Required: MFS, MFSS, TS, SS, SMEO, PBX1, LSC, MG, EBC, R, LS]** All IA and IA enabled Information Technology (IT) products shall be capable of being configured in accordance with all applicable DoD approved security configuration guidelines (i.e., STIGs).

    a. **[Required: MFSS, SS, LSC, MG, EBC]** VVoIP appliances shall be dedicated to VVoIP functions.

    b. **[Required: MFSS, SS, LSC, MG, EBC]** VVoIP appliances shall only have applications or routines that are necessary to support VVoIP functions.

Table 5.4.6-1. Acronyms and Appliances Specifying Type of Component

ACRONYM	APPLIANCES
MFS	Multifunction Switch
MFSS	Multifunction Softswitch
EO	End Office
TS	Tandem Switch
SS	Softswitch
LSC	Local Session Controller
SMEO	Small End Office
PBX1	Private Branch Exchange 1
MG	Media Gateway
EBC	Edge Boundary Controller
EI	End Instrument
LS	LAN Switch
R	Router

NOTE: The disabling or deletion of applications or routines via hardware or software mechanisms shall satisfy this requirement. For example, if an appliance by default is installed with a web browser and the web browser is not needed to support VVoIP, then the application shall be removed from the appliance. Another example is if a feature is part of the application, but is not needed in the DoD environment that feature shall be disabled via hardware or software mechanisms.

b. **[Required: MFSS, SS, LSC, MG, EBC, R, LS, EI]** Software patches shall only be installed if they originate from the system manufacturer and are applied in accordance with manufacturer's guidance.

(1) **[Required: MFSS, SS, LSC, MG, EBC, R, LS, EI]** The system shall only accept automatic software updates if they are cryptographically signed by the software vendor.

NOTE: It is assumed that manual updates will be validated by an authorized administrator prior to installation.

2. **[Conditional: MFSS, SS, LSC, MG, EBC, R, EI, LS]** If the system uses public domain software, unsupported software, or other software, it shall be covered under that system's warranty.

NOTE: If a vendor covers in its warranty all software, regardless of its source, within their product then this requirement is met. An example of unsupported software is Windows NT, which is no longer supported by Microsoft and it is unlikely that a vendor would support this operating system as part of its system.

a. **[Required: MFSS, SS, LSC, MG, EBC, R, EI, LS]** The systems shall only use open source software if all licensing requirements are met.

NOTE: Open source software refers to software that is copyrighted and distributed under a license that provides everyone the right to use, modify, and redistribute the source code of the software. Open source licenses impose certain obligations on users who exercise these rights. Some examples include publishing a copyright notice and placing a disclaimer of warranty on distributed copies.

3. **[Required: MFSS, SS, LSC, MG, EBC, R, LS, EI]** The system shall not use mobile code technologies (e.g., Java, JavaScript, VBScript, and ActiveX) unless the mobile code technology is categorized and controlled in accordance with policy.

NOTE: The policy specifying categories and risks associated with mobile code is defined in [5].

4. **[Conditional: EI]** If the softphones are used in remote connectivity situations, the system shall be capable of supporting a VPN for VVoIP traffic from the PC to the Enclave VPN access router/node.

NOTE: The data from the PC and VVoIP traffic from the PC softphone must be separated into the appropriate VLANs at the earliest point in the path.

5. **[Required: MFSS, SS, LSC, MG, EBC, R, LS]** The system shall be capable of being located in physically secure areas.

a. **[Required: MFSS, SS, LSC, MG, EBC]** The system shall be capable of enabling password protection of BIOS settings.

b. **[Required: MFSS, SS, LSC, MG, EBC]** The system shall be capable of disabling the ability to boot from a removable media.

6. **[Conditional: EI]** If the system has a speakerphone, the system shall be capable of disabling the speakerphone microphone.

NOTE: Acceptable methods for meeting this requirement include physically disabling the speakerphone or disabling the speakerphone using a configurable software parameter.

7. **[Conditional: EI]** If the system is used in a sensitive area where national security systems (NSS) are employed and/or within environments where national security information (NSI) is stored, processed, or transmitted, then the system shall be certified and accredited in

accordance with the Telephone Security Standard (TSG) 6, which is prepared by the National Telecommunications Security Working Group (NTSWG).

8. **[Required: MFSS, SS, LSC, MG, EBC, R, LS, EI]** The system shall be capable of using a static IP address.

9. **[Required: MFSS, SS, LSC]** The system shall only connect to the PSTN or coalition networks using PRI and/or CAS.

   NOTE: This precludes the exchange of SS7 or IP VVoIP signaling (and IP VVoIP media) information between the SBU voice (SS and LSC) and the PSTN and coalition networks.

10. **[Conditional: MFSS, SS, LSC, MG, EBC, EI]** If the system uses a Microsoft Windows based operating system, the system shall support the installation and operation of the DoD mandated Host Based Security System (HBSS).

    NOTE: The DoD currently has an enterprise wide license for McAfee's ePolicy Orchestrator (ePO) server, Host Intrusion Prevention System agent, and several associated agent applications. HBSS is being deployed by all C/C/S/As to all Windows based servers and workstations.

5.4.6.2.1 Authentication (Includes Authorization and Access Control)

5.4.6.2.1.1 Banners

1. **[Required: MFSS, SS, LSC, MG, EBC, R, LS]** The system shall be capable of having warning banners on all systems management ingress ports accessed by administrators or users as part of a human-to-machine interface for the purposes of network management. The banner shall function in the following manner:

   a. **[Required: MFSS, SS, LSC, MG, EBC, R, LS]** At the first point of entry, the system shall have the capability to display a warning message of up to 20 lines by 80 characters (1600 characters) in length.

   b. **[Required: MFSS, SS, LSC, MG, EBC, R, LS]** As part of delivered software, the system shall be capable of providing an appropriate default message that warns against unauthorized access or use.

      NOTE: The default message can be configured during the installation process.

c. [Required: MFSS, SS, LSC, MG, EBC, R, LS] The system banner shall be capable of being configured by authenticated and authorized personnel.

d. **[Required: MFSS, SS, LSC, MG, EBC, R, LS]** The system shall be capable of displaying the banner to the administrator or user prior to a login attempt to the system.

e. **[Required: MFSS, SS, LSC, MG, EBC]** The system shall be capable of requiring that the administrator or user acknowledges the banner after the user login but prior to accessing system processes.

(1) **[Required: MFSS, SS, LSC, EBC]** The system shall record the acknowledgement in the audit log in association with the administrator or user name.

NOTE: If the acknowledgement is an essential step in the successful login process, then it is sufficient to only log the completion of a successful login.

f. **[Required: MFSS, SS, LSC, MG, EBC, R, LS]** The system shall be capable of displaying the following information upon successful access to the system:

(1) **[Required: MFSS, SS, LSC, MG, EBC, R, LS]** The date and time of the administrator's or user's last successful access to the system.

(2) **[Required: MFSS, SS, LSC, MG, EBC, R, LS]** The number of unsuccessful attempts by that user-ID to gain system access to the system (e.g., mistyped password) since the last successful access by that user-ID.

5.4.6.2.1.2 System and User Names and Passwords

1. **[Required: MFSS, SS, LSC, MG, EBC, R, EI, LS]** Every communicating system entity (i.e., persons, processes, or remote systems) shall be identified by an entity identifier that is unique within the domain of the appliance or application being connected to.

a. **[Required: MFSS, SS, LSC, MG, EBC, R, EI, LS]** The system shall be capable of providing a primary access control method that is stronger than assigning passwords to specific actions (e.g., operations-related commands) although assigning passwords may be used to augment access control.

NOTE: If such a password is assigned, it loses its confidentiality because it has to be shared among all authorized users.

b. **[Required: MFSS, SS, LSC, MG, EBC, R, EI, LS]** The system shall be capable of ensuring that all users and customer passwords are used in a secure manner.

NOTE: This requirement is user/customer passwords to include passwords that are used for role-based authentication.

(1) **[Required: MFSS, SS, LSC, MG, EBC, R, EI, LS]** The system shall be capable of automatically suppressing or blotting out the clear text representation of a password on the data entry device.

(2) **[Required: MFSS, SS, LSC, MG, EBC, R, EI, LS]** The system shall ensure that passwords are safeguarded at the confidential level for sensitive but unclassified (SBU) systems.

NOTE: All components of a system will be at the same sensitivity level.

NOTE: The decision of how to properly safeguard the passwords is determined by the B/P/C/S DAA, but as a minimum shall consist of encrypting the passwords during transit or while in storage using FIPS 140-2 commercial encryption.

(a) **[Required: MFSS, SS, LSC, MG, EBC, R, EI, LS]** The system shall be capable of storing access passwords (user and administrator) in a one-way encrypted form.

(3) **[Required: MFSS, SS, LSC, MG, EBC, R, EI, LS]** The system shall be capable of ensuring that passwords are not available in clear text to any user, including appropriate administrators. An appropriate administrator may be allowed to retrieve encrypted passwords. However, encrypted passwords shall not be available to any other user.

NOTE: It is recognized that is may not be realistic to make the encrypted password file unavailable to administrators. The administrator may be able to view the file's content, but would not be able to decipher the encrypted passwords.

(4) **[Required: MFSS, SS, LSC, MG, EBC, R, EI, LS]** The system shall be capable of providing a mechanism for a password to be user changeable. This mechanism shall require reauthentication of user identity.

NOTE: This requirement applies to factory set, default, or standard user-ID passwords.

(a) **[Required: MFSS, SS, LSC, MG, EBC, R, EI, LS]** The system shall be capable of ensuring that a new user password differs from the previous password by at least four characters.

(b) **[Required: MFSS, SS, LSC, MG, EBC, R, EI, LS]** The system shall be capable of having a password history to prevent password reuse. The default shall be configurable and shall be at least the past eight passwords or 180 days of password history.

(5) **[Required: MFSS, SS, LSC, MG, EBC, R, LS]** After a password is assigned to a human user, when that user establishes a session for the first time, the system shall be capable of prompting the user to change the password and deny the session if the user does not comply.

(6) **[Required: MFSS, SS, LSC, MG, EBC, R, LS]** The system shall be capable of enforcing a configurable password aging interval (i.e., a password is required to be changed after a specified interval).

NOTE: The exception to these requirements is found in the emergency access requirements in this UCR 2008 (Section 5.4.6, paragraph 1 (l) and (m)).

(a) **[Required: MFSS, SS, LSC, MG, EBC, R, LS]** The system shall be capable of defining a system-wide default password aging interval.

(b) **[Conditional: MFSS, SS, LSC, MG, EBC, R, LS]** If the system supports long-lived sessions (i.e., two signaling appliances continuously connected), the system shall be capable of providing the capability to set the password aging interval on a "per-user-ID basis."

NOTE: If, due to some unforeseen reason, such as a power failure, the session is interrupted, an expired password may be a hindrance to re-establishing the session, especially if the appliance is not always attended by human users.

(c) **[Required: MFSS, SS, LSC, MG, EBC, R, LS]** If the system supports users, the system shall be capable of setting the password aging interval on a "per-user-ID basis.

i. **[Required: MFSS, SS, LSC, MG, EBC, R, LS]** The system shall notify the user a specified period of time before the password expiration.

ii. **[Required: MFSS, SS, LSC, MG, EBC, R, LS]** The system shall notify the user upon password expiration, but allow a specified additional number of subsequent logins within a specified time period before requiring a new password.

A. **[Required: MFSS, SS, LSC, MG, EBC, R, LS]** The default for the number of subsequent logins shall not be greater than three.

B. **[Required: MFSS, SS, LSC, MG, EBC, R, LS]** The default for the specified time period shall not be greater than 30 days.

iii. **[Required: MFSS, SS, LSC, MG, EBC, R, LS]** The system shall not hard code the notification mechanism for password expiration to allow for variation in variables such as “early warning period,” “grace period,” and subsequent login after password expiration.

(7) **[Required: MFSS, SS, LSC, MG, EBC, R, EI, LS]** For a user updating a password, the system shall be capable of enforcing a configurable minimum period of waiting before an existing password can be updated (except for the first time update, which is required to be performed when the user logs in for the first time after being assigned a password).

NOTE: This requirement discourages password "flipping" and is related to the history requirements stated previously.

(a) **[Required: MFSS, SS, LSC, MG, EBC, R, EI, LS]** The default for the minimum waiting period shall be 24 hours without administrator intervention.

(8) **[Required: MFSS, SS, LSC, MG, EBC, R, EI, LS]** The system shall be capable of ensuring that the all user entered passwords meet the following complexity requirements (so it cannot be “easily guessable”):

(a) **[Required: MFSS, SS, LSC, MG, EBC, R, LS]** The system shall be capable of ensuring that the password consists of a mix of a minimum of nine characters using at least two characters from each of the four

character sets (i.e., upper-case letters, lower-case letters, numbers, and special characters).

NOTE: Special characters are characters on a keyboard typically located above the numbers (i.e., !, @, #, etc.). NOTE: See the next requirement that is more stringent on certain users.

(b) **[Required: MFSS, SS, LSC, MG, EBC, R, LS]** The system shall be capable of ensuring that system security administrators, system administrators, and application administrator passwords consist of a mix of a minimum of 15 characters using at least two characters from each of the four character sets (i.e., upper-case letters, lower-case letters, numbers, and special characters).

NOTE: Special characters are characters on a keyboard typically located above the numbers (i.e., !, @, #, etc.).

(c) **[Required: MFSS, SS, LSC, MG, EBC, R, EI, LS]** The system shall be capable of ensuring that the password does not contain, repeat, or reverse the associated user-ID.

(d) **[Required: MFSS, SS, LSC, MG, EBC, R, EI, LS]** The system shall be capable of ensuring that the password does not contain three of the same characters used consecutively.

(e) **[Required: MFSS, SS, LSC, MG, EBC, R, EI, LS]** The system shall be capable of ensuring that a "null" password is not possible.

(9) **[Conditional: MFSS, SS, LSC, MG, EBC, R, EI, LS]** If passwords are generated by the system, the system passwords shall be capable of meeting the following requirements:

(a) **[Required: MFSS, SS, LSC, MG, EBC, R, EI, LS]** System supplied passwords shall be “reasonably” resistant to brute-force password guessing attacks, i.e., the total number of system-generated passwords shall be on the same order of magnitude as what a user could generate using the rules specified for user-entered passwords.

(b) **[Required: MFSS, SS, LSC, MG, EBC, R, EI, LS]** The generated sequence of passwords shall have the property of randomness, i.e.,

consecutive instances shall be uncorrelated, and the sequence shall not display periodicity.

(c) **[Conditional: MFSS, SS, LSC, MG, EBC, R, EI, LS]** If the "alphabet" used by the password-generation algorithm consists of syllables rather than characters, the security of the password shall not depend on the secrecy of the alphabet.

(10) **[Required: MFSS, SS, LSC, MG, EBC, R, EI, LS]** The system shall ensure that it does not prevent a user from choosing (e.g. unknowingly) a password that is already associated with another user-ID (Otherwise, an existing password may be divulged).

(11) **[Required: MFSS, SS, LSC, MG, EBC, R, EI, LS]** The system shall not permit passwords to be embedded in system defined access scripts or function keys.

(12) **[Conditional: MFSS, SS, LSC, MG, EBC, R, EI, LS]** If he system has the capability to display the “username of the last successful logon”, then the system shall have the capability to enable and disable that feature.

(13) **[Required: MFSS, SS, LSC, MG]** The system shall have the capability to disable and enable the last successful logon message feature that tells the user the last successful and unsuccessful logon time and date.

(14) **[Conditional: MFSS, SS, LSC, MG, EBC, R, EI, LS]** If PINs are used for passwords, the system shall have a configurable parameter for the PIN length and the range shall be between four (4) and twenty (20) characters with a default of four (4). NOTE: All password requirements defined in this Section apply to PINs when used as passwords.

(a) **[Conditional: MFSS, SS, LSC, MG, EBC, R, EI, LS]** If PINs are used for passwords, the system shall ensure that only numbers are allowed (i.e., no “#” or “*”).

c. **[Conditional: MFSS, SS, LSC, MG, EBC, R, EI, LS]** If PINs (User-ID) are used for user identification (versus password), the system shall be capable of ensuring that only one individual is permitted to use an assigned PIN.

NOTE: Since this can conflict with the preceding requirement, PINs (User-ID) must be assigned to users and they shall not be allowed to select their own PIN (User-ID).

This requirement only applies when a PIN is used for user identification without any other credential like a username or phone number.

(1) **[Conditional: MFSS, SS, LSC, MG, EBC, R, EI, LS]** If PINs (User-ID) are used for user identification, the system shall have a configurable length between six (6) and twenty (20) characters and the default shall be 6.

(2) **[Conditional: MFSS, SS, LSC, MG, EBC, R, EI, LS]** If PINs (User-ID) are used for user identification, the system shall only use numbers (i.e., no "#" or "*") when assigning the PIN (User-ID). NOTE: The uniqueness rules for the PIN (User-ID) are the same as for any User-ID as described in the following requirements.

d. **[Required: MFSS, SS, LSC, MG, EBC, R, EI, LS]** The system shall be capable of ensuring that all authorized users and customers have unambiguous user-IDs, such as MAC addresses or usernames, for identification purposes to support individual accountability, auditability, and access privilege.

(1) **[Required: MFSS, SS, LSC, MG, EBC, R, EI, LS]** The system shall be capable of supporting the unambiguity of a user-ID. This implies that the system shall prevent an appropriate administrator from creating (e.g., by mistake) a user-ID that already exists.

e. **[Required: MFSS, SS, LSC, MG, EBC, R, LS]** At any given instance of time, the system shall be capable of internally maintaining the identity of all user-IDs logged on at that time.

(1) **[Required: MFSS, SS, LSC, MG, EBC, R, LS]** The system shall be capable of associating a process that is invoked by a user or customer with the user-ID of that user.

(2) **[Required: MFSS, SS, LSC, MG, EBC, R, LS]** The system shall be capable of associating a process that is invoked by another process, with the ID of the invoking process.

(3) **[Required: MFSS, SS, LSC, MG, EBC, R, LS]** The system shall be capable of associating an autonomous processes (i.e., processes running without user or customer invocation) with an identification code (e.g., "system ownership").

NOTE: An example of this would be a daemon on a UNIX workstation.

f. **[Required: MFSS, SS, LSC, MG, EBC, R, LS]** A system shall have the capability to disable (as distinct from deleting) a user-ID after a configurable specified time interval, if that user-ID has never been used during that time interval.

(1) **[Required: MFSS, SS, LSC, MG, EBC, R, LS]** This capability shall be either an autonomous disabling of the user-ID by the system, or an alarm/alert generated by the system for an appropriate administrator who then, depending on the policy, may disable the user-ID by using appropriate commands.

(2) **[Required: MFSS, SS, LSC, MG, EBC, R, LS]** A disabled login ID shall not be re-enabled by the user or another application user.

g. **[Required: MFSS, SS, LSC, MG, EBC, R, LS]** The system shall have the capability to configure the default time interval for disabling a user-ID that has not been used during that time interval. The default time interval shall be 90 days In addition to disabling the user, the system shall be capable of sending an alert to the system security administrator.

h. **[Required: MFSS, SS, LSC, MG, EBC, R, LS]** The system shall be capable of verifying that a specified user (e.g., administrator) is only connected to the system a configurable number of times.

(1) **[Required: MFSS, SS, LSC, MG, EBC, R, LS]** An attempt for a specified user (e.g., administrator) to logon to the network a configurable number of times shall cause an alarm to be sent to the NMS unless an exception is granted per site policy.

i. **[Required: MFSS, SS, LSC, MG, EBC, R, EI, LS]** The system shall be capable of allowing the system security administrator to configure the number of consecutive failed logins for a user before the login procedure shall exit and end the attempted session. The number of times shall be between two and five and the default shall be three.

NOTE: The exception to these requirements is found in the emergency access requirements (Sections 5.4.6, paragraph 1 (l) and (m)).

(1) **[Required: MFSS, SS, LSC, MG, EBC, R, EI, LS]** The system shall be capable of immediately notifying the user of a failed login (i.e., “Login Failed”). The error feedback generated by the system after the user authentication procedure shall provide no information other than “invalid,” (i.e., it shall not reveal which part of the user-entered information (user-ID

and/or authenticator) is incorrect). Information such as "invalid user ID" or "invalid password" shall not be reported.

NOTE: It is acceptable to return a generic message such as "Account Locked" or "Account Disabled."

(2) **[Required: MFSS, SS, LSC, MG, EBC, R, EI, LS]** The system shall be capable of allowing a locked out user to be re-enabled by a configurable timer or manually by an application security administrator, a system administrator, or a system security administrator.

(a) **[Required: MFSS, SS, LSC, MG, EBC, R, EI, LS]** The default for the lock-out duration shall be configurable and the default shall be 60 seconds when the threshold for incorrect user-entered information has been exceeded. (This is because longer delays can be used to temporarily disrupt the service by systematically locking out all input ports.)

(3) **[Required: MFSS, SS, LSC, MG, EBC, R, EI, LS]** The system shall be capable of providing a mechanism to immediately notify (in real time) an appropriate administrator when the threshold for incorrect user-entered information is exceeded.

(4) **[Required: MFSS, SS, LSC, MG, EBC, R, EI, LS]** When the threshold for incorrect user-entered information has been exceeded, the system shall not, as a default arrangement, suspend the associated user-ID. (This is because suspension of user-IDs can be used to systematically disable all user-IDs.)

5.4.6.2.1.3 User Roles

1. **[Required: MFSS, SS, LSC, MG, EBC, R, LS, EI]** The system shall be capable of having different types of user's roles.

NOTE: Section 5.4.5.2.1, User Roles, defines the different types of user roles. A vendor may rename the user roles as long as the requirements are met. The user roles are used for the purposes of originating VVoIP sessions and for network management functions.

a. **[Required: MFSS, SS, LSC]** The system shall be capable of having at least five types of user roles: A system security administrator, a system administrator, an application administrator, a privileged application user, and an application user.

b. **[Required: R, LS, EBC, MG]** The system shall be capable of having at least three types of user roles: A system security administrator, a system administrator, and an application administrator.

c. **[Required: EI]** The system shall be capable of supporting at least three types of user roles: a system administrator, a privileged application user, and an application user.

NOTE: The system demonstrates the ability to support a privileged application user by being able to dial precedence digits to signal the LSC the precedence of the session.

d. **[Required: EI]** The system shall be capable of setting the default user precedence VVoIP session origination capability as ROUTINE.

e. **[Required: MFSS, SS, LSC, MG, EI]** The system default user role shall be an application user.

f. **[Required: R, LS, EBC]** The system default user role shall be a limited system administrator.

g. **[Required: MFSS, SS, LSC, MG, EBC, R, LS, EI]** The system shall be capable of working properly without Super User access privileges for any user application roles (system security administrator, a system administrator, an application administrator, and application user).

h. **[Required: MFSS, SS, LSC, MG, EBC, R, LS, EI]** The system shall support appropriate system administrator functions as "separate" from other user functions.

(1) **[Required: MFSS, SS, LSC, MG, EBC, R, LS, EI]** The security functions performed by an appropriate administrator shall be identified and documented.

(2) **[Conditional: MFSS, SS, LSC, MG, EBC, R, LS, EI]** If the ability to enable or disable the administrator's account is an option of a system, the systems shall not require that the account be enabled or activated during normal operation.

(3) **[Required: MFSS, SS, LSC, MG, EBC, R, LS]** The system shall be capable of providing a mechanism for the appropriate administrator to perform the following functions:

(a) Display all users currently logged onto the system.

(b) Independently and selectively monitor (in real time) the actions of any one or more users, based on individual user identity.

(c) Monitor the activities of a specific terminal, port, or network address in real time.

(d) Authorize users.

(e) Revoke users.

(f) Lock out and restore a specific port or interface.

(g) Identify all resources accessible to any specific user along with the associated privileges required to access them. NOTE: Resources (i.e., files, applications, processes, etc.) should be denied to users unless specifically authorized access.

(h) Deny the creation of a user-ID that is already in use.

(i) Disable a user-ID after a specific period of time during which the user-ID has not been used.

(j) Reinstate a disabled user-ID.

(k) Delete a disabled user-ID.

(l) Create or modify a password associated with a user-ID.

(m) Delete a user-ID along with its password.

(n) Prevent the retrieval of a password in clear text.

(o) Define a password aging interval.

(p) Define the interval during which an expired password of a user shall be denied reusing a password.

(q) Define the events that may trigger an alarm, the levels of alarms, the type of notification, and the routing of the alarm.

(r) Define the duration of session lock-out, which occurs when the threshold on the number of incorrect logins is exceeded.

(s) Specify a customized advisory warning banner that is displayed upon valid system entry.

(t) Define the duration of the time-out interval.

(u) Define the privilege of a user to access a resource.

(v) Define the privilege of an interface/port to be used to access a resource.

(w) Permit post-collection audit analysis tools for report generation.

(x) Permit the retrieval, copying, printing, or uploading of the security log.

(y) Deny the ability to modify or delete the security log.

(z) Provide a mechanism to specify the condition that would necessitate uploading the security log to avoid an overwrite in the buffer.

(aa) Provide a capability to validate the correct operation of the system.

(bb) Provide a capability to monitor the system resources and their availabilities.

(cc) Provide a capability to detect communication errors above an administrator defined threshold.

i. **[Required: MFSS, SS, LSC, MG, EBC]** The system shall be capable of ensuring that a user's role or precedence ability has not changed during the execution or exit from an application.

NOTE: The user shall not be able to use a control sequence mechanism, for example, shell escape to a SUPERUSER mode. Or, if the application fails, it must not leave the user in a different role with more privileges. The user must reauthenticate (relog-in) in order to

assume a different role. If a system administrator has granted a user role limited root access (e.g., *sudo* for UNIX) it is part of that person's user role. This primary method to mitigate the threats associated with this requirement is to use industry best practices when developing the system.

j. **[Required: MFSS, SS, LSC, MG, EBC, R, LS]** The system shall only transmit passwords that are encrypted.

NOTE: The Backbone Transport Services STIG requires that router administrative passwords are hashed using MD5.

k. **[Required: MFSS, SS, LSC, MG, EBC, R, LS]** The system shall be capable of limiting user access based on a time of day interval (i.e., duty hours).

5.4.6.2.1.4 Ancillary Equipment

1. **[Conditional: MFSS, SS, LSC, MG, EBC, R, LS, EI]** Systems that use ancillary AAA and syslog services shall do so in a secure manner.

a. **[Conditional: MFSS, SS, LSC, MG, EBC, R, LS, EI]** Systems that use external Authentication, Authorization, and Accounting (AAA) services provided by the Diameter Base Protocol shall do so in accordance with RFC 3588.

NOTE: An external AAA service is a service that is extends beyond the boundary of the system.

(1) **[Conditional: MFSS, SS, LSC, MG, EBC, R, LS, EI]** Systems that act as Diameter Agents shall be capable of being configured as Proxy Agents.

(a) **[Conditional: MFSS, SS, LSC, MG, EBC, R, LS, EI]** Systems that act as Proxy Agents shall maintain session state.

(2) **[Conditional: MFSS, SS, LSC, MG, EBC, R, LS, EI]** All Diameter implementations shall ignore answers received that do not match a known Hop-by-Hop Identifier field.

(3) **[Conditional: MFSS, SS, LSC, MG, EBC, R, LS, EI]** All Diameter implementations shall provide transport of its messages in accordance with the transport profile described in RFC 3539.

(4) **[Conditional: MFSS, SS, LSC, MG, EBC, R, LS, EI]** Systems that use the Extensible Authentication Protocol (EAP) within Diameter shall do so in accordance with RFC 4072.

b. **[Conditional: MFSS, SS, LSC, MG, EBC, R, LS, EI]** Systems that use external AAA services provided by the Remote Authentication Dial In User Service (RADIUS) shall do so in accordance with RFC 2865.

NOTE: The use of Diameter is preferred. Future requirement revisions may mandate the use of Diameter.

(1) **[Conditional: MFSS, SS, LSC, MG, EBC, R, LS, EI]** Systems that use the Extensible Authentication Protocol (EAP) within RADIUS shall do so in accordance with RFC 3579.

(2) **[Conditional: MFSS, SS, LSC, MG, EBC, R, LS, EI]** If the systems support RADIUS based accounting, the system shall do so in accordance with RFC 2866.

(3) **[Conditional: MFSS, SS, LSC, MG, EBC, R, LS, EI]** If the system supports RADIUS, it shall support the use of IPsec and/or TLS using non-null transforms as defined in the confidentiality section of this UCR 2008 (Section 5.4.6, Requirements).

(4) **[Conditional: MFSS, SS, LSC, MG, EBC, R, LS, EI]** If the system supports RADIUS and IPsec, it shall support the use of IKE for key management as defined in the confidentiality section of this UCR 2008 (Section 5.4.6, Requirements).

c. **[Conditional: MFSS, SS, LSC, MG, EBC, R, LS, EI]** Systems that use external AAA services provided by the Terminal Access Controller Access Control System (TACACS+) shall do so in accordance with the TACACS+ Protocol Specification 1.78 (or later). NOTE: The intent is to use the most current specification. The use of Diameter is preferred. Future requirement revisions may mandate the use of Diameter.

(1) **[Conditional: MFSS, SS, LSC, MG, EBC, R, LS, EI]** If the system supports TACACS+, it shall support the use of IPsec and/or TLS using non-null transforms as defined in the confidentiality section (Section 5.4.6, Requirements).

(2) **[Conditional: MFSS, SS, LSC, MG, EBC, R, LS, EI]** If the system suppoTACACS+ and IPsec, it shall support the use of IKE for key management as defined in the confidentiality section (Section 5.4.6, Requirements).

d. **[Conditional: EI]** Systems that use external address assignment services provided by the Dynamic Host Control Protocol (DHCP) shall do so in accordance with RFC 2131.

NOTE: An external address assignment service is a service that extends beyond the boundary of the system.

(1) **[Conditional: EI]** Systems that act as DHCP clients upon receipt of a new IP address shall probe (e.g., with ARP) the network with the newly received address to ensure the address is not already in use.

NOTE: The actions to take if a duplicate address is detected are found in RFC 2131.

(2) **[Conditional: EI]** Systems that act as DHCP clients upon receipt of a new IP address shall broadcast an ARP reply to announce the client's new IP address and clear outdated ARP cache entries in hosts on the client's subnet.

e. **[Conditional: R, LS, EI]** Systems that use external AAA services provided by port based network access control mechanisms shall do so in accordance with IEEE 802.1X-2004 in combination with a secure Extensible Authentication Protocol (EAP) type (EAP-TLS, EAP-TTLS, or PEAP).

(1) **[Conditional: R, LS, EI]** Systems that use external EAP services provided by EAP shall do so in accordance with RFC 3748 and its RFC extensions.

(a) **[Conditional: R, LS, EI]** Systems that support EAP as a minimum shall support authentication using shared secrets.

NOTE: RFC 3748 requires that systems support Identity, Notification, Nak, and MD-5 Challenge Request/Response exchanges.

f. **[Conditional: MFSS, SS, LSC, MG, EBC, R, LS]** Systems that use external syslog services shall do so in accordance with RFC 3164.

NOTE: It is understood that an Internet Draft is written that will deprecate RFC 3164, but that draft is new and it is unknown whether it will be approved.

(1) **[Conditional: MFSS, SS, LSC, MG, EBC, R, LS]** Systems that support syslog shall use UDP port 514 for the source port of the sender when using UDP for transport.

(2) **[Conditional: MFSS, SS, LSC, MG, EBC, R, LS]** Systems that support syslog shall transmit messages in the format defined by RFC 3164.

(3) **[Conditional: MFSS, SS, LSC, MG, EBC, R, LS]** Systems that support syslog shall have all the parts of the syslog packet as described in Section 4.1 of RFC 3164.

(a) **[Conditional: MFSS, SS, LSC, MG, EBC, R, LS]** If the originally formed message has a TIMESTAMP in the HEADER part, then it shall be the local time of the device within its time zone.

(b) **[Conditional: MFSS, SS, LSC, MG, EBC, R, LS]** If the originally formed message has a HOSTNAME field, then it shall contain the hostname as it knows itself. If it does not have a hostname, then it shall contain its own IP address.

(c) **[Conditional: MFSS, SS, LSC, MG, EBC, R, LS]** If the originally formed message has a TAG value, then it shall be the name of the program or process that generated the message.

(4) **[Conditional: MFSS, SS, LSC, MG, EBC, R, LS]** If systems use TCP for the delivery of syslog events, then the system shall do so in accordance with the RAW profile defined in RFC 3195.

NOTE: It is understood that an Internet Draft is written that will deprecate RFC 3195, but that draft is new and it is unknown whether it will be approved.

5.4.6.2.1.5 Authentication Practices

1. **[Required: MFSS, SS, LSC, MG, EBC, R, LS, EI]** The system shall be capable of authenticating users and appliances.

a. **[Required: MFSS, SS, LSC, MG, EBC, R, EI, LS]** The system shall only allow authenticated users and appliances to access the system.

(1) **[Required: MFSS, SS, LSC, MG, EBC, R, EI, LS]** The system shall ensure that authentication credentials are not transmitted in the "clear" (i.e., credentials are encrypted end-to-end).

NOTE: The PKI certificate does not fall under this requirement due to the nature of the public key authentication model.

(2) **[Required: MFSS, SS, LSC, MG, EBC, R, LS]** The system shall be capable of ensuring that system access points that provide remote login facility also provide authentication services that are capable of utilizing authentication mechanisms that are stronger than usernames and passwords (i.e., using two factor authentication(strong authentication)).

(3) **[Required: LSC]** The system shall be capable of authenticating the EI using TLS (or its equivalent) (Threshold) and/or with PKI certificates.

NOTE: This assumes the EI is served directly by the appliance.

(4) **[Required: EI]** The system shall be capable of authenticating the LSC using TLS (or its equivalent) (Threshold) and/or with PKI certificates.

b. **[Required: MFSS, SS, LSC, MG, EBC, R, LS]** The system shall be capable of authenticating an appliance using the DoD Public Key Infrastructure (PKI).

NOTE: The EI authentication is excluded from this requirement in FY08.

(1) **[Conditional: LSC, SS, EBC, MFSS, EI]** If the system is PKE, then the system shall use the DoD PKI certificates with the associated public key in the TLS certificate message for authenticating appliance when using AS-SIP.

NOTE: Some options considered to meet this requirement include the use of On-line Status Check and certificate trust lists as discussed in Section 5.4.5.2.7 paragraph 1(g).

(2) **[Conditional: MFSS, SS, LSC, MG, EBC]** If the system supports web browsers and web servers, the system shall be capable of using DoD PKI certificates with the associated public key in the TLS certificate message for authenticating users.

c. **[Required: MFSS, SS, LSC, MG, EBC, R, EI, LS]** The system shall be capable of ensuring that user authentication for logging in, logging, and auditing of an appliance shall be at least as strong as a user-ID and the appropriate password/PIN (user-ID) entered over a previously established trusted path.

NOTE: The previously established trusted path ensures that the password is not transmitted in the clear. It is acceptable for systems to use RADIUS, TACACS+, or DIAMETER for AAA services.

d. **[Required: MFSS, SS, LSC, MG, EBC, R, EI, LS]** The system shall not support ways to bypass the deployed authentication mechanism.

e. **[Required: MFSS, SS, LSC, MG, EBC, R, EI, LS]** The system shall perform the entire user authentication procedure even if the user-ID that is entered is not valid.

NOTE: The notification requirements associated with a failed login are covered in the other requirements in this section of the UCR 2008.

f. **[Required: MFSS, SS, LSC, MG, EBC, R, EI, LS]** The system shall protect (i.e., encrypt) all internal storage of authentication data to ensure confidentiality.
NOTE: This requirement is not meant to preserve session keys during a power cycle. It is primarily meant to ensure that an intruder that gains access to the system is not able to view the authentication information in clear text.

g. **[Required: EI]** The system shall be capable of allowing users to place ROUTINE precedence and emergency calls without authenticating.

h. **[Required: EI]** The system shall only allow authenticated users to access the system for services above the ROUTINE precedence.

(1) **[Conditional: LSC, EI]** If the system uses SIP, the system shall use digest authentication as specified in RFC 3261 and/or with PKI certificates for authenticating user credentials to the LSC via the EI.

NOTE: The LSC is responsible for the authentication decisions. The method for authenticating a user with their PKI certificate is a vendor decision due to the immaturity of the current standards. Vendors may choose to implement user authentication using PKI certificates as described in RFC 3261 or as described in RFC 3893.

(2) **[Required: LSC, EI]** The user authentication mechanism shall be software enabled or disabled.

NOTE: In certain deployments, the user does not have the time to input authentication credentials and the EI is located in a secure environment where credentials are not necessary due to the mission. By default this capability will be disabled to allow users to place calls without authenticating.

(a) **[Required: EI (Softphone)]** If the system is a softphone, the system shall provide user authentication by presenting the CAC credentials of the user to the LSC.

i. **[Required: EI]** The system shall only allow an authenticated system administrator to perform configuration functions.

NOTE: This requirement is focused on network and LSC configuration items and is not meant to preclude users from personalizing the phone through configuration items like volume control (to include mute), speakerphone enable/disable (if originally enabled by the system administrator), headset enable/disable, LCD contrast, voice mail features, speed dial and call forwarding features.

i. **[Required: EI]** The system shall not display configuration information without proper authentication.

NOTE: The minimum requirement for authentication is defined UCR 2008, Section 5.4.6.2.1.5, Authentication Practices, paragraph 1.c.

j. **[Required: MFSS, SS, LSC, MG, EBC, R, LS]** The system shall be capable of ensuring that all ports on a system that support operations related command inputs (e.g., SNMP SET commands) exercise strong authentication mechanisms for access control.

k. **[Required: MFSS, SS, LSC, MG, EBC, R, LS]** The system shall be capable of ensuring that all appliances that support connection-oriented communications also support mutual authentication between the requestor and the provider.

NOTE: A connection-oriented communication is a session between two VVoIP appliances where the Transport Layer Protocol sends acknowledgments to the sender regarding incoming data. This type of session usually provides for retransmission of corrupted or lost data.

l. **[Required: EI]** The system shall properly operate when auto-registration is disabled.

NOTE: Auto-registration is typically used during initial installation of large numbers of EIs. It involves the automatic registration of EIs to the LSC, automatic assignment of IP assignment of IP addresses and user-IDs, and automatic download of application files. Typically, auto-registration is disabled after installation and manual changes are made.

m. **[Required: MFSS, SS, LSC, MG, EBC, R, LS]** The default authentication mechanism for SNMPv3 shall be HMAC-SHA-96.

5.4.6.2.1.6 Public Key Infrastructure

1. **[Required: MFSS, SS, LSC, MG, EBC, R – Conditional: EI]** The system shall be capable of meeting the DoD Public Key Enabled (PKE) requirements for PKI based authentication.

NOTE: The requirement for an EI to be PKE is conditional for FY2008, but will be required for FY12. The condition for FY2008 is that if the EI is PKE, it shall meet the PKE requirements.

a. **[Required: MFSS, SS, LSC, MG, EBC, R – Conditional: EI]** The system shall be capable of generating asymmetric (public and private) key pairs and symmetric keys.

(1) **[Required: MFSS, SS, LSC, MG, EBC, R – Conditional: EI]** The system shall be capable of generating asymmetric keys whose length is at least 1024 for RSA.

(2) **[Required: MFSS, SS, LSC, MG, EBC, R – Conditional: EI]** The system shall be capable of generating symmetric keys whose length is at least 128 bits.

(a) **[Required: MFSS, SS, LSC, MG, EBC, R – Conditional: EI]** The system shall be capable of distributing keys used for symmetric encryption out-of-band or by secure cryptographic processes that comply with in FIPS 140-2.

(3) **[Required: MFSS, SS, LSC, MG, EBC, R – Conditional: EI]** The system shall be capable of generating keys using a random source algorithm that meets the requirements of FIPS 186.

b. **[Required: MFSS, SS, LSC, MG, EBC, R – Conditional: EI]** The system shall be capable of storing key pairs and their related certificates.

(1) **[Required: MFSS, SS, LSC, MG, EBC, R – Conditional: EI]** The system shall be capable of storing certificates for a subscriber.

NOTE: A subscriber may be itself, another appliance, or a user of the system. The certificates may have the same public key and may be associated with different issuers, different uses, or different validity periods. The certificates are stored on the appliance for a variety of reasons including for historical purposes. This requirement is for local authentication of the user and is not meant to obtain the private key of the subscriber.

(2) **[Required: MFSS, SS, LSC, MG, EBC, R – Conditional: EI]** The system shall be capable of protecting the private key from compromise or loss.

NOTE: The requirement may be satisfied by meeting the requirements of FIP 140-2 for protecting keys.

(a) **[Conditional: MFSS, SS, LSC, MG, EBC, R, EI]** If the certificate shall be used for non-repudiation purposes, the system shall be capable of ensuring that all copies of private keys generated for actual or possible non-repudiation purposes are under the owning entity's sole control.

NOTE: A subsequent requirement mandates that the system is capable of using the certificate for non-repudiation by setting the key usage extension for non-repudiation. An example of a need for non-repudiation is to verify that a user made a malicious configuration change on the platform.

(b) **[Required: MFSS, SS, LSC, MG, EBC, R, EI]** The system shall be capable of meeting the requirements for level 1 of FIPS 140-2 in FIPS Mode (i.e., approved for federal government use as opposed to commercial use).

NOTE: Where the requirements listed are more secure than FIPS 140-2, UCR 2008 requirements supersedes FIPS 140-2.

(c) **[Conditional: MFSS, SS, LSC, MG, EBC, R, EI]** If the system performs operations with the unencrypted key in software, the system shall be capable of encrypting or destroying the key as soon as the operation is complete.

(d) **[Conditional: MFSS, SS, LSC, MG, EBC, R, EI]** If passwords are used to protect private keys, the system shall be capable of ensuring that the password is selected from a space of at least 2^{56} possible passwords unless there is a means to detect and protect against deliberate attempts to search for passwords.

NOTE: This requirement is meant to prevent a malicious user from using password guessing to gain access to the private keys. The requirement may be met by meeting the requirement defined in requirements Section 5.4.5.2, Authentication.

(e) **[Required: MFSS, SS, LSC, MG, EBC, R – Conditional: EI]** The system shall operate with DoD trust points.

NOTE: Trust points are defined in UCR 2008, Appendix A, Definitions, Abbreviations and Acronyms, and References.

i. [Required: MFSS, SS, LSC, MG, EBC, R – Conditional: EI] The system shall authenticate up to a trust point.

ii. **[Conditional: MFSS, SS, LSC, MG, EBC, R, EI]** If the trust point is not established, the system shall authenticate to the root certificate or certification authority (CA).

c. **[Required: MFSS, SS, LSC, MG, EBC, R – Conditional: EI]** The system shall be capable of protecting certificates that are trust points.

NOTE: Methods used to protect trust points include restricting access to and use of this capability to designated individuals.

d. **[Required: MFSS, SS, LSC, MG, EBC, R – Conditional: EI]** The system shall be capable of generating and submitting certificate requests in accordance with methods described in the DoD Class 3 PKI Interface Specification.

(1) **[Required: MFSS, SS, LSC, MG, EBC, R – Conditional: EI]** The system shall be capable of using HTTPS to request and obtain certificates for the subscriber.

(a) **[Required: MFSS, SS, LSC, MG, EBC, R – Conditional: EI]** The system shall be capable of encrypting and decrypting using the Triple Data Encryption Algorithm (TDEA).

e. **[Required: MFSS, SS, LSC, MG, EBC, R – Conditional: EI]** The system shall be capable of importing key pairs, related certificates, and certificate revocation information.

(1) **[Required: MFSS, SS, LSC, MG, EBC, R – Conditional: EI]** The system shall be capable of using the Lightweight Directory Access Protocol (LDAP) or HTTP or HTTPS when communicating with the DoD PKI.

(2) **[Required: MFSS, SS, LSC, MG, EBC, R – Conditional: EI]** The system shall be capable of accepting needed old certificates (i.e., certificates that have expired or been revoked) and CRLs (Certificate Revocation List) (i.e., CRLs whose next update is after the current date) from the DoD PKI archive using HTTPS.

(3) **[Required: MFSS, SS, LSC, MG, EBC, R]** The system shall be capable of requesting and accepting information regarding the status of certificates using CRLs or the On-line Status Check (OSC).

(a) **[Conditional: MFSS, SS, LSC, MG, EBC, R]** If CRLs are used, the system shall be capable of using a configurable parameter to define the period associated with updating the CRLs.

i. **[Conditional: MFSS, SS, LSC, MG, EBC, R]** If CRLs are used, the default value for the period associated with updating the CRLs shall be 24 hours.

(4) **[Conditional: EI]** If the EI is DoD PKE, it shall support a mechanism for verifying the status of an LSC certificate using a Certificate Trust List (CTL) or via the OSC.

NOTE: It is understood that the systems administer must ensure that the CTL is current to ensure that the status is accurate.

(5) **[Conditional: LSC]** If the EI is DoD PKE, the LSC shall verify the status of an EI certificate using the CTL or a OSC.

NOTE: It is understood that the systems administer must ensure that the CTL is current to ensure that the status is accurate.

f. **[Required: MFSS, SS, LSC, MG, EBC, R – Conditional: EI]** The system shall be capable of performing public key operations necessary to verify signatures on DoD PKI signed objects (i.e. certificates, CRLs, and OSC responses).

(1) **[Required: MFSS, SS, LSC, MG, EBC, R – Conditional: EI]** The system shall be capable of producing SHA digests of messages to support verification of DoD PKI signed objects.

(2) **[Required: MFSS, SS, LSC, MG, EBC, R – Conditional: EI]** The system shall reject all new sessions associated with a revoked certificate.

(3) **[Required: MFSS, SS, LSC, MG, EBC, R]** The system shall log when a session is rejected due to a revoked certificate.

g. **[Required: MFSS, SS, LSC, MG, EBC, R – Conditional: EI]** The system shall be capable of supporting the development of a certificate path and be able to process the path.

NOTE: The path development process produces a sequence of certificates that connect a given end-entity certificate to a trust point. The process terminates when either the path tracks from a trust point to an end entity or a problem occurs that prohibits validation of the path.

(1) **[Required: MFSS, SS, LSC, MG, EBC, R – Conditional: EI]** The system shall be capable of verifying certificate signatures using the certificate issuer's public key.

(2) **[Required: MFSS, SS, LSC, MG, EBC, R – Conditional: EI]** The system shall be capable of ensuring that the effective date falls within the certificate's validity period.

NOTE: The effective date is the date when the transaction was initiated. Normally, the effective date should be considered the current date unless reliable evidence exists to establish an earlier effective date.

(3) **[Required: MFSS, SS, LSC, MG, EBC, R – Conditional: EI]** The path process shall fail when a problem that prohibits the validation of a path to occur.

(4) **[Required: MFSS, SS, LSC, MG, EBC, R – Conditional: EI]** The system shall be capable of ensuring the validity of certificates through a status check. NOTE: The status check is done at the time the certificate is presented to the appliance. Status checking involves checking the status of certificates in the path to ensure that none are revoked.

(a) **[Required: MFSS, SS, LSC, MG, EBC, R – Conditional: EI]** The system shall be capable of verifying the signature of the CRL or the OSC response.

i. **[Conditional: MFSS, SS, LSC, MG, EBC, R, EI]** If the system uses the OSC to validate a certificate and the system cannot contact the OSCR and backup OSCRs, the system will continue the process, but will log the event and send an alarm to the NMS.

(b) **[Required: MFSS, SS, LSC, MG, EBC, R – Conditional: EI]** The system shall be capable of verifying that the CRL has not expired (even if the target certificate has not expired) or shall be capable of verifying that the OSC response indicates the certificate is valid. NOTE: The intent of this requirement is to ensure that the OSCR or CRL is valid prior to completing the status check.

(c) **[Required: MFSS, SS, LSC, MG, EBC, R – Conditional: EI]** The system shall be capable of searching the list of revoked certificates to determine that the target certificate is not included or the revocation date is after the effective date.

(d) **[Required: MFSS, SS, LSC, MG, EBC, R – Conditional: EI]** The system shall be capable of rejecting expired certificates.

NOTE: An example of this case would exist if a certificate's effective date is reliable, but the certificate has since expired.

(e) **[Required: MFSS, SS, LSC, MG, EBC, R]** The system shall log an event if the certificate is rejected due to a status check.

(5) **[Required: MFSS, SS, LSC, MG, EBC, R – Conditional: EI]** The system shall be capable of ensuring that the intended use of the certificate is consistent with the DoD PKI extensions.

(6) **[Required: MFSS, SS, LSC, MG, EBC, R – Conditional: EI]** The system shall be capable of ensuring that the key usage extension in the end entity certificate is properly set.

(a) **[Required: MFSS, SS, LSC, MG, EBC, R – Conditional: EI]** The system shall be capable of ensuring that the digital signature bit is set for authentication uses.

(b) **[Required: MFSS, SS, LSC, MG, EBC, R – Conditional: EI]** The system shall be capable of ensuring that the non-repudiation bit is set for non-repudiation uses.

(c) **[Required: MFSS, SS, LSC, MG, EBC, R – Conditional: EI]** The system shall be capable of ensuring that the "common name" and "subject alternate name" fields are populated.

NOTE: The "subject alternate name" should be formatted in accordance with RFC 2459, and it should contain as a minimum the elements of the "common name."

5.4.6.2.1.7 Authorization

1. **[Required: MFSS, SS, LSC, MG, EBC, R, EI, LS]** The system shall be capable of providing authorization for services accessed on the system.

   a. **[Required: MFSS, SS, LSC, MG, EBC, R, LS]** The system shall be capable of denying system access to any user unless identified with a user-ID and authenticated. Only authorized users shall be allowed system access. This holds for all users (i.e., persons, processes, or remote systems).

   NOTE: This requirement applies to multiple access types to include remote login, telephony services, and direct system access. However,911 and emergency service needs may result in this requirement being exempt on some end instruments.

   b. **[Required: MFSS, SS, LSC, MG, EBC, R, EI, LS]** The system shall not allow the user to access a resource unless that user's user-ID has an appropriate privilege to access that resource.

NOTE: ROUTINE and above VVoIP sessions may be authorized for all users of the system and this feature may be disabled if the systems are located in secure facilities for precedence sessions.

(1) **[Required: LSC, MFSS, SS]** The system shall only forward a signaling message when the forwarding destination is authorized. NOTE: This is to ensure that sessions are not forwarded to an unauthorized destination. This includes on-net and off-net destinations.

c. **[Required: R, LS, EBC]** The system shall be capable of regulating remote access by employing positive technical controls such as proxies and screened subnets.

NOTE: Proxies and screened subnets are provided using border controllers, access control lists, firewalls, and virtual LANs.

d. **[Required: R, LS, EBC]** The system shall be capable of configuring proxies and screened subnets to limit access to only approved, network service classes and configured traffic levels for the authenticated users and end instruments. NOTE: Proxies and screened subnets are provided by using border controllers, access control lists, firewalls, and virtual LANs. Network service classes are defined by the QoS WG, and they may consist of voice, video, and data service classes.

(1) **[Required: R, LS, EBC]** The system shall have the capability of controlling the flow of traffic across an interface to the network based on the source/destination IP address, source/destination port number, DSCP, and protocol identifier ("6 tuple").

(a) **[Required: EBC]** The system shall have the capability of opening and closing "gates/pinholes" (i.e., packet filtering based on the "6 tuple") based on the information contained within the SDP body of the AS-SIP messages.

i. **[Required: EBC]** The system shall have the capability to close a "gate/pinhole" based on a configurable media inactivity timer and issue a BYE message to upstream and downstream AS-SIP signaling appliances (lost BYE scenario).

NOTE: The inactivity timer is based on the inactivity of the media stream.

A. **[Required: EBC]** The default media inactivity value for closing a session and issuing BYE messages shall be 15 minutes.

(2) **[Required: R, LS]** The system shall be capable of utilizing VLANs to segregate VVoIP and data traffic. Servers requiring access to multiple VLANs shall be kept in a DMZ connected to the firewall and separating the two VLANs.

NOTE: For the purposes of this UCR 2008, all streams of packets associated with a VTC session are considered video to include voice, video, and data streams. A DMZ, in this context, may exist between two VLANs within the Edge Segment.

(a) **[Required: R, LS]** The system shall be capable of supporting a minimum of five (5) distinct VLANs for VVoIP.

(b) **[Required: LS, R]** The system shall be capable of ensuring that EIs (that do not contain a multi-port switch) and VVoIP appliances are only connected to switchports with access to the VVoIP VLAN(s).

NOTE: This requirement is not applicable to an EI with an embedded multi-port switch.

(c) **[Conditional: EI]** If the system supports a data workstation, then the system shall be capable of supporting 802.1Q Trunking to separate VVoIP and data traffic, or it shall have a separate Network Interface Card (NIC) for the data and the VVoIP.

NOTE: The intent of this requirement is to prevent the workstation from accessing or viewing the voice traffic as well as to prevent the workstation from accessing the EI for configuration purposes.

i. **[Conditional: EI]** If the system supports a data workstation, then the system shall be capable of using separate 802.1Q VLAN tags for VVoIP and data or shall use separate NICs for the data and VVoIP interfaces.

ii. **[Conditional: EI]** If the system supports a data workstation, then the system shall be capable of routing the VVoIP and data traffic to the appropriate VLAN.

NOTE: This requirement differs from the previous requirement in that the previous requirement involves marking the packet and this requirement is focused on what action to take based on the marking or the output NIC.

(d) **[Required: R, LS]** The system shall be capable of configuring the maximum number of MAC addresses that can be dynamically configured on a given switchport (e.g., 1-3).

i. **[Required: R, LS]** The system shall be capable of notifying the NMS when the MAC address tables threshold is reached to avoid an overflow.

(e) **[Required: R, LS]** The system shall be capable of segregating softphones to a dedicated VLAN.

(f) **[Required: R, LS]** The system shall be capable of segregating signaling appliances to a dedicated VLAN.

(g) **[Required: R, LS]** The system shall be capable of segregating PSTN gateways to a dedicated VLAN.

(h) **[Required: R, LS]** The system shall be capable of segregating NMS appliances on a separate VLAN.

(3) **[Required: R, LS, EBC]** The system shall have the capability to deploy on a dedicated IP network(s) or subnetwork(s) that utilize separate address blocks from the normal data address blocks thus allowing traffic and access control via firewalls and router ACLs.

(a) **[Required: EBC]** The system shall be capable of using NAT and NAPT on all VVoIP enclave to WAN connections.

i. **[Required: R, EBC]** The system shall have the capability to deploy using private address space in accordance with RFC 1918.

ii. **[Required: EBC]** The EBC shall be an AS-SIP intermediary in all WAN signaling sessions.

A. **[Required: EBC]** To enable the application of NAT and NAPT, the EBC shall be able to inspect and modify

the SDP body (i.e., the SDP "c=" and the "m=" lines) of the corresponding AS-SIP message.

iii. **[Conditional: EBC]** If the system supports H.323 video sessions, the EBC shall be capable of supporting H.323 NAT and NAPT.

(b) **[Required: R, LS, EBC]** The system shall have the capability to be configured to ensure that the data network perimeter (i.e., data edge router or data perimeter firewall) blocks all external traffic destined to or sourced from the VVoIP VLANs and/or IP address space.

NOTE: The VVoIP VLANs may include a softphone VLAN, a non-softphone voice VLAN, and a video VLAN.

(c) **[Required: R, LS, EBC]** The system shall have the capability to limit management appliance access to the IP addresses of appropriate workstations.

(4) **[Conditional: R, LS]** If DHCP is used, the system shall have the capability to deploy different DHCP servers for VVoIP and non-VVoIP components and the DHCP servers shall be located on physically diverse platforms from the routers and LAN switches.

(5) **[Conditional: R, LS]** If DHCP is used, DHCP servers shall reside in their respective VVoIP or non-VVoIP address space and the DHCP servers shall be located on physically diverse platforms from the routers and LAN switches.

(a) **[Conditional: R, LS, EI]** If DHCP is used, the system shall be capable of using 802.1X in combination with a secure EAP type (EAP-TLS, EAP-TTLS, or PEAP) residing on the authentication server and within the operating system or application software of the EI in order to authenticate to the LAN.

i. **[Conditional: R, LS]** If 802.1X port authentication is used, the system shall ensure that all access ports start in unauthorized state. NOTE: The system should set AuthControlledPortControl equal to Auto mode for ports that will support VVoIP.

ii. **[Conditional: R, LS, EI]** If 802.1X port authentication is used, the system shall ensure that reauthentication occurs every 60 minutes.

iii. **[Conditional: R, LS, EI]** If 802.1X port authentication is used the system shall also use 802.1AE and 802.1af to ensure a continuation of the authenticated relationship continues after the 802.1X authentication event to prevent parallel attacks.

(6) **[Required: EBC]** The system shall be capable of being configured to ensure that VVoIP and non-VVoIP traffic between their respective VLANs is filtered and controlled by a stateful inspection firewall, such that traffic is restricted to planned and approved traffic between authorized devices using approved ports, protocols, and services.

NOTE: The EBC used in this case may not have the full feature set of an EBC. For instance, NAT is not required in this instance.

(7) **[Required: EBC]** The system shall have the capability to deploy VVoIP aware firewalls at all VVoIP enclave to WAN boundaries.

(a) **[Required: EBC]** The system firewalls deployed at the boundaries of the VVoIP enclave shall have the capability to employ stateful packet inspection.

(b) **[Required: EBC]** The system firewalls deployed at VVoIP enclave boundaries shall have the capability to be dedicated to VVoIP traffic.

(c) **[Required: R]** The system shall be capable of implementing traffic conditioning at all VVoIP enclaves associated with the system.

NOTE: This includes limiting the bandwidth associated with external sessions.

e. **[Required: MFSS, SS, LSC, MG, EBC, R, EI, LS]** The system documentation shall list all of the IP ports and protocols required by the system and the boundaries they transit as defined in the PPS Assurance Category Assignments List and which is maintained by DISA and is described in DoDI 8551.1.

(1) **[Required: MFSS, SS, LSC, MG, EBC, R, EI, LS]** The system shall not use IP ports and protocols deemed “red” as defined by the PPS Assurance Category Assignments List, which is maintained by DISA and is described in DoDI 8551.1.

f. **[Required: MFSS, SS, LSC, MG, EBC, R, LS]** Systems that support critical commands, operational commands or critical objects shall be capable of establishing access privileges for these objects and commands. Critical objects include authentication data storage.

(1) **[Required: MFSS, SS, LSC, MG, EBC, R, LS]** The default policy on a system that supports operations-related or critical commands shall be capable of disallowing command issuance unless the issuer has been authenticated and authorized to use that command.

(a) **[Required: MFSS, SS, LSC, MG, EBC, R, LS]** Assigning passwords to specific actions shall not be used as a primary access method.

(2) **[Required: MFSS, SS, LSC, MG, EBC, R, LS]** All portsof the system that accept operations-related or critical command inputs shall be capable of exercising system access control. This includes ports that provide direct access, dial-up access, access via a wireless interface, network access, and access via a Data Communications Channel (DCC) as in the case of an Add Drop Multiplexer (ADM) in a Synchronous Optical Network (SONET).

(a) **[Conditional: MFSS, SS, LSC, MG, EBC, R, LS]** Depending on the application, if the system is to be accessed by administrative users who need to keep this access (including the fact that an access is being made) confidential from other administrative users, such as unauthorized B/P/C/S Director of Information Management (DOIM) employees (i.e., CALEA type requirements), the system shall be capable of providing a separate interface/port for such confidential access. It shall be capable of ensuring that messages (including login requests) at this “special” interface/port are kept confidential from users logged on at other interfaces/ports.

NOTE: It is acceptable to implement the CALEA logging functions in a separate security log on a different appliance than the normal security log.

(b) **[Required: MFSS, SS, LSC, MG, EBC, R, LS]** The system shall be capable of controlling access to resources over a given interface/port on the basis of privileges assigned to that interface/port.

g. **[Required: R, LS, EBC]** The system shall have the capability of monitoring the flow of traffic across an interface to the network.

h. **[Required: MFSS, SS, LSC, MG, EBC]** The system shall have the capability to provide a secure method for allowing automatic interconnections.

NOTE: Automatic interconnection is only allowed between an incoming long-distance SBU voice call and the local commercial system (off-netting).

(1) **[Required: MFSS, SS, LSC, MG, EBC]** Automatic interconnection between DoD IP VVoIP calls and local commercial systems shall only be permitted with proper authorization.

NOTE: The authorization is granted based on successful authentication in combination with an acceptable profile allowing the interconnection.

(2) **[Required: MFSS, SS, LSC, MG, EBC]** The system shall have the capability of identifying all calls made through the automatic interconnection.

(3) **[Required: MFSS, SS, LSC, MG, EBC]** The system shall be capable of ensuring that all automatic calls are periodically verified by the user.

i. **[Required: MFSS, SS, LSC, MG, EBC, R, LS]** The NMS shall possess read-access and limited write/controlled access capabilities unless Service/agency operational command personnel are available to make changes 24X7 to all DoD IP VVoIP database tables (excluding tables associated with non-DISA controlled devices). NOTE: The intent of this requirement is to ensure that authenticated and authorized NMS personnel have limited capability to resolve issues in the event that a problem occurs and there are no on-site maintenance personnel available.

j. **[Required: MFSS, SS, LSC, MG, EBC]** The system shall have the capability to provide an identification system that allows the operators to detect and prevent disruptive fraud, abuse, and compromise within 30 minutes. (Definition of disruptive is found in UCR 2008, Appendix A, Definitions, Abbreviations and Acronyms, and References.)

NOTE: The threats associated with this requirement are summarized earlier in this UCR 2008.

(1) **[Required: MFSS, SS, LSC, MG, EBC]** The system shall have an identification system that allows operators to detect a disruptive fraud, abuse, or compromise within 5 minutes.

NOTE: The threats associated with this requirement are summarized earlier in this UCR 2008 section.

k. **[Required: MFSS, SS, LSC, EBC]** The system shall have the capability to deny system access to all session requests (i.e., disable the points of ingress) in response to appropriate messages received from the NMS.

NOTE: Sessions in this context are associated with NMS sessions, such as a SSH session.

l. **[Conditional: MFSS, SS, LSC, MG, EBC, R, LS]** If the system provides an emergency entry port (Emergency Action Interface) with system access control, the system shall have the capability to meet the following requirements:

(1) **[Required: MFSS, SS, LSC, MG, EBC, R, LS]** The system shall be capable of using strong authentication.

(2) **[Required: MFSS, SS, LSC, MG, EBC, R, LS]** The system shall log all access attempts in an audit log.

(3) **[Required: MFSS, SS, LSC, MG, EBC, R, LS]** The system shall be capable of ensuring at least one, and not more than two, system security administrator accounts cannot be locked out due to login failures.

m. **[Conditional: MFSS, SS, LSC, MG, EBC, R, LS]** If the system provides an emergency entry port without system access control then the following requirements shall be met.

(1) **[Required: MFSS, SS, LSC, MG, EBC, R, LS]** The system emergency entry port shall recognize only those commands that perform system restoration (for example, from a disk) and no other operations commands.

(2) **[Required: MFSS, SS, LSC, MG, EBC, R, LS]** The system shall generate a real time alarm/alert when this port is used to gain access to the system and transmit that alarm to the appropriate NOC.

n. **[Required: MFSS, SS, LSC, MG, EBC, R, LS]** The system shall have the capability to deny the establishment of any session via a port that is not designed to accept operations-related command inputs. For example, if the output port receives a login request, the system shall not respond.

o. **[Required: MFSS, SS, LSC, MG, EBC, R, LS]** The system shall be capable of providing a time-out feature for users of the system. This implies that, if during a session, there has not been any exchange of messages for a specified period, the system shall lock out that session for subsequent inputs (or re-authenticate user before accepting subsequent inputs).

(1) **[Required: MFSS, SS, LSC, MG, EBC, R, LS]** The default for session inactivity is 15 minutes and shall be configurable.

(2) **[Conditional: MFSS, SS, LSC, MG, EBC]** If the system uses a keyboard, the system shall be capable of providing a mechanism for user-initiated keyboard locking. When a keyboard is locked, the session time-out feature shall be suspended. The unlocking of a locked keyboard shall require authentication (e.g., entering the password). When the keyboard is unlocked, the session time-out feature shall be resumed.

(3) **[Conditional: MFSS, SS, LSC, MG, EBC]** If the system does not use a keyboard (i.e., SSH or other type of remote NMS session), the system shall terminate the session and automatically log the user out after the session inactivity timer has expired.

p. **[Required: MFSS, SS, LSC, MG, EBC, R, LS]** The system shall be capable of providing a mechanism to end a user session through a secure logoff procedure. This implies that when a user terminates a session by logging off, the system shall be capable of ensuring that the port drops immediately and the processes running at the time of logoff are terminated. When a subsequent user attempts to log on to that port, the user shall be required to go through the entire login procedure including identification and authentication, and shall not be granted automatic access (i.e., bypassing the login procedure) to any process invoked by the previous user.

q. **[Required: MFSS, SS, LSC, MG, EBC, R, LS]** The system shall be capable of dropping a port if a session is interrupted due to reasons such as time-out, power failure, link disconnection, etc., and the same login procedure as described above shall be required of a subsequent session request.

NOTE: Serial Ports must drop the session immediately. A delay in dropping the session may occur with Ethernet connections due to the nature of the TCP keep alive capabilities that may appear to keep the session alive. When the disconnected Ethernet connection is attempted to be used to pass data, the connection should drop. If the session drop is not induced by the application, the session should eventually drop on its own once the keep alive fails.

r. **[Conditional: MFSS, SS, LSC, MG, EBC, R, LS]** Depending on the application, if the system employs external modems to perform dial/dial-back, the corresponding modems shall be capable of having the following characteristics:

(1) The modem, after receiving a call from a session requester, shall disconnect the line before dialing the authorized number to reestablish the contact.

(2) The dial-back shall be performed over a line different from the line over which the session request arrived at the modem.

(3) A loss of power to the modem shall not cause the modem to fall back to a default password.

(4) The password file in the modem shall not be readable by a user.

(5) The modem shall prevent any modification of its stored configuration unless the user attempting this modification is properly authenticated and found to be authorized for this action.

s. **[Required: MFSS, SS, LSC, MG, EBC, R, LS]** The system shall be capable of limiting the access to newly created resources in conformance with the privilege of the creator of the resource. This should be the default configuration.

t. **[Conditional: MFSS, SS, LSC, MG, EBC, R, LS]** If the application requires the system to provide different interfaces/ports for different functions, access to system resources over a given interface/port shall be controlled on the basis of privileges assigned to that interface/port.

u. **[Required: MFSS, SS, LSC, MG, EBC, R, LS]** The system shall be capable of providing a level of granularity such that, for any specified resource controlled by the system (to include precedence calls), it shall be possible to do the following:

(1) Grant access rights to a specified user/customer or group of users/customers.

(2) Deny access rights to a specified user/customer or a group of users/customers.

(3) Grant access rights to a specified interface/port or a group of interfaces/port.

(4) Deny access rights to a specified interface/port or a group of interfaces/ports.

(5) Deny a user access to potentially damaging processes and transactions that the user does not have to access to be functional.

(6) Deny an interface/port access to potentially damaging processes and transactions that the interface/port does not have to access to be functional.

(7) Deny a user (as well as a interface/port) access to data files and/or tables unless the user (as well as the interface/port) is authorized for it.

(8) **[Conditional]** If the system has its operations database structured based on commands, views, records, and fields, the system shall restrict, based on user-ID as well as interface/port, the execution of any specifiable command on any specifiable view, record, or field.

5.4.6.2.2 Integrity

1. **[Required: MFSS, SS, LSC, MG, EBC, R, EI, LS]** The system shall be capable of providing data and system integrity.

   a. **[Required: MFSS, SS, LSC, MG, EBC, EI]** The system shall be capable of ensuring the integrity of signaling messages.

      (1) **[Required: MFSS, SS, LSC, EBC – Conditional: EI]** The system shall be capable of using TLS for providing integrity of AS-SIP messages. NOTE: The condition for the EI is the support of AS-SIP.

         (a) **[Required: MFSS, SS, LSC, EBC – Conditional: EI]** The system shall be capable of using HMAC-SHA1-160 with 160 bit keys.

      (2) **[Conditional: MFSS, SS, LSC, EI]** If the system uses H.323, the system shall be capable of using H.235.1 Baseline Security Profile guidance for mutually authenticated shared keys and HMAC-SHA1-96 with 160 bit keys.

   b. **[Required: MFSS, SS, LSC, MG, EBC]** The systems shall be capable of protecting data integrity by performing integrity checks and/or data updates. Examples include:

(1) Proper rule checking on data update

(2) Adequate alert messages (e.g., "Do you really mean it?") in response to potentially damaging commands before executing them, so that involuntary human errors may be reduced.

(3) Proper handling of duplicate/multiple inputs

(4) Checking return status

(5) Checking intermediate results

(6) Checking inputs for reasonable values

(7) Proper serialization of update transactions.

c. **[Required: MFSS, SS, LSC, MG, EBC]** The system shall be capable of providing mechanisms or procedures that can be used to periodically validate its correct operation (such as proper functioning of the security log, proper functioning of various trigger mechanisms, etc.).

d. **[Required: MFSS, SS, LSC, MG, EBC, R, LS]** The system shall be capable of providing mechanisms to monitor system resources and their availabilities (e.g., overflow indication, lost messages, and buffer queues).

e, **[Required: MFSS, SS, LSC, MG, EBC, R, LS]** The system shall be capable of providing mechanisms to detect communication errors (relevant to the system) above a specifiable threshold.

f. **[Required: MFSS, SS, LSC, EBC]** The system shall be capable of providing a mechanism to monitor the integrity of the system and generate a status report detailing the values of all parameters and flags that affect the secure operation of the system.

NOTE: The vendor shall document parameters and flags that affect the secure operation of the system and the IA test team will provide technical advisement to the DSAWG regarding their adequacy.

g. **[Required: MFSS, SS, LSC, MG, EBC]** The system shall be capable of automatically running file or disk integrity checking utilities by vendor-supplied software.

h. **[Required: EI, MG, MFSS]** The system shall be capable of providing data integrity of the bearer (Transport) packets.

(1) **[Required: EI, MG, MFSS]** The system shall be capable of using HMAC-SHA1-32 for the authentication tag with 160 bit key length as the default integrity mechanism for SRTP packets.

(2) **[Required: EI, MG, MFSS]** The system shall be capable of using HMAC-SHA1-80 for the authentication tag with 160 bit key length as the default integrity mechanism for SRTCP.

NOTE: The use of this protocol is optional, but the capability is required.

i. **[Required: MFSS, SS, LSC, MG, EBC, R, LS]** Systems that support remote network management functions and/or critical network resources and services shall be capable of providing appropriate standard (FIPS 140-2) cryptography based data integrity services to protect and detect against unauthorized modification of messages.

j. **[Required: MFSS, SS, LSC, MG, EBC, R, EI, LS]** An appliance and its applications shall be capable of ensuring that it cannot be made to enter an insecure state as a result of the operation of non-privileged code.

NOTE: It is understood that systems shall satisfy this requirement using industry best practices and will mitigate any findings associated with this requirement discovered during IA testing.

k. **[Required: MFSS, SS, LSC, MG, EBC, R, EI, LS]** The system shall be capable of ensuring that default user-IDs and passwords, previously modified by the administrator, do not revert to the vendor delivered default user-IDs and passwords when the system is restarted unless configured to do so by an appropriate administrator.

l. **[Required: MFSS, SS, LSC, MG, EBC, R, EI, LS]** The system shall be capable of providing mechanisms to ensure the integrity of the data that is stored on the appliance and is used to support authentication processes. This includes protecting the information from malicious deletion, modification, or insertion. NOTE: Examples of the data stored would be private keys or certificates.

m. **[Conditional: MFSS, SS, LSC, MG]** If the system uses IPsec, the system shall be capable of using HMAC-SHA (class value 2) as the default IKE integrity mechanism as defined in RFC 2409.

n. **[Required: MFSS, SS, LSC, MG, EBC, R, LS]** The entire SNMPv3 message shall be checked for integrity and shall use the HMAC-SHA1-96 with 160 bit key length.

o. **[Conditional: MFSS, SS, LSC, MG, EBC, R, LS]** If the system uses SSHv2, the system shall use HMAC-SHA1-96 with 160 bit key length for data integrity.

p. **[Conditional: MFSS, SS, LSC, MG, EBC, EI]** If the system uses TLS, the system shall be capable of using TLS (SSLv3.1 or higher) in combination with HMAC-SHA1-160 with 160 bit keys to provide integrity for the session packets.

5.4.6.2.3 Confidentiality

1. **[Required: MFSS, SS, LSC, MG, EBC, EI, R, LS]** The system shall be capable of providing data and signaling confidentiality for all VVoIP traffic.

   a. **[Required: MFSS, SS, LSC, MG, EBC, EI, R, LS]** The system shall implement FIPS 140-2 Level 1 validated cryptographic hardware modules or software toolkits operated in FIPS Mode for all encryption mechanisms.

      NOTE: FIPS 140-2 addresses many aspects of the cryptographic module to include the encryptor and the random number generator. The application does not have to be FIPS 140-2 compliant, but the cryptographic module within the application must be compliant. It is expected that a vendor either will purchase an approved FIPS 140-2 cryptographic module for their application or will submit their developed cryptographic module to an approved FIPS140-2 certification laboratory prior to submitting their solution to the Government for testing. It is anticipated that the Government will accept a Letter of Compliance (LOC) from a vendor as a means of satisfying this requirement.

   b. **[Required: EI, MG]** The system shall be capable of providing confidentiality for media streams using SRTP with either the AES_CM_128 encryption algorithm as the default or **[Required FY12]** AES 256-bit algorithm.

      (1) **[Required: EI]** The system shall be capable of generating keys using a random source algorithm that meets the requirements of FIP 186 to support SRTP.

(2) **[Required: MFSS, SS, LSC, MG, EI]** The system shall be capable of distributing the Master Key and the Salt Key in the VVoIP signaling messages.

(3) **[Required: MFSS, SS, LSC, MG, EI]** The system shall be capable of distributing the Master Key and the Salt Key in concatenated form.

(4) **[Required: EI, MG]** The system shall use a Master Key of 128 bits in order to support 128-bit AES encryption.

NOTE: This implies that the Master Salt Key may be null.

(5) **[Required FY12: EI, MG]** The Master Key and a random Master Salt Key shall be supported for SRTP sessions.

NOTE: This is in addition to the 256-bit requirement.

c. **[Required: MFSS, SS, LSC, MG, EBC, EI]** The system shall be capable of providing confidentiality for signaling messages using TLS or IPSec (or its equivalent) using either:

AES 128-bit algorithm or **[Required FY12]** AES 256-bit algorithm.

(1) **[Conditional: MFSS, SS, LSC, MG, EI]** If H.323, MGCP, or H.248 (MEGACO) is used, the system shall be capable of using IPSec to provide confidentiality.

(a) **[Conditional: MFSS, SS, LSC, MG]** If the system uses H.248 (MEGACO), the system shall be capable of distributing the SRTP Master Key and Salt Key in the Session Description Protocol (SDP) “k =” crypto field when using H.248.15.

(b) **[Conditional: MFSS, SS, LSC, MG, EI]** If H.323 is used, the system shall be capable of distributing the SRTP Master Key and Salt Key in H.235 using the H235Key as described in H.235.0 and H.235.8.

(c) **[Conditional: MFSS, SS, LSC, MG, EI]** If IPSec is used, the system shall be capable of using Internet Key Exchange (IKE) for IPSec key distribution:

i. **[Required]** IKE version 1.

ii. [Required FY 10] IKE version 2.

NOTE: IKEv2 requirements are found in UCR 2008, Section 5.3.5, IPv6 Requirements.

iii. **[Conditional: MFSS, SS, LSC, MG, EI]** If IPSec is used, the system shall be capable of using the Revised Mode of public key encryption during Phase I of the ISAKMP negotiation for authentication.

iv. **[Conditional: MFSS, SS, LSC, MG, EI]** If IPSec is used, the system shall be capable of using the Quick Mode as the default Phase II authentication mechanism.

v. **[Conditional: MFSS, SS, LSC, MG, EI]** If IPSec is used, the system shall be capable of using interpreting certificate requests for PKCS#7 wrapped certificates as a request for the whole path of certificates.

vi. **[Conditional: MFSS, SS, LSC, MG, EI]** If IPSec is used, the system shall be capable of using Main Mode associated with the Diffie-Hellman approach for key generation for the security association negotiation.

A. **[Conditional: MFSS, SS, LSC, MG, EI]** If IPSec is used, the system shall only support the following erroneous messages associated with a certificate request:

1. Invalid Key
2. Invalid ID
3. Invalid certificate encoding
4. Invalid certificate
5. Certificate type unsupported
6. Invalid CA
7. Invalid hash
8. Authentication failed
9. Invalid signature
10. Certificate unavailable

vii. **[Conditional: MFSS, SS, LSC, MG, EI]** If IPSec is used, the system shall be capable of using Oakley Groups 1 and 2 as a minimum.

(d) **[Conditional: MFSS, SS, LSC, MG, EI]** If IPSec is used, the system shall be capable of using AES_128_CBC as the default encryption algorithm.

(2) **[Required: MFSS, SS, LSC, MG, EBC – Conditional: EI]** The system shall be capable of using TLS to provide confidentiality for the Assured Service Session Initiation Protocol (AS-SIP).

NOTE: The condition for the EI is the support of AS-SIP.

(a) **[Required: MFSS, SS, LSC, MG, EBC – Conditional: EI]** The underlying protocol for AS-SIP shall be the Transmission Control Protocol (TCP).

(b) **[Required: MFSS, SS, LSC, MG, EBC – Conditional: EI]** The system shall be capable of using as its default cipher either:

[Conditional] TLS_RSA_WITH_AES_128_CBC_SHA or

[Conditional, Required FY12]
TLS_RSA_WITH_AES_256_CBC_SHA

(c) **[Required: MFSS, SS, LSC, MG, EBC – Conditional: EI]** The system shall be capable of using a default of no compression for AS-SIP messages.

(d) **[Required: MFSS, SS, LSC, MG, EBC – Conditional: EI]** The system shall be capable of exchanging AS-SIP TLS messages in a single exchange or multiple exchanges.

(e) **[Required: MFSS, SS, LSC, MG, EBC – Conditional: EI]** The system shall be capable of distributing the SRTP Master Key and Salt Key in the AS-SIP message using the SDP crypto= field. NOTE: EI condition is whether it supports AS-SIP.

(f) **[Conditional: MFSS, SS, LSC, MG, EBC, EI]** If TLS session resumption is used, a timer associated with TLS session resumption shall be configurable and the default shall be 1 hour.

NOTE: This requirement is not associated with Network Management related sessions.

i. **[Conditional: MFSS, SS, LSC, MG, EBC, EI]** If TLS session resumption is used, the maximum time allowed for a TLS session to resume (session resumption) without repeating the TLS authentication/ confidentiality/authorization process is 1 hour.

(g) **[Conditional: MFSS, SS, LSC, EI, EBC]** If AS-SIP is used, the system shall only transmit packets that are secured with TLS and use port 5061.

NOTE: The systems may use other signaling protocols for interfacing to MGs, EIs, etc.

(h) **[Required: MFSS, SS, LSC, EI, EBC]** The system shall reject all received AS-SIP packets associated with port 5061 that are not secured with TLS.

NOTE: This ensures that the system does not process UDP, SCTP, and TCP SIP packets that are not secured using a combination of TLS and TCP.

(i) **[Required: MFSS, SS, LSC, EI, EBC]** The system shall only accept and process AS-SIP packets that arrive on port 5061.

NOTE: The system should discard AS-SIP packets that arrive on a different port.

d. **[Conditional: MFSS, SS, LSC, MG, EBC]** If the system uses web browsers or web servers, the system web browsers and web servers shall be capable of supporting TLS (Secure Socket Layer (SSL) v3.1) or higher for confidentiality.

e. **[Required: MFSS, SS, LSC, MG, EBC, R, LS]** The system shall be capable of using SSHv2 or TLS (SSLv3.1) or higher for remote configuration of appliances.

NOTE: EIs remote manual configurations shall not be enabled and all non-automatic processes shall be performed locally.

f. **[Conditional: MFSS, SS, LSC, MG, EBC]** If the system uses TLS, the system shall do so in a secure manner as defined by the following subtended requirements.

(1) **[Conditional: MFSS, SS, LSC, MG, EBC]** If the system uses TLS, the system shall be capable of using TLS_RSA_WITH_AES_128_CBC_SHA or TLS_RSA_WITH_AES_256_CBC_SHA **[REQUIRED FY12]** as its default cipher.

(2) **[Conditional: MFSS, SS, LSC, MG, EBC]** If the system uses TLS, the system shall be capable of using a default of no compression.

(3) **[Conditional: MFSS, SS, LSC, MG, EBC]** If the system uses TLS, the system shall be capable of exchanging TLS messages in a single exchange or multiple exchanges.

(4) **[Conditional: MFSS, SS, LSC, MG, EBC**] If TLS session resumption is used, a timer associated with TLS session resumption shall be configurable and the default shall be 1 hour.

NOTE: This requirement is not associated with Network Management related sessions.

(a) **[Conditional: MFSS, SS, LSC, MG, EBC]** If TLS session resumption is used, the maximum time allowed for a TLS session to resume (session resumption) without repeating the TLS authentication/confidentiality/authorization process is 1 hour.

g. **[Conditional: MFSS, SS, LSC, MG, EBC, R, LS]** If the system uses SSH, the system shall do so in a secure manner as defined by the following subtended requirements.

NOTE: EIs remote manual configurations shall not be enabled and all non-automatic processes shall be performed locally.

(1) **[Conditional: MFSS, SS, LSC, MG, EBC, R, LS]** If the system uses SSH, the system shall be capable of supporting the RSA 2,048-bit key algorithm.

(2) **[Conditional: MFSS, SS, LSC, MG, EBC, R, LS]** If the system uses SSH, the system shall use SSH in a secure manner.

(a) **[Conditional: MFSS, SS, LSC, MG, EBC, R, LS]** If the system uses SSH, a client shall close the session if it receives a request to initiate a SSH session whose version is less than 2.0.

(b) **[Conditional: MFSS, SS, LSC, MG, EBC, R, LS]** If the system uses SSH, SSH sessions shall rekey at a minimum every 2^{31} of transmitted data or every 60 minutes, whichever comes first.

(c) **[Conditional: MFSS, SS, LSC, MG, EBC, R, LS]** If the system uses SSH, SSH sessions shall transmit less than 2^{32} packets after a key exchange has occurred.

(d) **[Conditional: MFSS, SS, LSC, MG, EBC, R, LS]** If the system uses SSH, SSH sessions shall rekey at a minimum after receiving 2^{31} packets or every 60 minutes, whichever comes first.

(e) **[Conditional: MFSS, SS, LSC, MG, EBC, R, LS]** If the system uses SSH, SSH sessions shall accept less than 2^{32} packets after a key exchange has occurred.

NOTE: These requirements are consistent with the SSHv2 recommendation formula for the number of packets to accept ($2^{(L/4)}$ where L is the key length – 128 bits).

(f) **[Conditional: MFSS, SS, LSC, MG, EBC, R, LS]** If the system uses SSH, SSH sessions shall use as the default encryption algorithm either:

AES128-CBC or
[Conditional FY12] AES256-CBC .

(g) **[Conditional: MFSS, SS, LSC, MG, EBC, R, LS]** If the system uses SSH, SSH sessions shall use TCP as the underlying protocol.

(h) **[Conditional: MFSS, SS, LSC, MG, EBC, R, LS]** If the system uses SSH, SSH packets shall have a configurable maximum uncompressed payload and the default shall be of 32,768 bytes. This

does not preclude system from automatically sizing the MTU if it is less than 32,768.

i. **[Conditional: MFSS, SS, LSC, MG, EBC, R, LS]** If the system uses SSH, SSH packets shall have a maximum packet size and the default shall be 35,000 bytes including the packet_length, padding_length, payload, random padding, and mac.

ii. **[Conditional: MFSS, SS, LSC, MG, EBC, R, LS]** If the system uses SSH, the appliance shall discard SSH packets that exceed the maximum packet size to avoid denial of service attacks or buffer overflow attacks.

iii. **[Conditional: MFSS, SS, LSC, MG, EBC, R, LS]** If the system uses SSH, SSH packets shall use random bytes if packet padding is required.

(i) **[Conditional: MFSS, SS, LSC, MG, EBC, R, LS]** If the system uses SSH, the system shall treat all SSH encrypted packets sent in one direction as a single data stream. For example, the initialization vectors shall be passed from the end of one packet to the beginning of the next packet.

(j) **[Conditional: MFSS, SS, LSC, MG, EBC, R, LS]** If the system uses SSH, the system shall use Diffie-Hellman-Group1-SHA1 as the default key exchange mechanism for SSH.

(k) **[Conditional FY12: MFSS, SS, LSC, MG, EBC, R, LS]** If the system uses SSH, the system using SSH shall be PKE and shall use the PKI to authenticate.

i. **[Conditional FY12: MFSS, SS, LSC, MG, EBC, R, LS]** If the system uses SSH, the system server using SSH shall have a host key.

ii. **[Conditional FY12: MFSS, SS, LSC, MG, EBC, R, LS]** If the system uses SSH, the system shall certify and validate a server's host key using the DoD PKI prior to connecting with a SSH session.

iii. **[Conditional FY12: MFSS, SS, LSC, MG, EBC, R, LS]** If the system uses SSH, the system shall certify and validate a server's host key prior to connecting with a SSH session.

(l) **[Conditional: MFSS, SS, LSC, MG, EBC, R, LS]** If the system uses SSH, the system shall disconnect a session if the authentication has not been accepted within 10 minutes.

(m) **[Conditional: MFSS, SS, LSC, MG, EBC, R, LS]** If the system uses SSH, the system shall disconnect if the number of failed authentication attempts for a single session exceeds a configurable parameter and the default shall be three attempts.

h. **[Required: MFSS, SS, LSC, MG, EBC, R, LS]** The system shall be capable of using SNMPv3 for all SNMP sessions. NOTE: If the system is using Version 1 or Version 2 (instead of SNMPv3) with all of the appropriate patches to mitigate the known security vulnerabilities, any findings associated with this requirement may be downgraded. In addition, if the system has also developed a migration plan to implement Version 3, any findings associated with this requirement may be further downgraded.

(1) **[Required: MFSS, SS, LSC, MG, EBC, R, LS]** The security level for SNMPv3 in the DoD VVoIP environment shall be authentication with privacy – snmpSecurityLevel=authPriv.

(2) **[Required: MFSS, SS, LSC, MG, EBC, R, LS]** The SNMPv3 architecture shall be capable of allowing an appropriate administrator to manually configure the snmpEngineID from the operator console. A default unique snmpEngineID may be assigned to avoid unnecessary administrative overhead, but this must be changeable.

(3) **[Required: MFSS, SS, LSC, MG, EBC, R, LS]** The security model for SNMPv3 shall be User-Based Security Model – snmpSecurityModel =3.

(a) **[Conditional: MFSS, SS, LSC, MG, EBC, R, LS]** If the system receives response messages, the the system shall conduct a timeliness check on the SNMPv3 message.

(b) **[Required: MFSS, SS, LSC, MG, EBC, R, LS]** An SNMPv3 engine shall perform time synchronization using authenticated messages.

(4) **[Required: MFSS, SS, LSC, MG, EBC, R, LS]** The message processing model shall be SNMPv3 – snmpMessageProcessingModel=3.

(5) **[Required: MFSS, SS, LSC, MG, EBC, R, LS]** The default encryption cipher for SNMPv3 shall be CBC-DES-128 – usmDESPrivProtocol – CBC-DES_128.

(6) **[Conditional: MFSS, SS, LSC, MG, EBC, R, LS]** If the system receives SNMPv3 response messages, then the SNMPv3 engine shall discard SNMP response messages that do not correspond to any current outstanding Request messages.

(7) **[Conditional: MFSS, SS, LSC, MG, EBC, R, LS]** If the system receives SNMPv3 responses, then the SNMPv3 Command Generator Application shall discard any Response Class PDU for which there is no outstanding Confirmed Class PDU.

(8) **[Required: MFSS, SS, LSC, MG, EBC, R, LS]** When using msgID for correlating Response messages to outstanding Request messages, the SNMPv3 engine shall use different msgIDs in all such Request messages that it sends out during a 150 second Time Window and shall have a default of 150 seconds.

(9) **[Required: MFSS, SS, LSC, MG, EBC, R, LS]** An SNMPv3 command Generator or Notification Originator Application shall use different request-ids in all Request PDUs that it sends out during a Time Window.

(10) **[Required: MFSS, SS, LSC, MG, EBC, R, LS]** When sending state altering messages to a managed authoritative SNMPv3 engine, a Command Generator Application should delay sending successive messages to that managed SNMPv3 engine until a positive acknowledgement is received from the previous message or until the message expires.

(11) **[Required: MFSS, SS, LSC, MG, EBC, R, LS]** The appliance using SNMPv3 shall implement the key-localization mechanism.

i. **[Required: MFSS, SS, LSC, MG, EBC]** The system shall be capable of ensuring confidentiality by protecting one user's resource from being accessed by others who do not have such authorization.

NOTE: An instance of this is if the system is accessed by users (including third party service providers) who need confidentiality of their respective resources (which may

contain proprietary, confidential, or sensitive information) from one another or from unauthorized personnel.

NOTE: If resource control mechanisms such as command control, object control, record control, and field control fail to provide the required confidentiality, it may be necessary to partition the system database to protect one user's data from being accessed by another user.

j. **[Required: MFSS, SS, LSC, MG, EBC, R, LS]** The system shall be capable of using a separate interface for management traffic.

NOTE: The separate interface may be a logically or physically separate interface.

(1) **[Required: MFSS, SS, LSC, MG, EBC, R, LS]** The system shall be capable of protecting the management interface using filters.

NOTE: Within a router, the filters may be achieved using ACLs. Within an appliance, the filters may include internal routing procedures to the different physical interfaces or VLAN tagging.

(2) **[Required: MFSS, SS, LSC, MG, EBC, R, LS]** The system shall be capable of using VLANs to segregate management traffic from other types of traffic where feasible. NOTE: The R and LS will implement the VLAN, but the other appliances will have to tag the packets appropriately with the correct VLAN tag.

k. **[Conditional: MFSS, SS, LSC, MG]** If the system uses IPSec, the system shall be capable of using 3DES-CBC (class value 5) as the default IKE encryption algorithm **[Threshold]** AES-CBC **[Objective]**.

l. **[Conditional: MFSS, SS, LSC, MG]** If the system uses different signaling protocols (i.e., H.323 and AS-SIP), the system shall be capable of translating/ transferring the bearer keys between different signaling protocols.

m. **[Required: MFSS, SS, LSC, MG, EBC, R, LS]** The system shall rekey each encrypted session once the session has transmitted a maximum of $2^{(L/4)}$ blocks of data. L is the block length in bits (e.g., 128 for AES_128) and shall be configurable.

NOTE: This is to prevent birthday property and other modes of attack.

n. **[Conditional: MFSS, SS, LSC, MG, EI]** If the system is the originating party and receives a 181 message indicating that the call is being forwarded, then upon completion of the session establishment between the originating party and the forwarded-to party, the originating party must initiate a rekeying.
NOTE: The rekeying is designed to prevent the *forwarding party* from having the key to the bearer session associated with the originating party and the forwarded-to party. If the forwarding party had the key to the bearer session they would be able to eavesdrop on the forwarded session. LSCs, MFSS, and SS may act as a B2BUA for an EI and would therefore originate the AS-SIP session on behalf of the EI.

o. **[Conditional: EI]** If the EI acts as a bridge or a MCU, it shall establish a unique key for each EI connection.

5.4.6.2.4 Non-Repudiation

1. **[Required: MFSS, SS, LSC, MG, EBC, R, LS]** The system shall be capable of providing non-repudiation and accountability services.

NOTE: This assumes that authentication has already occurred as required previously.

a. **[Required: MFSS, SS, LSC, MG, EBC, R, LS]** For user-accessible resources in the system that are created or modified by a user-ID via standard operations and maintenance procedures, the system shall be capable of providing a mechanism to identify the said user-ID, date, and time associated with the said resource creation or modification.

b. **[Required: MFSS, SS, LSC, MG, EBC, R, LS]** The system shall be capable of auditing at the operating system and database management system (DBMS) levels and shall have a security log that contains information to support after the fact investigation of loss or impropriety and appropriate management response.

(1) **[Required: MFSS, SS, LSC, MG, EBC, R, LS]** The security log entry of any request or activity that is invoked by a user-ID shall be capable of including that user-ID so it becomes possible to establish user accountability.

NOTE: The term user-ID shall be interpreted for this requirement to include users as well as processes.

(2) **[Required: MFSS, SS, LSC, MG, EBC, R, LS]** The security log shall be capable of protecting itself from unauthorized access or destruction.

(a) **[Required: MFSS, SS, LSC, MG, EBC, R, LS]** The security log protection, as a minimum, shall be capable of providing access control based on user privileges and interface (logical or physical) privileges.

(b) **[Required: MFSS, SS, LSC, MG, EBC, R, LS]** The appliance shall have no mechanism for any external user (human or machine), including the administrator, to modify or delete the security log.

(3) **[Required: MFSS, SS, LSC, MG, EBC, R, LS]** The security log shall be capable of using a circular (or equivalent) recording mechanism (i.e., oldest record overwritten by newest).

(a) **[Required: MFSS, SS, LSC, MG, EBC, R, LS]** The system shall be capable of generating a security log alarm based upon specific conditions (e.g., percentage full by new entries since last upload, time interval elapsed since the last upload, disk space used). The alarm may necessitate uploading the security log (typically to some remote facility or other facility for long-term storage) to avoid an overwrite in the buffer. This upload may be automatically performed by the system or by an appropriate administrator.

(4) **[Required: MFSS, SS, LSC, MG, EBC, R, LS]** Only the system security administrator and system administrator roles shall have the ability to retrieve, print, copy, and upload the security log(s).

(a) **[Required: MFSS, SS, LSC, MG, EBC, R, LS]** The system shall be capable of ensuring security log copies maintain time sequentially and include all records stored in the security log up to the initiation of the copy.

(5) **[Required: MFSS, SS, LSC, MG, EBC, R, LS]** The system security log shall survive system restart (e.g. via reloading).

(6) **[Required: MFSS, SS, LSC, MG, EBC, R, LS]** The security log shall be capable of recording any action that changes the security attributes and services, access controls, or other configuration parameters of devices; each login attempt and its result; and each logout or session termination (whether remote or console) to include the following events by default as a minimum:

(a) Invalid user authentication attempt.

(b) Unauthorized attempts to access system resources.

(c) Changes made in a user's security profile and attributes.

(d) Changes made in security profiles and attributes associated with a interface/port.

(e) Changes made in access rights associated with resources (i.e., privileges required of a user and a interface/port to access).

(f) Changes made in system security configuration.

(g) Creation and modification of the system resources performed via standard operations and maintenance procedures.

(h) Disabling a user profile.

(i) Events associated with privileged users.

(j) **[Conditional]** If the system contains resources that are deemed mission critical (for example a risk analysis classifies it as critical), then the system should log any events associated with access to those mission critical resources.

(k) Successful login attempts.

(l) Failed login attempts to include the following:

i. Failed login attempt due to an excessive number of logon attempts.

ii. Failed logon attempt due to blocking or blacklisting of a user ID.

iii. Failed logon attempt due to blocking or blacklisting of a terminal.

iv. Failed logon attempt due to blocking or blacklisting an access port.

(7) **[Required: MFSS, SS, LSC, MG, EBC, R, LS]** The security log event record shall be capable of including at least the following information:

(a) Date and time of the event (both start and stop)

(b) User ID including associated terminal, port, network address, or communication device

(c) Event type

(d) Names of resources accessed

(e) Success or failure of the event.

(8) **[Required: MFSS, SS, LSC, MG, EBC, R, LS]** The system shall have the capability to notify (e.g., via critical alarm, alert, or online report), within 30 seconds, an appropriate Network Operations Center (NOC) if the security log fails to record the events that are required to be recorded.

(9) **[Required: MFSS, SS, LSC, MG, EBC, R, LS]** The system shall not record actual or attempted passwords in the security log.

(10) **[Required: MFSS, SS, LSC, MG, EBC, R, LS]** The system shall ensure that security and audit logs are maintained separate from other audit logs (history or CDR audit logs).

(11) **[Required: MFSS, SS, LSC, MG, EBC, R, LS]** The system shall be capable of transmitting all logs to a remote log server in a secure manner.

NOTE: Secure manner may be accomplished by using industry best practices to ensure the confidentiality and integrity of the logs during transfer.

c. **[Conditional: MFSS, SS, LSC, MG, EBC, R, LS]** If the system accesses other systems to pass on a request or activity that has a user-ID associated with it, the system shall have the capability to make that user-ID available to other systems. Thus, if the other systems have the capability to accept the user-ID information, the said user can be traceable for the lifetime of the request or activity.

d. **[Required: MFSS, SS, LSC, MG, EBC, R, LS]** The system shall be capable of providing post-collection audit analysis tools that can produce typical reports (e.g.,

exception reports, summary reports, and detailed reports) on specific data items, users, or communication facilities.

5.4.6.2.5 Availability

1. **[Required: MFSS, SS, LSC, MG, EBC, R, LS]** The VVoIP system (MFSS, LSC1, etc.) shall meet the availability requirements as stated in the UCR 2008, Section 5.3.2.2.3.8, System Quality Factors. There are additional IA specific IA availability requirements specified below that are not covered in the System Quality Factors section of this UCR.

   a. **[Required: MFSS, SS, LSC, MG, EBC, R, LS]** The system shall have robustness through the maximum use of alternative routing, backup.

      NOTE: From a vendor's perspective this requirement is associated with meeting the reliability numbers for the system.

   b. **[Required: MFSS, SS, LSC, MG, EBC, R, LS]** The system shall have mechanisms to allow "secure recovery" to reduce vulnerability due to failure or discontinuity making it vulnerable to security compromise.

      NOTE: This requirement will ensure that as a system is reestablished it does not reboot in an unsecured mode such as with factory set configurations.

   c. **[Required: MFSS, SS, LSC, MG, EBC, R, LS]** The system shall have the capability to rebuild the system to a base version and subsequent vendor modifications of that version, if that version and modification are currently in use.

   d. **[Required: MFSS, SS, LSC, MG, EBC, R, LS]** The system shall have the capability to provide adequate check points in a process flow of the software system so that, upon detection of service deterioration, a recovery to an acceptable level is facilitated.

   e. **[Required: MFSS, SS, LSC, MG, EBC, R, LS]** The system shall have a capability to define a threshold (e.g., percentage full by new entries since last upload, time interval elapsed since last upload) to initiate a warning prior to a security log buffer overflow.

5.4.6.3 Time Division Multiplexing (TDM) Unique

[Required: TS, EOS, MFS, SMEO, PBX1] The system shall meet security requirements in GR-815-CORE, Issue 2, March 2002.

5.4.7 Quality Assurance Provisions

5.4.7.1 Responsibility for Inspection

The responsibility for inspection of the requirements is assigned to one of two organizations depending on whether the satisfaction of the requirement is related to interoperability. If the requirement is an interoperability issue then the JITC will test the system to ensure that the requirement has been met and is interoperable through the Telecom Switched Services Interoperability (TSSI) Program. The TSSI program includes interoperability certification of the DoD's voice, video, and data services. Regardless of whether the requirement has an interoperable aspect, the IA Test Team (IATT) will conduct an IA assessment of the system to ensure that all IA requirements are satisfied in accordance with the VVoIP IA Test Plan (IATP) and the appropriate STIGs. Due to constantly evolving security threats, the IATP is also used to test IA related aspects of a solution that are not mandated by requirements.

The Voice Connection Approval Office (VCAO) has the responsibility for the coordination of all testing, both IA and interoperability. The IATT is part of the JITC and is sponsored by the DISA Office for IA engineering and the DSN PM. The IATT reports the test results of the IA assessment to the DISA Field Security Office (FSO). The FSO is responsible for writing a recommendation to the DISN Security Accreditation Working Group (DSAWG), in coordination with the Certifying Authority (CA) who signs the DSAWG recommendation letter. The DSAWG is the organization which makes the final decision to accept any residual risks associated with the system prior to its IA certification and accreditation. Once the system receives DSAWG accreditation and JITC interoperability certification, it is placed on the APL. The details of the IATP can be found on the JITC TSSI Web site (http://jitc.fhu.disa.mil/tssi/index.html) and the details of the STIGs can be found on the DISA FSO website (http://iase.disa.mil/stigs/stig/index.html).

Once an APL system is procured and installed at a location, it shall comply with the appropriate STIGs and shall report its status to the appropriate Single System Manager (SSM) annually. It is imperative that the system configuration is consistent with the configuration used during the APL process. Upon installation, the IA configuration settings must be validated as part of the DoD Information Assurance Certification & Accreditation Process (DIACAP) as described in the Interim Department of Defense (DoD) Certification and Accreditation (C&A) Process Guidance in order to attain its Certification and Accreditation (C&A), Authorization to Operate (ATO), and/or its Authorization to Connect (ATC). Subsequently, these system settings and IA posture must be reviewed and revalidated annually as part of the annually status update to the appropriate SSM. In addition, the system must be kept up to date with any relevant Information Assurance Vulnerability Management (IAVAM) notices. This is usually accomplished by installing security patches that are tested, verified, and distributed by the vendor and/or by

upgrading to the latest software or operating system release that is certified and approved for installation.

The DIACAP process includes the generation of a System Security Authorization Agreement (SSAA). SSAAs are written to cover a single system or an entire enclave that encompasses multiple systems. The SSAA documents details of the system/enclave architecture, configuration, physical security and operating environment, security settings, users, owners, IA personnel, threats, vulnerabilities, mitigations, and IA requirements for the system. The SSAA is a living document for the lifecycle of the system and is updated as modifications are made to the system/enclave or as its IA posture changes. The DIACAP process is the responsibility of the IA personnel (DAA, IAM, IAO, and system administrators) at the site where the system is installed. A download link to a "DSN Site SSAA Template" can be found at the bottom of the following web page: http://www.disa.mil/gs/dsn/ia_canda.html. The type of template(s) is determined by the types of services provided at the site.

APL C&A and APL listing is not a replacement for DIACAP and local instantiation C&A. Listing on the APL states that the system, in the configuration that was presented for testing, is capable of meeting DoD requirements for IA and interoperability, and is therefore able to be purchased by DoD components. The DIACAP on the other hand is necessary to validate and document that the system is properly installed and meets all relevant IA requirements before it is allowed to operate with or connect to the DISN. Annual reviews and revalidation is necessary to validate and document that the system is being operated in compliance with the IA requirements and remains secure.

5.4.8 Mitigated Risks

The VVoIP IA Architecture is designed to mitigate the IA risks associated with the VVoIP architecture. This goal was accomplished using a combination of commercial "best practices" and DoD unique approaches that are consistent with DoD policies and instructions. The result of this effort was the documentation of a set of requirements for the different appliances used within the DoD VVoIP environment. Based on the requirements, in combination with the VVoIP IA Architecture, and in the knowledge that this UCR 2008 complements the STIGs, the IA threats associated with the VVoIP environment have been adjusted to reflect the mitigated risk and the results are shown in Tables 5.4.8-1 through 5.4.8-8. It is understood that in most cases, the impact of the attack remains constant and the mitigation efforts are mainly focused on reducing the likelihood of the attack.

Table 5.4.8-1. Adjusted General Threat Risk Assessment

	THREAT	LIKELIHOOD	IMPACT	RISK	COMMENT
G1	Eavesdropping on VVoIP subscriber transport data	1	2	2	The use of SRTP with AES 128 mitigates likelihood to a 1. In addition, the rekeying of a call transferred session mitigates this threat.
G2	Corruption of transport data	1	3	3	The use of an SHA-1 hash mitigates the likelihood of this attack to a 1.
G3	Eavesdropping on a valid telephone number to determine its location or to masquerade	1	3	3	The use of AS-SIP with TLS (or its equivalent) for all signaling sessions mitigates this threat to a 1
G4	Eavesdropping on the signaling data	1	3	3	The use of AS-SIP with TLS (or its equivalent) for all signaling sessions mitigates the likelihood to a 1
G5	Corruption of signaling data	1	3	3	The use of TLS with SHA-1 mitigates the likelihood to a 1
G6	Eavesdropping on network management traffic	2	1	2	The use of SNMPv3, SSHv2, SSLv3.1, or TLSv1.0 with 128 bit encryption mitigates this risk. The reason why the likelihood was not reduced to a 1 is that many vendors cannot implement SNMPv3 and in addition it is possible other NM protocols, like TFTP, will still be used in the architecture.
G7	Corruption of network management data	1	3	3	The use of SHA-1 for SNMPv3, SSHv2, SSLv3.1, or TLSv1.0 reduces the likelihood of this type of attack. At this time, these are the only network management protocols defined for the VVoIP architecture
G8	Obtaining telephone number from VVoIP end instrument	1	2	2	The elimination of remote configuration and the use of a PIN (User-ID) and password (2nd PIN) for configuration reduce the likelihood of this attack to a 1.

	THREAT	LIKELIHOOD	IMPACT	RISK	COMMENT
G9	Denial of service	2	2	4	This type of attack is one of the most difficult to mitigate. However, the use of VLANs in combination with filtering and traffic conditioning limit the impact this attack. In addition, appropriate network management and authentication limits the likelihood of this type of attack.
G10	Unauthorized access to data	1	3	3	The requirements associated with this type of attack such as access controls based on user profiles and the requirements associated with authentication limit this attack.
G11	Flooding the network	2	2	4	Similar reasons to DoS attacks.
G12	Stolen terminals	1	3	3	The use of CRL or OSCR in combination with user authentication for above ROUTINE precedence sessions mitigates the likelihood of this attack. Another consideration is that if the terminal is in a high risk environment (forward deployment), it is possible to require user authentication for any session, to include ROUTINE. Finally, the use of network management capabilities (Code Block) in combination with the ability to disable individual terminals also mitigates the likelihood to a 1
G13	Subscription fraud	2	1	2	The implementation of authentication in combination with non-repudiation limits the likelihood of this attack
G14	Unauthorized access to network management or subscriber database	1	3	3	The limiting of access to the database to authenticated and authorized personnel in addition to the database IA requirements mitigates the likelihood of this type of attack.

	THREAT	LIKELIHOOD	IMPACT	RISK	COMMENT
G15	Unauthorized access to data in end instruments	1	1	1	The elimination of remote configuration and the use of a User-ID (PIN) and password (2nd PIN) for configuration reduce the likelihood of this attack to a 1. In addition, the compliance of the EI with FIPS 140-2 also reduces the likelihood of this attack
G16	Masquerading as one legitimate subscriber or signaling device to another	1	3	3	The use of mutual authentication for signaling appliances reduces the likelihood of this attack. In addition, the authentication of the EI to the LSC also reduces the likelihood of this type of attack
G17	Man-in-the-middle attack	1	3	3	The use of 128-bit encryption for all session streams in combination with authentication and traffic segmentation (VLANs, filtering, etc.) reduces the likelihood of this type of attack to a 1
G18	Repudiation of actions	1	2	2	The logging of information and the requirements associated with the storage of logged information reduces the likelihood of this type of attack. In addition, the authentication of appliances and users facilitates the rapid detection of a malicious user
G19	Replay Attack	1	2	2	The integrity mechanisms required by the system mitigate the likelihood of this attack
G20	SIP Parser Attack	1	2	2	The requirement to authenticate and the hardening of the EIs and SIP signaling should mitigate the likelihood of this attack.
G21	SIP Registration or INVITE Flooding or DoS Attack	1	2	2	The requirement to authenticate and the hardening of the EIs and SIP signaling appliances should mitigate the likelihood of this attack. This is primarily an insider attack threat and the defense in depth strategy should make this an easily detected and isolated attack.

	THREAT	LIKELIHOOD	IMPACT	RISK	COMMENT
G22	Buffer Overflow Attack	1	3	3	The likelihood of this attack is small due to the requirement to mutually authenticate all signaling appliances. This attack is associated with malformed SIP messages causing the buffer to overflow.
G23	SIP INVITE	2	1	2	The SIP timers should clear this issue within approximately 32 seconds. In addition, this attack would only affect one phone at a time.
G24	SPAM over Internet Telephony (SPIT)	1	2	2	This attack would have to originate within the SBU voice due to the TDM constraint to the PSTN.
G25	Worms, Viruses, and Trojans	1	3	3	Remove applications that are not VVoIP related from VVoIP appliances. Install anti-virus software on appliances that have applications.

Table 5.4.8-2. Data Deletion Threat Risk Assessment

	THREAT	LIKELIHOOD	IMPACT	RISK	COMMENT
D1	Eavesdropping of old address	2	1	2	The use of NAT may mitigate the likelihood of this attack
D2	Masquerading as a subscriber to delete data	1	3	3	The limiting of access to the database to authenticated and authorized personnel in addition to the database IA requirements mitigates the likelihood of this type of attack.

Table 5.4.8-3. Subscriber Registration Threat Risk Assessment

	THREAT	LIKELIHOOD	IMPACT	RISK	COMMENT
SR1	Illegal registration by an attacker masquerading as a voice or video switch/appliance	1	1	1	The use of mutual authentication for signaling appliances reduces the likelihood of this attack. In addition, the authentication of the EI to the LSC also reduces the likelihood of this type of attack

Table 5.4.8-4. Subscriber De-Registration Threat Risk Assessment

	THREAT	LIKELIHOOD	IMPACT	RISK	COMMENT
SD1	Illegal de-registration by an attacker masquerading as a voice or video switch/appliance	1	1	1	The requirements associated with authentication of a system before processing commands may mitigate the likelihood of this type of attack
SD2	Subscriber does not allow de-registration by manipulating the end instrument	2	1	2	The impact is minimal since the subscriber should be easily isolated using firewalls and other security mechanisms such as authentication of the EI to the LSC, the use of User-ID (PIN) and password (2nd PIN) for the configuration of the EI, and the encryption of network management.
SD3	Subscriber does not allow de-registration by manipulating VVoIP server	1	3	3	The requirements for authentication and authorization of a user on the system mitigate the likelihood of this type of attack. In addition, the requirements associated with hardening the system and ensuring the integrity of the system also mitigates the likelihood of this type of attack

Table 5.4.8-5. Incoming Call Threat Risk Assessment

	THREAT	LIKELIHOOD	IMPACT	RISK	COMMENT
I1	Masquerading by using someone's ID	1	2	2	Since authentication is mandatory the likelihood is low.
I2	Masquerading by using someone's ID and authentication	1	3	3	The design of the authentication mechanism should be sufficient to minimize the likelihood of an attack. However, if the mechanism is broken it makes a large segment of the network vulnerable.
I3	Eavesdropping of the communication on the access interface by use of a session key	1	2	2	There are many requirements in the system associated with the protection of the session key to include the FIPS-140-2 compliance requirements that mitigate the likelihood of this threat In addition, session keys have a shorter lifespan than the time it should take to break the key. The key is not sent in the clear making it difficult to obtain.

	THREAT	LIKELIHOOD	IMPACT	RISK	COMMENT
I4	Eavesdropping of the start of a communication on the end instrument	1	1	1	This threat is mitigated by completing authentication of the session before the session is established in combination with completing the distribution of the session key before the session is established
I5	Modification of routing data	1	3	3	This is mitigated by requiring mutual authentication between routing appliances in combination with the encryption and applying integrity checks to the routing packets.

Table 5.4.8-6. Outgoing Call Threat Risk Assessment

	THREAT	LIKELIHOOD	IMPACT	RISK	COMMENT
01	Masquerading using a subscriber's ID	1	2	2	This attack is associated with outgoing calls and the likelihood is minimized if authentication is required.
02	Masquerading using a subscriber's ID and authentication	1	3	3	There are many policies and procedures established in the DoD that address how one must protect their passwords. This UCR 2008 does not address those policies and procedures.
03	Eavesdropping on the access interface by using a session key	1	2	2	There are many requirements in the system associated with the protection of the session key to include the FIPS-140-2 compliance requirements that mitigate the likelihood of this threat In addition, session keys have a shorter lifespan than the time it should take to break the key. The key is not sent in the clear making it difficult to obtain.
04	Eavesdropping on the network	1	3	3	The use of encryption for all layers should minimize the likelihood of this event occurring.
05	Eavesdropping on the start of a communication on the end instrument	1	1	1	This threat is mitigated by completing authentication of the session before the session is established in combination with completing the distribution of the session key before the session is established

	THREAT	LIKELIHOOD	IMPACT	RISK	COMMENT
06	Eavesdropping on the phone number of a called party	1	1	1	This threat is mitigated by completing authentication of the session before the session is established in combination with completing the distribution of the session key before the session is established.
07	Modification of the dialed number	1	3	3	This threat is mitigates by the use of authentication by appliances and users (for above ROUTINE precedence sessions) in combination with encryption and integrity checks for all sessions
08	Masquerading using someone's ID	1	1	1	This is not allowed since authentication is required prior to allowing a session to be established

Table 5.4.8-7. Emergency and Precedence Call Threat Risk Assessment

	THREAT	LIKELIHOOD	IMPACT	RISK	COMMENT
E1	Misuse of emergency call	2	1	2	The use of non-repudiation does not prevent this type of attack, but does allow for the rapid discovery of the malicious user or EI
E2	Misuse of precedence calls	1	3	3	This threat is mitigated by the requirements associated with user authentication and EI authentication for above ROUTINE level sessions
E3	Manipulation of emergency database information	1	3	3	The requirements associated with user authentication and authorization for database access decrease the likelihood of this type of attack.
E4	Manipulation of precedence database information	1	3	3	The requirements associated with user authentication and authorization for database access decrease the likelihood of this type of attack.

Table 5.4.8-8. Survivability Threat Risk Assessment

	THREAT	LIKELIHOOD	IMPACT	RISK	COMMENT
S1	A node in the network is destroyed or disabled	3	1	3	The requirements associated with survivability such as dual homing, FFR, backup power, COOP requirements, standalone capabilities reduce the impact of this attack
S2	A device in the network is disabled or destroyed	3	1	3	The requirements associated with survivability such as dual homing, FFR, backup power, COOP requirements, standalone capabilities reduce the impact of this attack

As discussed in the earlier threat section, the threats are defined as critical, major, and minor according to the product of their likelihood of an attack being successful score and the impact of a successful attack score as shown in Figure 5.4.8-1.

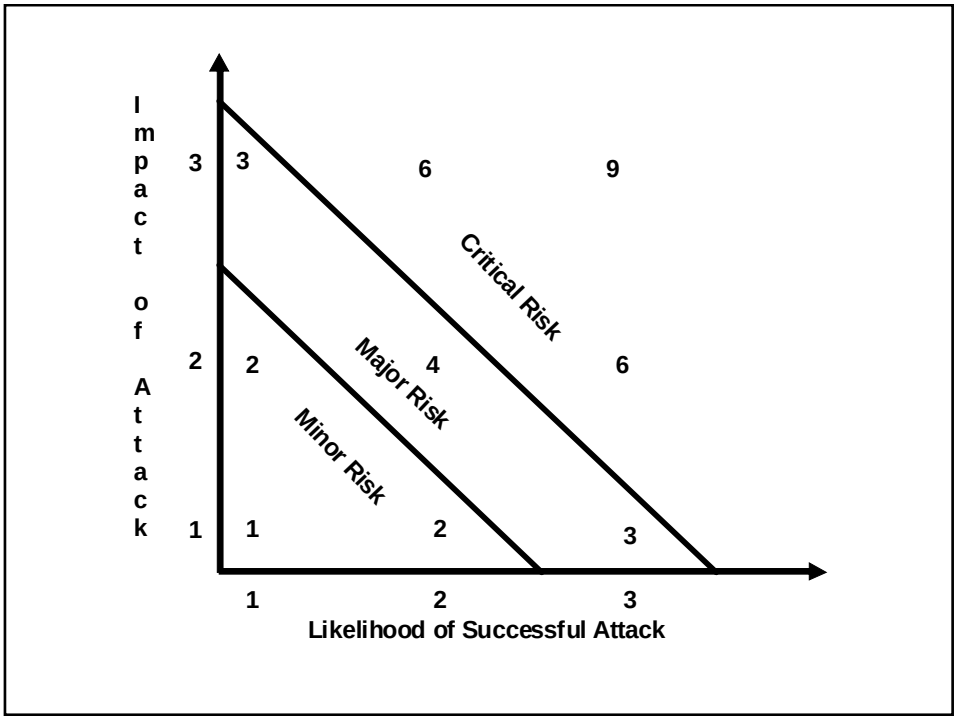


Figure 5.4.8-1. ETSI TIPHON Threat Risk Score

Based on the mitigations discussed in UCR 2008, all of the critical risk threats have been mitigated to a major risk or below category. In addition, many of the major risk threats have been mitigated to a lower score or have been reduced to a minor risk. Table 5.4.8-9, Adjusted Risk Summary, tabulates the results of the risk mitigation effort.

Table 5.4.8-9. Adjusted Risk Summary

RISK LEVEL	NUMBER OF RISKS (BEFORE MITIGATION)	NUMBER OF RISKS (AFTER MITIGATION)
Critical Risks	22	0
Major Risks	13	25
Minor Risks	16	26
Total	**51**	**51**

THIS PAGE INTENTIONALLY LEFT BLANK

TABLE OF CONTENTS

SECTION **PAGE**

5.5 Network Infrastructure Product Requirements 1317
5.5.1 DISN Terrestrial Network Overview 1317
5.5.1.1 DISN Terrestrial Network Functions 1318
5.5.1.2 TNE – Optical Transport System 1319
5.5.1.2.1 Wavelength Services 1319
5.5.1.2.2 Fiber Span 1320
5.5.1.3 Switching (ODXC) 1321
5.5.1.4 Access (MSPP) 1322
5.5.1.4.1 Edge Services 1323
5.5.1.5 Routing 1325
5.5.1.6 DISN IP Hierarchy 1327
5.5.2 DISN Transport Network Element(s) Requirements 1327
5.5.2.1 Optical Transport System Requirements 1327
5.5.2.1.1 Overall Requirements 1327
5.5.2.1.2 Formats Supported 1328
5.5.2.1.3 Fiber 1329
5.5.2.2 Protection and Restoration 1330
5.5.2.3 Performance Requirements 1330
5.5.2.4 Reliability and Quality Assurance 1333
5.5.2.6 Interface Requirements 1335
5.5.2.7 Muxponder Requirements 1336
5.5.2.8 Common Physical Design Requirements 1338
5.5.2.9 Optical Line Amplifier (OLA) 1343
5.5.2.10 Optical Supervisory Channel (OSC) 1346
5.5.2.11 OADM 1348
5.5.2.12 Planning Tools 1351
5.5.2.12.1 Optical Layer (Physical) Planning Tool 1351
5.5.2.12.2 Network Layer Planning Tool 1353
5.5.2.13 Standards Compliance 1354
5.5.3 DISN ODXC Requirements 1357
5.5.3.1 ODXC SONET/SDH Interface Requirements 1357
5.5.3.2 ODXC Ethernet Interface Requirements 1358
5.5.3.3 ODXC Framing Requirements 1359
5.5.3.4 ODXC Switch Fabric Requirements 1360
5.5.3.5 ODXC Performance Requirements 1361
5.5.3.6 General Link Protection Requirements 1361

5.5.3.7 Linear Protection Requirements 1362
5.5.3.8 Ring Protection Requirements 1364
5.5.3.9 Fault Management Requirements 1365
5.5.3.10 Performance Management Requirements 1365
5.5.3.11 EMS Requirements 1366
5.5.3.12 Standards Compliance Requirements 1367
5.5.4 DISN Access Requirements.....1368
5.5.4.1 MSPP, M13, Sub-T-1 Mux Requirements.....1368
5.5.4.2 SONET Interface Requirements 1368
5.5.4.3 SDH Interface Requirements 1371
5.5.4.4. Lambda Interface Requirements 1372
5.5.4.5 Electrical Interface Requirements.....1372
5.5.4.6 Ethernet Interface Requirements 1373
5.5.4.7 SAN Interface Requirements 1374
5.5.4.8 Cross Connect Requirements.....1374
5.5.4.9 Performance Requirements.....1375
5.5.4.10 Equipment Redundancy Requirements.....1377
5.5.4.11 General Protection Requirements 1378
5.5.4.12 Interoperability Requirements 1379
5.5.4.13 Fault Management Requirements 1379
5.5.4.14 Performance Management Requirements 1380
5.5.4.15 EMS Requirements 1381
5.5.4.16 Standards Compliance Requirements 1382
5.5.5 DISN Router Requirements 1382
5.5.5.1 Interface Requirements 1383
5.5.5.1.1 POS Interface Requirements.....1383
5.5.5.1.2 ATM Interface Requirements 1389
5.5.5.1.3 Ethernet Interface Requirements.....1393
5.5.5.1.4 Packet Ring Requirements 1394
5.5.5.2 IPv6 Requirements.....1394
5.5.5.3 Performance Requirements.....1394
5.5.5.4 ISIS Requirements 1395
5.5.5.5 OSPF Requirements.....1398
5.5.5.6 BGP Requirements 1398
5.5.5.7 MPLS Requirements.....1401
5.5.5.8 RSVP Requirements 1402
5.5.5.9 LDP Requirements.....1403
5.5.5.10 DiffServ Requirements 1403
5.5.5.11 Intserv Requirements 1404
5.5.5.12 Congestion Control Requirements.....1404
5.5.5.13 Queuing Requirements 1405

5.5.5.14 Multicast Requirements 1405
5.5.5.15 Equipment Redundancy Requirements....1406
5.5.5.16 Management Requirements 1406
5.5.6 DISN Transport Timing and Synchronization Requirements....1406
5.5.6.1 DISN Switch Timing and Synchronization Requirements 1406
5.5.6.2 DISN Access Element Timing and Synchronization Requirements 1409
5.5.7 DISN Transport Encryption for Overseas Connections (TBD)....1411
5.5.8 DISN Transport OSS (TBD)....1411
5.6 Generic Encryption Device Requirements....1413
5.6.1 Introduction....1413
5.6.2 Encryption Products Overview....1413
5.6.3 Minimum Requirements 1417
5.6.3.1 Flexible and Robust Security....1417
5.6.3.2 Interfaces....1417
5.6.3.3 Operational Management....1417
5.6.3.4 Zeroization....1418
5.6.3.5 Maintainability and Serviceability....1419
5.6.3.6 Data Recovery....1419
5.6.3.7 External Interfaces 1419
5.6.3.8 Programmability 1419
5.6.3.9 Performance....1419
5.6.3.10 Network Operations....1420
5.6.3.11 Key Management....1420
5.6.4 Operational Control over Features and Capabilities Management....1420
5.6.5 General GCIRD Specification Language 1420
5.6.6 Relationships Among Unified Capabilities Requirements Documents 1421
5.6.6.1 Assumptions and Dependencies 1421
5.6.6.2 Applicable Documents....1421
5.7 Instant Messaging, Chat and Presence/Awareness 1427
5.7.1 Introduction....1427
5.7.2 Presence/Awareness, IM and Chat Standards....1427
5.7.3 Routing and Addressing....1427
5.7.4 Ports and Protocols 1428
5.7.5 Standards Requirements 1429
5.7.5.1 Instant Messaging and Chat....1429
5.7.5.2 Presence/Awareness....1431
5.7.6 Security Requirements for Presence/Awareness, IM, and Chat 1431

5.5 NETWORK INFRASTRUCTURE PRODUCT REQUIREMENTS

5.5.1 DISN Terrestrial Network Overview

DISN Terrestrial Network (sometimes referred to as "Core Network" but here it is referred to as "DISN") is the collection of telecommunications equipment and associated NMS systems that aggregates, switches, routes large amounts of customer voice, video, and data information in a reliable manner across large geographical distances between Service Delivery Nodes (SDN) connected via fiber or leased capacity.

In 2008, DISN is fully deployed. Figure 5.5.1, High Level DISN Node Design FY 2008, shows a high-level architecture of a DISN node in 2008. In this architecture, there is a separation between IP and Transport services. Transport provides not only "wavelength" and "dedicated facilities" between IP equipment but also provides facilities to transport legacy and TDM traffic by Multi-service Provisioning Platform (MSPP) and Optical Digital Cross-connect System (ODXC). Some customers that require 10G (OC-192 or 10GbE LAN/WAN PHY) transport is provided via Optical Transport System (OTS) using OC-192 and/or G.709 compliant transceivers.

As new DISN services are deployed on Internet Protocol (IP) MPLS technology the existing circuit based services will transition/migrate to IP/MPLS. Today's TDM interfaces are expected to mostly migrate to Ethernet; Ethernet is expected to be the standard interfaces not only between DISN equipment but also for external customer interfaces. There will still be some customer requirements for TDM-only based transport services. Considering the IP/MPLS as the service convergence layer, Ethernet as the standard interface for customer access and between equipments at the SDNs it is natural to assess packet aware transport technologies as the evolution of the DISN transport. The connectivity between core sites over fiber will be OTN (ITU-T G.709) based, initially 10G/40G capable and then possibly 100G per wavelength, high capacity, multi-degree all optical DWDM system. Today's OC-192 and 10GbE LAN/WAN PHY wavelength services are expected to evolve to higher rates and become protected wavelength services via DWDM layer.

NOTE: This section of UCR 2008 is a working document. It presents the requirements for the equipment in the 2008 architecture. This section will be updated with the description and requirements for the next generation technologies envisioned for DISN network in the near future.

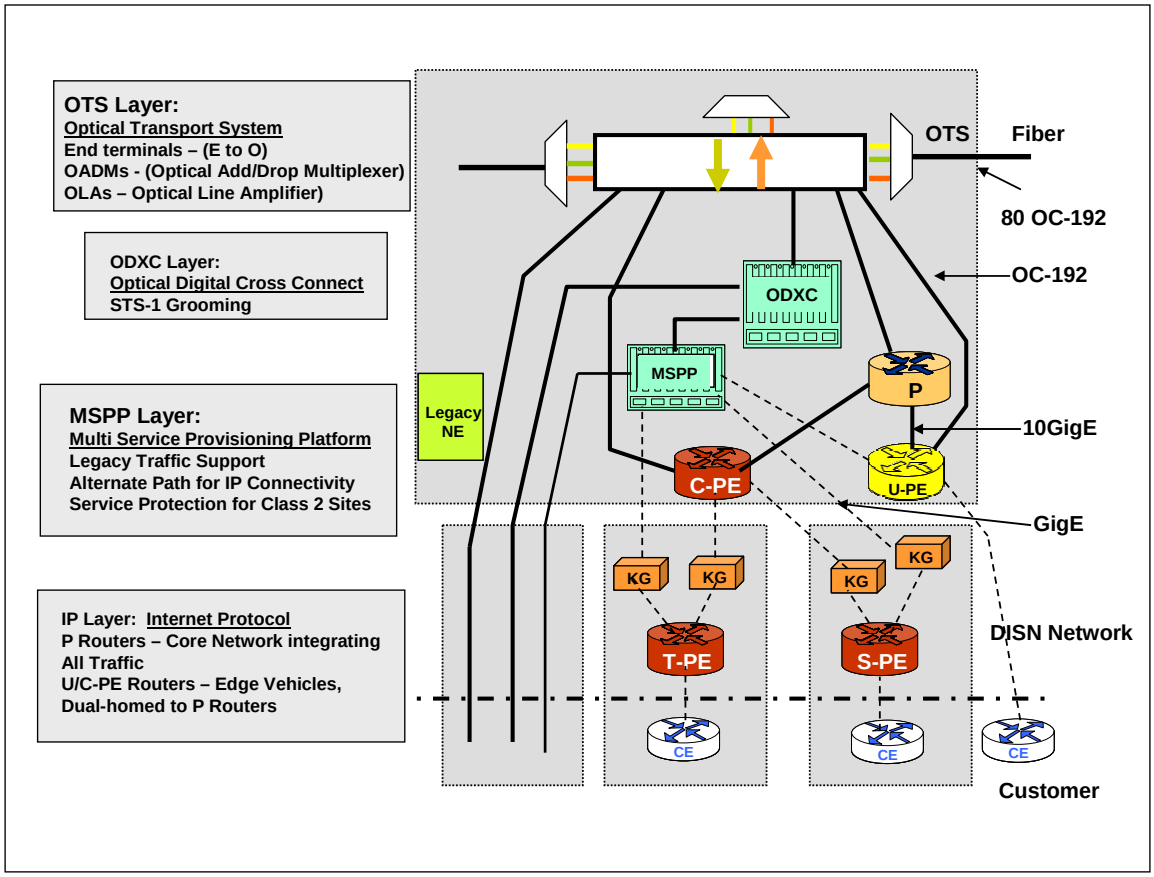


Figure 5.5-1. High Level DISN Node Design FY 2008

5.5.1.1 DISN Terrestrial Network Functions

DISN performs four distinct functions:

- Transport
- Switching
- Access
- Routing

DISN equipment specialized in performing one of these four functions are typically interconnected in specific ways to create an applicable topology for a given operational need. DISN element described in this document is labeled according to its main functional purpose as follows:

- Transport Network Element(s)
  - Transport
  - Switching

  - Access Element
- Router
  - Routing

In the 2008 design, the four functions (Transport, Switching, Access, Routing) are provided by the following equipment suite.

- Transport Network Element(s)
  - Transport is provided by OTS
  - Switching is provided by ODXC
  - Access Element function is provided by MSPP

- Router
  - Routing is provided by P and PE routers

5.5.1.2 TNE – Optical Transport System

Optical Transport System multiplexes the optical signals from Transport Network Element(s) at the SDN or IP Router(s) or customer-dedicated signals onto fiber and transport signals to other SDNs over outside fiber plant. In 2008, OTS system is a point-to point 80, 10 Gbps channel capable DWDM system and consists of the following NEs: End Terminal, 2-degree OADM and OLA.

1. End Terminal. Optical terminal with multi-wavelength line interface in one direction.

2. Optical Add Drop Multiplexer (OADM). Optical terminal equipment with 2-bidirectional multi-wavelength line side interfaces. It performs wavelength add and drop functions, as well as allowing wavelengths to pass through.

3. Optical Line Amplifier. Provides optical signal re-amplification without converting to electrical signal along the spans between optical terminal equipment

5.5.1.2.1 Wavelength Services

For this document, DISN transport services are divided into two categories:

- Transport service (service that is not wavelength service – end point of the service from OTS perspective is a DISN IP or TNE)

- Wavelength service (service that DISN provides on the optical core to end users, without aggregation/grooming in OEO network elements.)

A wavelength service is further classified as either Framed or Unframed service.

1. Framed Services. A Framed wavelength service is a service transported across an optical link that performs Optical-to-Electrical-to-Optical (OEO) Reamplification and Reshaping (2R), or Reamplification, Reshaping, and Retiming (3R) of the optical signal.

2. Unframed Services. An Unframed wavelength service is a service transported across an optical link that performs only Optical-to-Optical (OO) Reamplification (1R) of the optical signal. Unframed wavelength services are transported in an optically transparent manner, since the optical signal carrying the services does not undergo Optical-to-Electrical-to-Optical (OEO) processing. However, since unframed services are not reshaped or retimed, the span (or distance) these services can be transported between OADMs are limited, due to the gradual reduction of the Optical Signal to Noise Ratio (OSNR) of an optical signal as it traverses an optical fiber.

5.5.1.2.2 Fiber Span

The span loss is the attenuation between DWDM equipment at adjacent DWDM locations (OLA, OADM, End Terminal). The span loss consists of the outside plant (OSP) loss, the intra-office loss, and the fiber maintenance margin. The OSP loss is the loss from FSDP (Fiber Service Delivery Point) to FSDP. The intra-office is from FSDP to DWDM equipment as illustrated in Figure 5.5-2, Difference between OSP Loss and the Span Loss. The entrance/exist points of the DWDM equipment are the reference points MPI-S/R according to ITU-T REC. G.692.

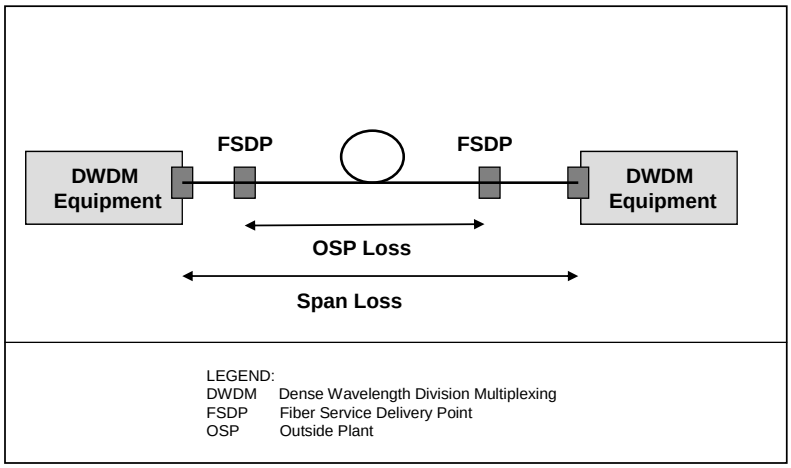


Figure 5.5-2. Difference between OSP Loss and the Span Loss

The Fiber Maintenance Margin is the additional margin allocated to the fiber network to warrantee the continuous operation to the end of life of the DWDM system. This Fiber Maintenance Margin does not include any margins for DWDM vendor's equipment.

The OSP loss is measured from the fiber connector in the FSDP of a DWDM equipment location to the fiber connector (at the other end of the fiber) in the FSDP of the next DWDM equipment location. The OSP loss is the combined loss of the fiber attenuation itself and the attenuation due to splices and connectors across the span.

5.5.1.3 Switching (ODXC)

A DISN switch is any device that receives data traffic on its ports, and directs this traffic between its ports in a user pre-configured manner via internal cross-connects between its ports. Switches are normally located at completely separate sites, where client services originate or terminate.

The main purpose of a switch is to provide high-speed cross-connection (or switching) of traffic across the DISN. All end-to-end circuits originate and terminate at a switch, and typically pass through Transport links.

Typically, the DISN Access element (described in the next subsection) at a local site aggregates low-speed traffic from the local network edge and delivers the aggregated high-speed traffic to the client ports of the switch at the same local site. The local switch switches this traffic via its cross-connects to other switches at remote sites. A switch at a remote site passes its received traffic to a Access element at the same remote site. The remote Access element then delivers the traffic in the form of low-speed tributaries to the remote network edge.

Figure 5.5-3, DISN Switch, depicts a typical switch and Figure 5.5-4, Typical Network-Side Connections from a DISN Switch, illustrates the typical network-side connections from a switch.

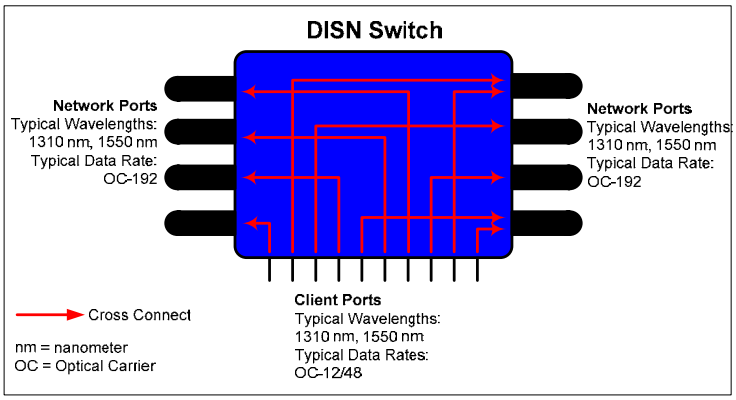


Figure 5.5-3 DISN Switch

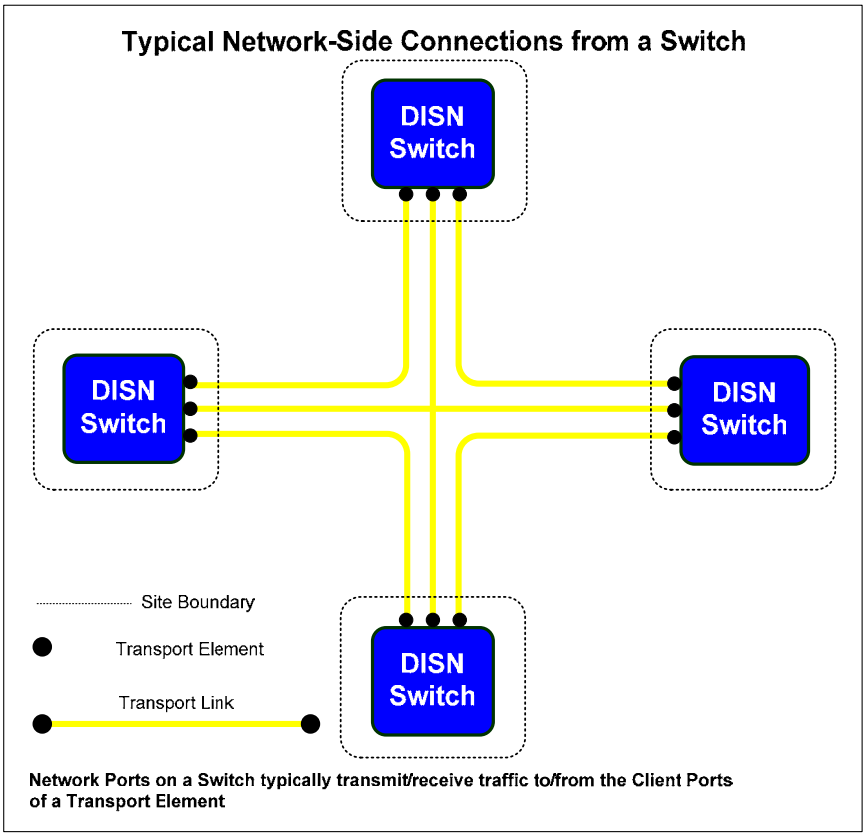


Figure 5.5-4. Typical Network-Side Connections from a DISN Switch

5.5.1.4 Access (MSPP)

A DISN Access element is any device that receives low-speed traffic streams on multiple client ports, aggregates and multiplexes these traffic streams via TDM into a high-speed traffic stream, and transmits this TDM stream to one of its network ports. The multiplexing of traffic is user pre-configured via multiple internal cross-connects between the low-speed client ports and the high-speed network port. Access elements are normally located at completely separate sites, where client services originate or terminate.

The main purpose of an Access element is to provide network edge access for low-speed services onto the network core. A low-speed Access circuit is typically mapped directly onto a high-speed switch circuit and passed through the network core via switches. When a switch is not available or needed, Access traffic may be passed directly to a Transport element. A circuit originating from an Access element typically terminates on another Access element.

In order to provide protection of Access circuits in case a fiber link breaks, at least two network ports are present on the Access element. To protect a circuit originating at a client port, two cross-connects would be configured by the user. For the Working Path of the circuit, the first

cross-connect would be configured between the client port and one of the network ports. For the Protect Path of the circuit, a second cross-connect would be configured between the same client port and the other network port.

Figure 5.5-5, DISN Access Element, depicts a typical Access element and Figure 5.5-6, Typical Network-Side Connections from a DISN Access Element, illustrates the typical network-side connections from an Access element.

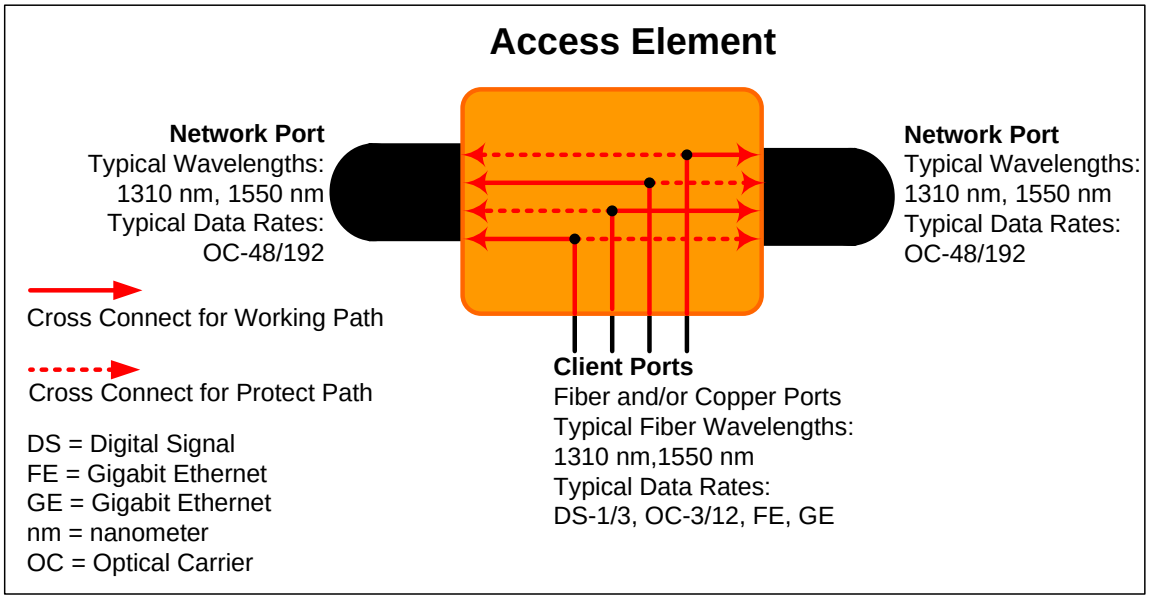


Figure 5.5-5. DISN Access Element

5.5.1.4.1 Edge Services

The Access system supports and aggregates a variety of Network Edge Services via its physical interfaces:

1. Concatenated SONET/SDH. A Concatenated (or Unchannelized) SONET/SDH Frame contains a single Header (containing information about its trailing Payload) preceeding the adjacent Payloads (containing data only) of its TDM-multiplexed lower-speed frames. Concatenation is indicated with a lowercase “c” for the stream, such as OC-12c, which is a stream of four TDM-multiplexed and concatenated OC-3 streams. (TBD is anything less than OC-192 used in the DISN/Core?)

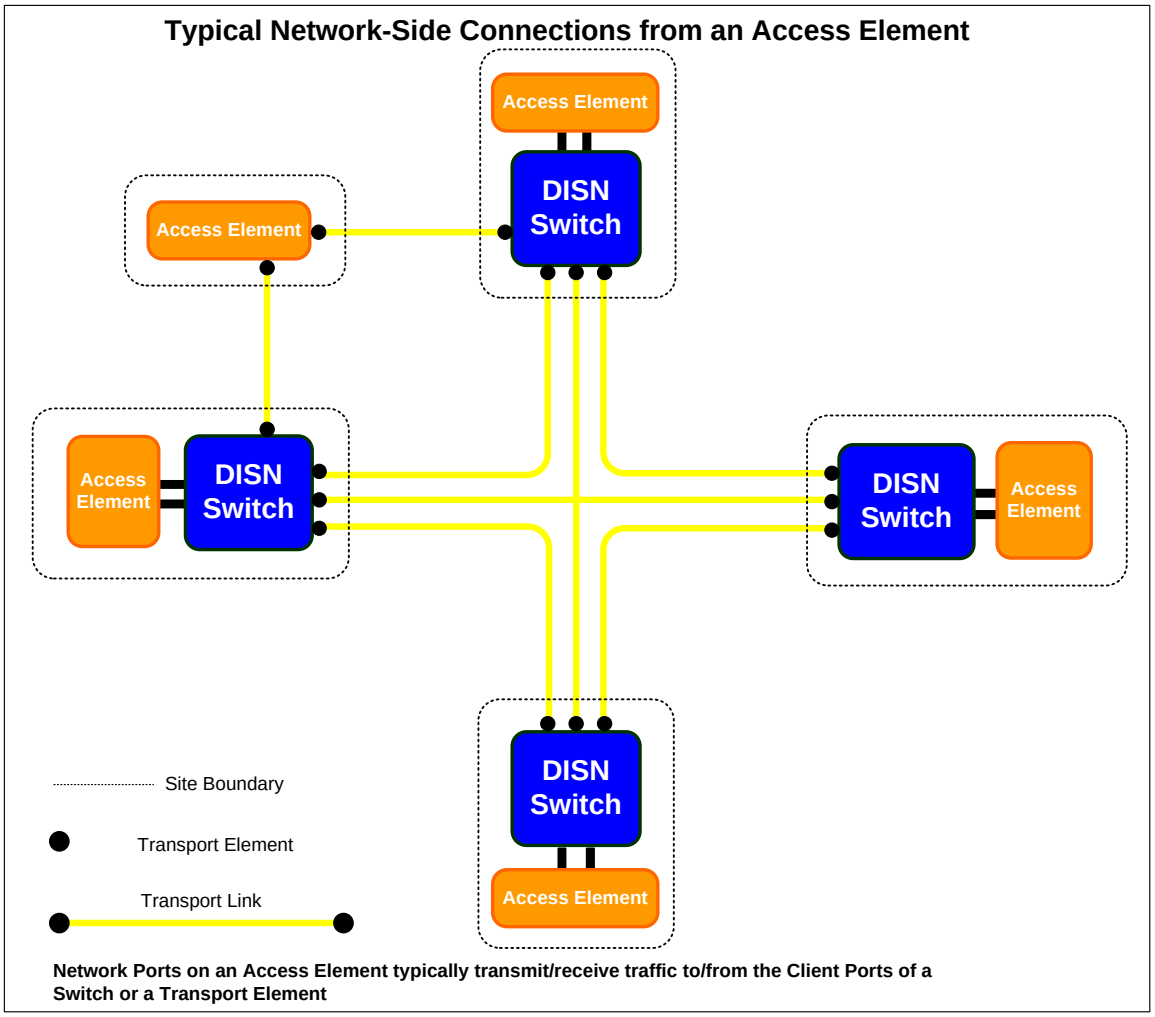


Figure 5.5-6. Typical Network-Side Connections from a DISN Access Element

2. Unconcatenated SONET/SDH. An Unconcatenated (or Channelized) SONET/SDH Frame retains both the Headers and Payloads of its TDM-multiplexed lower-speed frames. Unconcatenation is indicated when a lower-case "c" is not present for the stream, such as OC-12, which is a stream of four TDM-multiplexed and channelized OC-3 streams. (TBD is anything less than OC-192 used in the DISN/Core?)

3. Ethernet. Ethernet is a frame-based data communication technology for Local Area Networks (LAN). The data rate is 10 Megabits per second for Regular Ethernet, 100 Mbps for Fast Ethernet (FE), 1 Gigabit per second (Gbps) for Gigabit Ethernet (GE), and 10 Gbps for 10 Gigabit Ethernet (10 GE)).

4. Digital Signal. Digital Signal is a T-Carrier signalling scheme devised by Bell Laboratories. The DS-1 (also called T-1) circuit was originally devised to carry 24 channels of voice

traffic, and has a data rate of 1.544 Mbps. The DS-3 (also called T-3) circuit has a data rate of 44.736 Mbps. An improvement of the T-Carrier technology was developed in Europe, and is called the E-Carrier. The transmission speed is 2.048 Mbps for an E-1 line and 34.368 Mbps for an E-3 line. T-Carrier technology is used in the United States and Japan, while E-Carrier technology is used in the rest of the world.

The Access system provisions Edge Services through the Switch layer and Transport layer of the network, and provides functions such as Fault Detection, Isolation, Reroute, and Restoration of these services. These functions are provided in an automated fashion using minimal human intervention.

5.5.1.5 Routing

A DISN Router is any device that receives IP-type traffic on its ports and routes this traffic between its ports via internal Forwarding Paths. IP-type traffic consists of data packets specified by the IP family of networking protocols.

The internal forwarding paths of a DISN Router are not user pre-configurable like the internal cross-connects of a DISN Switch or DISN Access element. Internal Router forwarding paths for data traffic are created and updated in real-time by the Router itself, based on its knowledge of the best network path to the traffic's destination at any moment in time.

The Router obtains knowledge of the best network paths for its traffic by communicating with the other DISN Routers on the network via routing protocols such as Open Shortest Path First (OSPF), Intermediate System to Intermediate System (ISIS), and Border Gateway Protocol (BGP). This knowledge is stored in the Routing Table of the DISN Router and kept current at all times.

The main purpose of a DISN Router is to provide reliable IP-type traffic routing to all of the other DISN Routers on the network. All IP-type traffic over the network core originates and terminates at a DISN Router, and usually passes through multiple DISN Transport links. DISN Routers are normally located at completely separate sites, where IP-type traffic originates or terminates.

Figure 5.5-7, DISN Router, depicts a typical DISN Router, and Figure 5.5-8, Typical Network-Side Connections from a DISN Router, illustrates the typical network-side connections from a DISN Router.

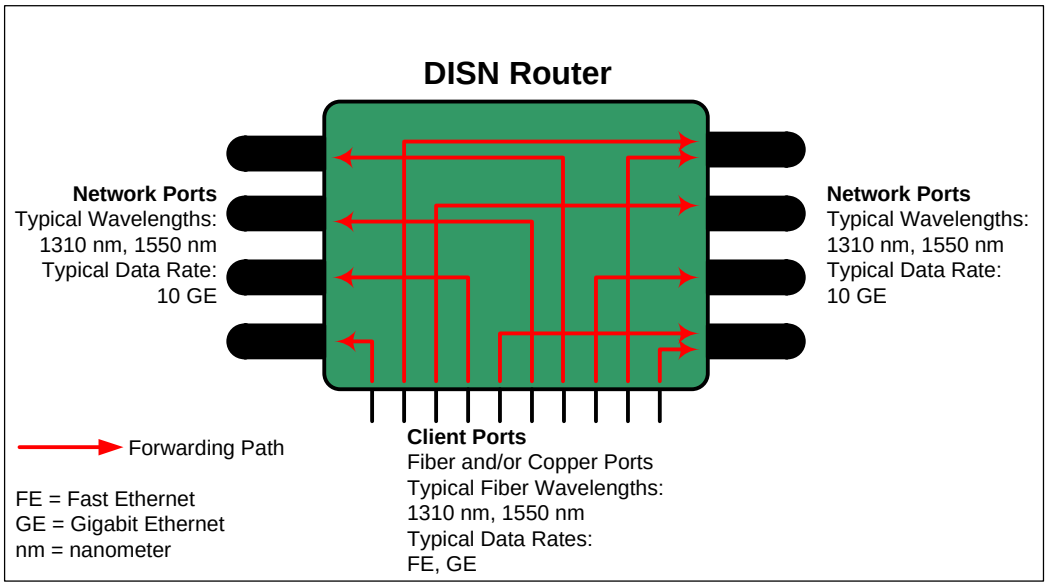


Figure 5.5-7. DISN Router

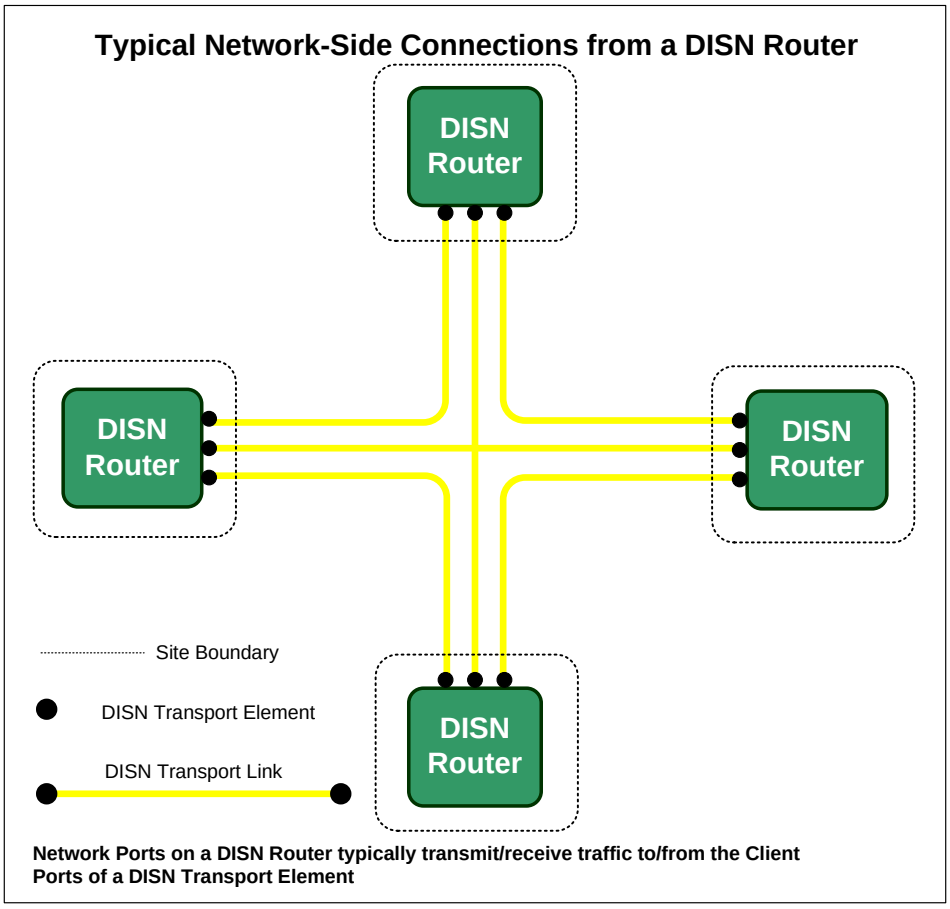


Figure 5.5-8. Typical Network-Side Connections from a DISN Router

5.5.1.6 DISN IP Hierarchy

The typical IP DISN consists of a two-level network hierarchy of PE Routers for routing of traffic within the network edge, and Provider (P) Routers routing of traffic across the DISN.

An Interior Gateway Protocol (IGP), such as the Intermediate System-to-Intermediate System (ISIS), is used by the Provider Edge DISN Routers to exchange Routing Data (to be distinguished from User Data) among themselves.

An Exterior Gateway Protocol (EGP), such as the Border Gateway Protocol (BGP), is used to exchange Routing Data between the Provider Edge DISN Router and the Provider DISN Router.

Multi-Protocol Label Switching (MPLS) is typically used for the forwarding of User Data (to be distinguished from Routing Data) between the Provider Edge Router and the Provider Router. MPLS is used as well for the forwarding of User Data between Provider Routers across the DISN. Provider Edge Routers act as MPLS Label Edge Routers (LER), and Provider Routers act as Label Switched Routers (LSR). Label Switched Paths (LSP) are typically set up using the Resource Reservation Protocol (RSVP).

5.5.2 DISN Transport Network Element(s) Requirements

The requirements in this section are specific to DISN Terrestrial Transport Network Element(s).

5.5.2.1 Optical Transport System Requirements

5.5.2.1.1 Overall Requirements

1. **[Required]** The OTS family of equipment shall be currently available, commercial-off-the-shelf (COTS) equipment.

2. **[Required]** The OTS shall support a minimum of 80 ITU G.694.1 grid wavelengths per line-side optical fiber.

3. **[Conditional]** The OTS shall support a minimum of 160 ITU G.694.1 grid wavelengths per line-side optical fiber.

4. **[Required]** The OTS shall support mixed bit rate signals: 2.5 Gbps, 10 Gbps, and 40 Gbps.

5. **[Conditional]** The OTS shall support mixed bit rate signals: 2.5 Gbps, 10 Gbps, 40 Gbps, and 100 Gbps.

6. **[Required]** The OTS shall utilize the ITU-T specified Optical Supervisory Channel (OSC) for in-band management communication.

7. **[Required]** The OTS shall support all specified wavelengths for all specified bit rate and signal format.

8. **[Required]** The OTS shall support at least SSMF (post-1993), ELEAF, TW-RS, and TW-C.

9. **[Required]** The OTS shall support the ability of 80, 10G wavelengths to transverse a minimum of 5 OADM using fibers specified above for a minimum reach of 2,000 km without regeneration at BER less than 1x 10^{-15}.

10. **[Required]** The OTS shall support the ability of 80, 40G wavelengths to transverse a minimum of 5 OADM using fibers specified above for a minimum reach of 1,500 km without regeneration at BER less than 1x 10^{-15}.

11. **[Required]** The OTS shall support the ability of 80, 100G wavelengths to transverse a minimum of 5 OADM using fibers specified above for a minimum reach of 1,200 km without regeneration at BER less than 1x 10^{-15}.

12. **[Required]** The OTS shall support span length up to 150 km and span loss up to 42 dB. The reach shall not be limited by optical supervisory channel performance.

13. **[Required]** The system shall allow the remote configuration of wavelengths added or dropped from the system.

14. **[Required]** Client interfaces available on the system shall meet the generally accepted standards or specifications for the interface (e.g. OC-192 GR-253 standards, Synchronous Transport Module (STM)-16 and STM-64 International Telecommunications Union (ITU)-T G.707 standards, and Gigabit Ethernet (GE) and 10 GE IEEE 802.3 standards).

5.5.2.1.2 Formats Supported

5.5.2.1.2.1 Framed

1. **[Required]** The OTS shall support the transport of the following SONET/SDH services: OC-192/STM64, OC-48/STM16, OC768/STM256.

2. **[Required]** The OTS shall support the transport of the following Ethernet services: GigE (via 10:1 Muxponder), 10GigE WAN PHY, 10GigE LAN PHY.

3. **[Conditional]** The OTS shall support the transport of the following OTN services: OTU1, OTU2, OTU3.

4. **[Required]** The OTS shall be transparent to the bit pattern of all optical channels (i.e., the OTS shall not modify the payload bit pattern of any signal that traverses it).

5. **[Required]** Framed wavelength services shall be supported for 2.5 and 10 Gbps SONET/SDH signals formatted for OTN transport (ITU-T G.709).

6. **[Required]** Framed wavelength services shall be supported for GigE/10 GigE signals, and signals formatted for OTN transport (ITU-T G.709).

7. **[Required]** Framed wavelength services shall be supported for 40 (ITU-T G.709) and 100 Gbps (STD TBD) signals.

8. **[Required]** The OTS shall support, in hardware and in software, the possibility to feed a specified ITU-T grid wavelength, with undefined framing, directly into the multiplexer through a "colored interface" that shall verify the wavelength and power levels (commonly known as ALIEN wavelength). Identify other characteristics of the tributary signal required to be known and monitored for proper OTS system operation with such tributary signals.

5.5.2.1.2.2 Unframed

1. **[Required]** The OTS shall support unframed wavelength services. Describe your strategy for handling unframed wavelength services.

2. **[Required]** The OTS shall support mixed framed and unframed wavelength services

5.5.2.1.3 Fiber

Table 5.5-1 lists characteristics of major fiber types. Note that the vendor should support the variation of specifications defined by the manufacturers.

1. **[Required]** Besides the fiber types described above, vendor shall list all other fiber types the system supports.

2. **[Required]** Vendor shall describe their strategy to handle routes with mixed fiber types and possible impacts on capacity and cost.

Table 5.5-1. Fiber Types and Their Characteristics

FIBER TYPE	EFFECTIVE AREA (μM^2)	AVERAGE DISPERSION (PS/NM/KM) @1550 NM	DISPERSION SLOPE ($PS/NM^2/KM$)	PMD LINK DESIGN VALUE FOR 75-KM SPAN (MEAN, PS/√KM)
Post 1993 SSMF	80	17	0.06	<0.1
TW-RS	55	4.4	0.045	<0.1
E-LEAF	72	4.2	0.09	<0.1
TW-C (1996)	55	2.7 ± 1.2	0.068	0.1

3. **[Required]** Vendor shall provide the reach table, using same format outlined in Table 5.5-2, Table 5.5-3, and Table 5.5-4, for each of the following 5 cases: (1) 50% Post 1993 SSMF and 50% TW-C (2) 50% TW-C and 50% ELEAF (3) 50% TW-C and 50% TW-RS and (4) 50% TW-RS and 50% ELEAF and (5) 34% TW-C, 33% TW-RS, and 33% ELEAF. Assume spans of the same fiber are grouped together, and no mixed fiber in any single span.

4. **[Required]** Vendor shall describe the impacts if the spans of different fiber types are intermixed, e.g., one span of Post 1993 SSMF, followed by one span of TW-C, followed by one span of Post 1993 SSMF, etc.

5. **[Required]** Vendor shall present the impacts if a single span consists of different fiber types.

5.5.2.2 Protection and Restoration

1. Protection. Protection is defined as a pre-planned alternate path for the service.

2. Restoration. Restoration is defined as the switching of the service to an alternate path after the failure.

[Required] Vendor shall describe their strategy for wavelength protection and restoration.

5.5.2.3 Performance Requirements

1. **[Required]** Jitter tolerance shall be in compliance with GR-253 Type II and ITU G.958.

2. **[Required]** Jitter transfer shall comply with GR-253 and International Telecommunications Union (ITU) G.958.

3. **[Required]** Vendor shall describe control algorithms including non-exhaustively, optical power/ VOA (variable optical attenuator) at optical line amplifiers (OLAs), OADMs and End

Terminals decision level at receiver, compensation on dispersion and PMD variation, fiber cut, add drop channels, turn up and shut down.

4. **[Required]** Vendor shall describe integrated or non-integrated optical monitoring features, what is being monitored and how the parameters will be used in the system. A block diagram is required.

5. **[Required]** In a single vendor environment, a wavelength shall traverse up to at least 20 transponders before termination of the signals is required at a terminal site. This shall be true for all data rates specified.

6. **[Required]** The OTS shall tolerate a persistent input channel signal timing deviation of at least +/- 20 ppm. This implies that the OTS must (1) operate properly in normal condition (i.e. without alarms) when any one or all of the tributaries have long-term frequency offsets of up to +/- 20 ppm and (2) maintain the system performance objectives for concatenated OTS systems.

7. **[Required]** When a signal passes through concatenated OTS sections, the output jitter shall not exceed the network interface limits of ITU-T REC. G.825.

8. **[Required]** Vendor shall describe optical layer fast and slow system control loops and techniques, as well as response times.

9. **[Required]** When one or more channels (up to 75%) fail or are removed, the remaining channels shall not experience increasing bit errors or loss of operating margin. In addition, when failed channels are restored or new channels are added, the existing channels shall not experience any transient or long-term performance deterioration.

10. **[Required]** When all channels except one fail or are removed (either instantaneously or sequentially) from all configurations, the remaining channel shall not experience an increase of bit errors or loss of operating margin. In addition, when those failed channels are restored, the existing channel shall not experience any transient or long-term performance deterioration.

11. **[Required]** Describe total system margin in terms of Q and OSNR at EOL for 40, 80, and fully loaded channels with and without OADMs at maximum reach according to Table 5.5-2, System Margins for Channel Loadings.

Table 5.5-2. System Margins for Channel Loadings

Number of OADMs	0	1	…	5
System Reach[1] (km)				
Total EOL system margin for 40 channels (dB)				
Total EOL system margin for 80 channels (dB)				
Total EOL system margin for fully loaded systems (dB)				
NOTE 1. Assume each span length is 0 km and the span loss is 23 dB.				

12. **[Required]** Describe the allocation of **itemized** system margin at EOL and in the worst-case condition (fully loaded system with all bands at maximum reach) according to the following table. Assume no OADMs. In Table 5.5.3, Allocations of Itemized System Margin at EOL, "Margin/penalty x" (x=1..n) is e.g. PMD, chromatic dispersion tolerance, aging, MPI, etc.

Table 5.5-3. Allocations of Itemized System Margin at EOL

System Reach[1] (km)	
Required OSNR for BER 10^{-15} (dB)	
BOL OSNR (dB)	
Q (dB)	
Margin/penalty 1 (dB)	
Margin/penalty 2 (dB)	
…	
Margin/penalty n (dB)	
Total EOL OSNR (dB)	

13. **[Required]** Describe total system margin in terms of Q and OSNR at EOL for 40, 80 and fully loaded channels with and without OADMs at the maximum reach (without regeneration) according to Table 5.5-4, System Margin in terms of Q and OSNR.

14. **[Required]** Describe the following related topics:
    - What is the maximum uncompensated residual chromatic dispersion the system can tolerate for 10 / 40 / 100 Gbps rates.
    - Dispersion compensation scheme (pre, post, in-line, OADM, per sub-band and per channel).
    - Techniques and technologies (fiber or DSP based) used for dispersion management.

- Granularity of dispersion compensation modules.
- Any tuning of dispersion compensation at installation or during operation.
- The dependence of modulation format on the dispersion map.
- On a per span basis, how tight is the dispersion map and what is the dispersion tolerance for future repair or re-route without a service impact.
- Dispersion tolerance due to an outside plant temperature change between –20C and 40C.

15. **[Required]** State the maximum uncompensated PMD the system can tolerate at 10/40/100 Gbps and highest rate. State how much of it is for fiber PMD. The vendor shall also describe the impacts on reach if this PMD value is exceeded.

16. **[Required]** Describe the maximum single point of reflection the system can tolerate and if there are restrictions on single splice reflectance and location in a span (for example, near the entrance point of high Raman power etc.).

17. **[Required]** Describe the tolerance of the system to multiple points of reflection and if there are restrictions on splice reflectance, splice count and location in a span (for example, near the entrance point of high Raman power etc.).

18. **[Required]** State the maximum tolerated optical return loss at the transmit and receive end of the fiber in each span.

19. **[Required]** State how the values for margin and allocations for transmission impairments (as specified in the requirements in this section on span loss, dispersion, PMD, reflection were tested and verified.

5.5.2.4 Reliability and Quality Assurance

1. **[Required]** The vendor shall conform to the following reliability and quality program requirements, unless specifically overridden or modified by another requirement in this document:

   - Telcordia GR-282-CORE, Software Reliability and Quality Acceptance Criteria,
   - Telcordia GR-2911-CORE, Software Inventory for Network Element Software Management,
   - Telcordia TR-NWT-000179, Software Quality Program Generic Requirements,

- Telcordia TR-NWT-000418, Generic Reliability Assurance for Fiber Optic Transport Systems, and

- Telcordia SR-NWT-002419, Software Architecture Review Checklists.

2. **[Required]** Provide the list of critical components in your system, the strategy for sourcing those critical components, and describe in detail the risk mitigation strategy for critical components and the impact on technology selection.

3. **[Required]** Provide country of origin of the critical components as well as final assembly location of the system.

5.5.2.5 Transponder Requirements

1. **[Required]** Transponders shall comply with the DWDM wavelength grid as specified in ITU G.694.1.

2. **[Required]** Transponders shall support tunable lasers, which are tunable over whole band for both transmit and receive functions.

3. **[Required]** All transponders shall support built-in self BER test function.

4. **[Required]** Transponders shall support G.709 specifications for OTN services.

5. **[Required]** Transponders shall have non-intrusive SONET/SDH B1 monitoring capability.

6. **[Required]** Describe FEC overhead, if it is standardized or proprietary, and how much coding gain will be achieved.

7. **[Required]** Describe the maximum uncompensated residual chromatic dispersion the transponder can tolerate for 10/40/100 Gbs rates in a back-to-back mode for a penalty number as allocated in the margin table.

8. **[Required]** Describe details of modulation format and how it optimizes the system performance.

9. **[Required]** Describe any pre-emphasis techniques used in the system and details of how it is implemented as channels are added and dropped.

10. **[Required]** Describe economic solutions for different reaches (e.g. 500~1000 km traffic). Describe the cost reduction strategies, such as transponders with shorter reaches. The vendor

shall note any additional circuit pack codes and any deviation from requirement responses provided for the ULH system in this document.

11. **[Required]** Describe the approach used for simple line protection (e.g. 1+1) and any additional circuit packs to achieve this.

12. **[Required]** The vendor shall supply through-transponder(s) to eliminate unnecessary O/E conversions for wavelength regeneration at OADM, OXC and regenerator sites.

13. **[Required]** Provide a transponder to interface with 10/40/100Gbps unframed wavelength services.

14. **[Required]** A transponder shelf shall support all types of transponders, or a combination of them. No slot shall be bit-rate specific.

15. **[Required]** There shall be no human (manual) tuning or intervention (such as power or wavelength adjustment) involved after adding transponders.

16. **[Required]** Transponder shall support all wavelengths and required transmission rates with a minimum reach of 2000 kilometers without O-E-O regeneration.

5.5.2.6 Interface Requirements

1. **[Required]** Transponders shall support an OC48/STM16 interface.

2. **[Required]** Transponders shall support an OC192/STM64 interface.

3. **[Required]** Transponders shall support a GigE interface.

4. **[Required]** Transponders shall support a 10GigE WAN PHY interface.

5. **[Required]** Transponders shall support a 10GigE LAN PHY interface.

6. **[Required]** The transponders shall support OC768/STM256 interfaces.

7. **[Required]** The transponder shall support all OTN rates including ODU1/ODU2/ODU3 and 100Gbs in future.

8. **[Required]** The transponders shall support Short Reach (SR) optics per Telcordia GR-253-CORE.

9. **[Required]** Provide information on the availability of additional client interface types, besides SR (for example: LR-1, LR-2, LR-3, IR-1, IR-2, etc.).

10. **[Required]** The transponders shall support client interfaces at 1310 and 1550 nm.

11. **[Required]** The transponders shall support client interface at 850 and 1310 nm. for GigE signals.

5.5.2.7 Muxponder Requirements

In order to better utilize the wavelength capacity, 4:1 muxponders would be needed for SONET/SDH signals and 10:1 muxponder for 1GbE signal.

1. **[Required]** Transponders shall support a four-into-one mux-ponder (4 2.5G signals multiplexed into one 10G signal). If the vendor equipment supports this functionality, the equipment shall meet the requirements listed in this section (3.2.1.3).

2. **[Required]** The Vendor shall support a 4:1 10G Mux. The 4:1 10G multiplexer shall receive four standards compliant OC-48/STM-16 signals, from one to four sources, and multiplex them onto a signal for transport over a 10G-capable channel on the system.

3. **[Required]** The 4:1 10G multiplexer shall transmit a 10G channel in each of the operating bands specified by the vendor. The vendor shall indicate any excluded band.

4. **[Required]** The 4:1 10G multiplexer shall occupy no more physical space than an OC-192/STM-64 transmit/receive pack.

5. **[Required]** The 4:1 Mux shall transfer the OC-48/STM-16 signals through the system transparently.

6. **[Required]** Describe how the transparency is accomplished through the 4:1 Mux system.

7. **[Required]** It shall be possible to have any mixture of payload types in the OC-48 or the STM-16 input (e.g. for SONET input: STS-1, STS-3c, STS-12c, STS-48c and any combination thereof).

8. **[Required]** The engineering rules for the 4:1 10G multiplexer configuration shall be the same as the standard OC-192/STM-64 configuration without the need to change any system components, including dispersion compensation.

9. **[Required]** The OC-48/STM-16 interface (i.e. SR, etc.) for a 4:1 10G mux shall have identical compliance to all of the requirements for an OC-48/STM-16 interface to an OC-48/STM-16 standard transponder as specified in this document.

10. **[Required]** An OC-48/STM-16 through the OTS that is multiplexed and demultiplexed through the 4:1 10G multiplexers shall meet the same performance requirements as an OC-48/STM-16 signal through the OTS using OC-48/STM-16 transponders. Performance requirements include, but are not limited to BER, Errored Seconds, Severely Errored Seconds and Availability.

11. **[Required]** An OC-48/STM-16 through multiple concatenated systems containing 4:1 10G multiplexers shall meet the same performance requirements as an OC-48/STM-16 signal through concatenated OTSs using OC-48/STM-16 transponders. The same number of concatenated 4:1 10G multiplexers shall be supported as the number of concatenated OC-48/STM-16 transponders. Performance requirements include, but are not limited to Jitter Generation and Tolerance.

12. **[Required]** The maximum number of 10G channels equipped with 4:1 10G multiplexers in an OTS must be equal to the maximum number of OC-192/STM-64 channels supported in an OTS.

13. **[Required]** The 4:1 10G multiplexer shall operate without degradation if less than four of the OC-48/STM-16s have a valid OC-48/STM-16 signal. There shall be no requirement that any number of the OC-48/STM-16 wavelengths should be provisioned.

14. **[Required]** The loss of one or more provisioned OC-48/STM-16 inputs to a 4:1 10G mux shall not affect the performance of any other provisioned OC-48/STM-16 on that multiplexed channel.

15. **[Required]** Describe the timing options available with your mux-ponders, including line timing from one or more of the incoming lines, external timing, internal timing, etc.

16. **[Required]** Describe the expected clock performance (including stratum level), any applicable standards they are using, and your clock redundancy plan.

17. **[Required]** Describe if it is possible to pass the payload timing transparently through your system, and how is this accomplished.

18. **[Required]** Describe your methodology for controlling jitter within your mux-ponders, and how this is measured and verified for each type of input and multiplexed signal.

5.5.2.8 Common Physical Design Requirements

This section defines all common requirements that are applicable to all the OTS network elements. Responses to this section must also address ancillary equipment that are required in the vendor's solution.

The following documents are used throughout the physical design section and are referenced within each requirement, when appropriate:

- Telcordia GR-63-CORE, *Network Equipment-Building System (NEBS) Generic Equipment Requirements*, Issue 1, October 1995. Available through Telcordia Publications (1-800-521-2673).
- Telcordia GR-78-CORE, *General Physical Design Requirements for Telecommunications Products and Equipment*, Issue 1, September 1997. Available through Telcordia.
- Telcordia GR-383-CORE, *Generic Requirements for Common Language Bar Code Labels*, Issue 1, July 1997. Available through Telcordia.
- Telcordia TR-NWT-000295, *Isolated Ground Planes: Definition and Application to Telephone Central Offices*, July 1992. Available through Telcordia.
- Telcordia GR-1089-CORE, *Electromagnetic Compatibility and Electrical Safety - Generic Criteria for Network Telecommunications Equipment*, Issue 2, Revision 1, February 1999. Available through Telcordia.
- Telcordia SR-3580, *Network Equipment-Building System (NEBS) Criteria Levels*, Issue 1, November 1995. Available through Telcordia.
- Telcordia GR-1274-CORE, *Generic Requirements for Reliability Qualification Testing of Printed Wiring Assemblies Exposed to Airborne Hygroscopic Dust*, Issue 1, May 1994. Available through Telcordia.
- ANSI T1.315-1994, *Voltage Levels for DC-Powered Equipment - Used in the Telecommunications Environment*, May 1994. Available through ANSI.

All equipment to be deployed in the central office environment, regardless of application, must comply with the requirements of this section. Mission criticality or presence of network traffic bring other criteria into play, but this set must always be present to protect the people working in the facility and the other more critical equipment.

1. **[Required]** Each network element shall meet requirements addressed in this document and shall have met European Community (EC) or Pacific Host Nation approvals required for foreign countries. Provide information on the countries that the equipment is currently approved, including equipment part numbers and other applicable documentation.

2. **[Required]** The Vendor shall have obtained EC (European Community) and Pacific areas approvals and permits for connection and operation with to the public networks for each network element. Provide information on the countries that the equipment is currently approved, including equipment part numbers and the public network providers approved.

3. **[Required]** Each network element shall meet requirements addressed in this section and shall be compliant, at a minimum, without future hardware and/or memory upgrades or replacements.

4. **[Required]** Equipment racks' weight shall be within generally acceptable standards defined for raised floor application.

5. **[Required]** Equipment racks shall allow cable installation above and below each rack.

6. **[Required]** The NE shall be able to receive all types of cables from the top or bottom of the bay/cabinets. When receiving from the bottom it shall be able to accommodate a raised floor environment.

7. **[Required]** All inter-bay cabling shall be routed above and below each rack allowing various different cable lengths up to 100 m. If the equipment cannot support 100 m, the vendor shall state the maximum cable length supported.

8. **[Required]** Within a NE, all intra-system cabling shall maximize separation of redundant cables and fibers (i.e. working/protection, east/west, timing cables, switch cables, etc.).

9. **[Required]** All working signal cables shall be routed on separate physical paths from the protection cables within the system. Between systems, all separations shall be maintained. All inter-system connections shall be able to support a minimum distance of 100m.

10. **[Required]** A and B power cables shall have physically diverse routing within the bay/cabinet.

11. **[Required]** Current Drain information shall be provided to outline current draws in both normal and worst case voltage scenarios. (The latter information shall also address impacts of failed feeds and temperature where variable speed fans or other make such considerations appropriate). When multiple configurations are possible because of card variety, test data on

several "generic" configurations shall be provided with a table of power numbers to help the user interpolate the approximate values of other configurations.

12. **[Required]** Each element/shelf/circuit pack, whichever is the smallest independent load device of the NE, shall obtain power from two completely independent power units. Furthermore, the return path from the power units shall remain completely independent (Telcordia TR-NWT-000295). If one of the power units fails, an alarm shall be generated and the load shall be carried by the other unit without manual intervention and without interruption of service or functionality. The other power unit shall support the operation of the element/shelf/circuit pack until the problem with the faulty unit is corrected.

13. **[Required]** All network equipment shall conform to the spatial and environmental criteria specified in Telcordia FR 796 and GR-63-CORE.

14. **[Required]** All network equipment, along with its power distribution panel and all associated/ancillary hardware, shall be capable of being mounted in standard EIA 310C 23" relay rack, 84" in height.

15. **[Required]** All network equipment shall be capable of being operated and maintained with access only to the front of the unit.

16. **[Required]** All network equipment shall be capable of being mounted in a back-to-back arrangement or directly against a building wall.

17. **[Required]** All network equipment, along with its power distribution panel and all associated/ancillary hardware, shall be capable of being mounted in standard EIA 310C 23" relay rack, 78" in height.

18. **[Required]** All network equipment, along with its power distribution panel and all associated/ancillary hardware, shall be capable of being mounted in standard EIA 19" relay rack, 78" in height.

19. **[Required]** All network equipment, along with its power distribution panel and all associated/ancillary hardware, shall be capable of being mounted in X-Mark/CDT Cabinets, part number XSL78-4-1S0002, size 78" x 23" x 30".

20. **[Required]** All network equipment shall demonstrate an operational availability of all functions and services of 99.9997 %.

21. **[Required]** All network equipment shall comply with the earthquake, office vibration, and transportation vibration criteria specified in: Telcordia GR-63, section 4.4.

22. **[Required]** All network equipment shall be fully NEBS, Level 3 compliant.

23. **[Required]** All network equipment shall meet the environmental conditions described in: Telcordia GR-63-CORE NEBS Requirements: Physical Protection.

24. **[Required]** All network equipment shall meet the environmental conditions described in: ETS-300-019 Environmental Engineering (EE); Environmental Conditions and Environmental Tests for Telecommunications Equipment.

25. **[Required]** All network equipment shall be designed to operate in a communication equipment environment, adjacent to or in the vicinity of others types of equipment which may include digital radio equipment, fiber optic terminal equipment, FDM analog microwave, VHF/UHF base stations, satellite ground terminals, transfer trip and power line carrier equipment, and telephone signaling equipment.

26. **[Required]** All network equipment shall meet the EMC/EMI requirements defined in: Telcordia GR-1089-CORE Electromagnetic Compatibility and Electrical Safety - Generic Criteria for Network Telecommunications Equipment.

27. **[Required]** All network equipment shall meet the EMC/EMI requirements defined in: FCC Part 15 Class A.

28. **[Required]** All network equipment shall meet the EMC/EMI requirements defined in: ETS EN 50082.

29. **[Required]** All network equipment shall meet the EMC/EMI requirements defined in: ETS EN 55022 Information Technology Equipment - Radio Disturbance Characteristics - Limits and Methods of Measurement.

30. **[Required]** All network equipment shall meet the EMC/EMI requirements defined in: ETS EN 300-386 Electromagnetic Compatibility and Radio Spectrum Matters (ERM); Telecommunication Network Equipment; Electromagnetic Compatibility (EMC) Requirements.

31. **[Required]** All network equipment shall be designed to operate continuously in the following environment ranges without degradation. Temperature: 0 to +50°C, Humidity: 5 to 95% relative humidity, without condensation.

32. **[Required]** All network equipment shall be designed to be fully operational after transportation and/or storage in the following environment ranges: Temperature: -40 to +70°C, Humidity: 5 to 95 % relative humidity, without condensation.

33. **[Required]** All network equipment shall be designed to operate continuously in the following environment range without degradation. Altitude: -100 to 15,000 ft AMSL.

34. **[Required]** All network equipment shall be designed to be fully operational after transportation and/or storage in the following environment range: Transport Altitude: -100 ft to +40,000 ft AMSL.

35. **[Required]** All network equipment shall adhere to NEBS level 3 compliance standards for acceptable voltage ranges, EMI, and ESD safety, and shall be operable using standard 48V DC power as well as having redundant isolated power input feeds. For certain sites, an alternative AC/DC rectifier may need to be supplied to power the system and shall be able to switch 110/220 V with redundant isolated power modules.

36. **[Required]** All network equipment shall be fully operational throughout the battery voltage range of: -41.5 to -56 VDC.

37. **[Required]** All network equipment shall not be damaged and recover to normal performance following application of the following maximum transient voltages for the duration's given (nominal voltage 48 VDC): 75 Vp-p for 1 msec, 60Vp-p for 500 msec.

38. **[Required]** All network equipment in the transport layer primary OS interface shall provide the capability for reporting alarms of external equipment and general housekeeping alarms. A minimum of 16 user-defined alarms shall be provided, with the option to expand to 32 user-defined alarm points. Capability shall be provided for minimum of 8 user defined remote control points for external functions. This capability shall be provide by relays, not TTL.

39. **[Required]** The OTS shall support having all data cross connects stored locally and redundantly; and automatically restored without user intervention, in the case of failure, within a period of five minutes.

40. **[Required]** The OTS shall provide the capability to rollback to the previous operational version of software.

41. **[Required]** The OTS shall conform to memory administration, and system administration and security standards as documented. Telcordia TR-472 and GR-253.

42. **[Required]** All future software for the OTS shall interoperate with the previous deployed GIG-BE system operational software version/release.

43. **[Required]** The OTS shall support software upgrades that directly use or translate the previous version's configuration database.

44. **[Required]** The software of the OTS shall be designed and upgraded in a modular fashion so that an entire code does not have to be replaced when a portion is upgraded.

45. **[Required]** The OTS shall be designed with an accessible file system to allow for multiple versions of software, logs, and file manipulation/integrity checks to be performed prior to upgrading or downgrading software and/or firmware.

5.5.2.9 Optical Line Amplifier (OLA)

1. **[Required]** Describe the architecture, including all internal components, of the optical amplifier(s) with text and diagram(s).

2. **[Required]** Describe the number of optical amplifier codes for all amplifiers (e.g. power booster, in-line amplifier or pre-amplifier, as well as Raman amplification, if applicable).

3. **[Required]** Describe any fixed and dynamic gain flattening devices and equalization technique used in the amplifiers. In particular, describe how the SRS tilt is being adjusted in the system when adding channels and when adding a band. Describe how often and how flexible the dynamic gain flattening devices are used.

4. **[Required]** Describe the in-line dispersion compensation technique (over- or under compensated, slope / non-slope, etc.) and technology used.

5. **[Required]** The system shall support the use of a connector to the system fiber; Raman amplifiers may not be directly spliced to the transmission fiber and must be field-replaceable, without the need for special equipment.

6. **[Required]** Describe the use of Raman Amplification in the system. This shall include information on the following:
   - Optical channels that are supported with Raman Amplification?
   - How many pumps and wavelengths, and maximum optical power at each wavelength for different supported fiber types.
   - If the Raman is forward or backward pumped.
   - Raman pump reliability and the impact to the system if one of the pumps fails.
   - Any restrictions to connector and fiber splices in terms of high Raman pumping power and reflections.

- Is it optional or required? Can the system be configured with or without it depending on the actual route design? If so, the vendor shall provide the Engineering Rules with and without Raman Amplification using fibers described in Table 3.1.3.2-1 (section 3.1.3.2)

7. **[Required]** The total optical power emitted from the OTS to be coupled into the fiber, shall not exceed the power limit of IEC Class 3B (+27dBm).

8. **[Required]** The OTS shall monitor and report on the operation of the Raman pumping lasers including power on, off, optical output power, operating current, and total ORL.

9. **[Required]** Once detecting the failure of Raman pumping lasers, the OTS shall generate an alarm, but shall not shut off the system.

10. **[Required]** The Raman pumping lasers shall automatically shut off if a fiber is broken or a connector disconnected in the span pumped by the Raman amplifier.

11. **[Required]** The vendor shall document all special cleaning procedures required by the use of Raman Amplification or excessive power levels in any other part of the system. The vendor shall supply a test plan which documents testing methods for the adequacy of the cleaning procedures.

12. **[Required]** Provide any tools or instruments needed to perform special cleaning procedures required by the use of Raman Amplification or excessive power levels in any other part of the OTS as part of the OTS system for maintenance.

13. **[Required]** The OTS shall have an integrated power management algorithm, which invokes power monitoring and adjustment devices to compensate for power variations across the optical wavelengths.

14. **[Required]** The OLA system shall be able to balance individual wavelengths so that power output levels exhibit less than 0.5 dB variance from the mean output level without remote or direct intervention from a network operator.

15. **[Required]** When one or more channels fail or are removed, the remaining channels shall not experience increased bit errors or loss of operating margin.

16. In addition, when failed channels are restored or new channels are added, the existing channels shall not experience any transient or long-term performance deterioration.

17. **[Required]** The power management algorithm shall cause no interruptions in OSC communications at any time.

18. **[Required]** OSC signals shall experience no increased errors at any time up to End-Of-Life (EOL), including during wavelength provisioning or line equalization.

19. **[Required]** Amplifiers shall require less than 1 ms to return all wavelength power output levels to within 1 dB of pre-insertion/drop levels – transient suppression statistics shall be provided for OLA systems.

20. **[Required]** OLA systems shall maintain safe (Hazard level 1) system operation in the event of input signal loss or fiber cut.

21. **[Required]** Chromatic dispersion compensation shall be able to fully compensate a 150 km span for each fiber type, as specified in the fiber requirements section.

22. **[Required]** Chromatic dispersion compensation shall be provided for different fiber lengths in 10, 20, or 30 km increments, if the technique requires the compensation to be periodically dispersed.

23. **[Required]** The OTS equipment shall enable pre- and post- dispersion compensation options.

24. **[Required]** A secured external monitor port is required at each optical amplifier. For devices that contain a full-featured internal OSA, an external monitor port shall still be required.

25. **[Required]** Internal OSA functionality shall support 25 GHz ITU grid spacing with minimum 5 % wavelength accuracy.

26. **[Required]** Internal OSA functionality shall provide a minimum accuracy of 0.2 dB for each wavelength.

27. **[Required]** Internal OSAs **shall** provide sweep times of less than 1 sec.

28. **[Required]** Internal OSAs shall provide the ability to display all wavelengths simultaneously.

29. **[Required]** Internal OSAs shall provide the ability to retrieve data to be stored at a remote storage site.

30. **[Required]** Internal OSAs shall provide the ability to view various calculated data such as gain tilt, output tilt, gain variation, gain difference, noise level, total received power, total launched power, etc.

31. **[Required]** Internal OSAs shall provide the ability to report Q factor. (not critical)

32. **[Required]** Internal OSAs shall have the ability to show eye diagrams. (not critical)

33. **[Required]** Internal OSAs shall have the ability to estimate Optical Signal to Noise Ratio (OSNR) for each wavelength.

34. **[Required]** All measurements made available at the internal OSA shall be available at the external OSA port. (not critical)

5.5.2.10 Optical Supervisory Channel (OSC)

The OTS shall include an Optical Supervisory Channel (OSC) linking the two OTS Gateway Network Elements (GNEs), with access at each OTS OLA site. All telemetry, data, and voice traffic originating at OTS OLA sites shall be routed over this service channel.
A diagram of the OSC appears below in Figure 5.5-9, Optical Supervisory Channel. The optical line rate, the optical format and interface partitioning internal to the OTS may be a proprietary implementation.

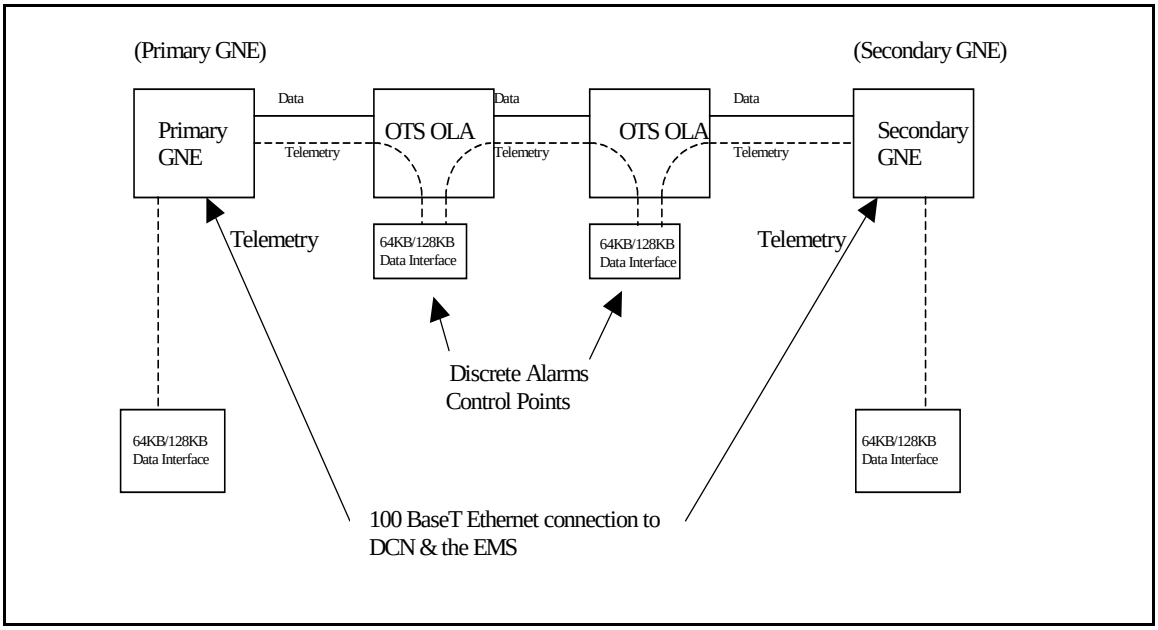


Figure 5.5-9. Optical Supervisory Channel

1. **[Required]** The OLA, ROADM, ET systems shall terminate/insert an Optical Supervisory Channel (OSC) with a wavelength that adheres to ITU-T specifications

2. **[Required]** The OLA, ROADM, and END TERMINAL systems shall utilize the ITU-T specified OSC for in-band management communications.

3. **[Required]** The OLA, ROADM, and END TERMINAL systems shall use the same OSC wavelength.

4. **[Required]** The internal diagnostics for OLA, ROADM, and END TERMINAL systems shall report OSC failure.

5. **[Required]** The OLA, ROADM, and END TERMINAL systems shall report any OSC channel input/output failure (via out-of-band DCN).

6. **[Required]** The OLA, ROADM, and END TERMINAL systems shall report any OSC channel BER threshold violation.

7. **[Required]** The OLA, ROADM, and END TERMINAL systems shall provide OSC interfaces that allow for interoperability with all adjacent equipment within the optical network (wavelength, modulation, protocol, etc) from the same vendor.

8. **[Required]** The OSC shall be able to operate error-free across 150 km of each specified fiber type with a span loss of 50 dB.

9. **[Required]** The OSC shall operate at 2 Mb/s and above.

10. **[Required]** Architecturally, the OSC shall be passively optically separated from the transport optical signals immediately after input connection of the OTS.

Below are the OLA-specific physical design requirements.

1. **[Required]** The vendor shall comply with all requirements listed in section 3.4 of this document. The vendor shall list all discrepancies.

2. **[Required]** The OLA shall support hot swappable modular components, including but not limited to fans, amplifier modules, in-band/out-of-band management interfaces, power supplies, and control processor.

3. **[Required]** The OLA shall support redundant fans, management interfaces, power supplies, and control processors.

4. **[Required]** The optical amplifier shall be able to fit in either a 19” or a 23” rack with depth no greater than 30” and height no more than 84”

5. **[Required]** The OLA overall dimensions shall be no more than one 7.2 ft standard Telco rack for a full 80 wavelengths bi-directionally, or two racks for 160 wavelengths, including out of band management functions

6. **[Required]** The OLA power consumption shall be kept below 2000 Watts for all equipment at an OLA site.

7. **[Required]** The vendor shall identify their OLA power and space requirements for all specified configurations.

5.5.2.11 OADM

This section presents the requirements for 2-degree OADM. Multi-degree OADM requirements will be incorporated in the next release of this document.

1. **[Required]** The OADM shall be capable of supporting a minimum of two network-side interfaces and perform both optical bypass and add/drop functions.

2. **[Required]** The Vendor shall explain the following:
   - At any given OADM site, the allowed add and drop wavelength percentage of the total system capacity. Any wavelength not explicitly dropped or added shall be passed through the OADM.
   - Any wavelength banding restriction.
   - Wavelength reuse.

3. **[Required]** It shall be possible to add/drop, or pass express, any of the optical channels at an OADM site in any order.

4. **[Required]** If a wavelength is dropped at an OADM site, then the same wavelength shall be able to be added at that site. However there shall be no requirement that the wavelength that is dropped must be matched by a corresponding wavelength that is added, and vice versa. In summary, the options for a given wavelength at an OADM site shall include (but not be limited to).

   - Dropping an incoming wavelength and not adding a new corresponding outgoing wavelength
   - Accepting a non-provisioned incoming wavelength and adding a new outgoing wavelength.

- Dropping an incoming wavelength and adding a new corresponding outgoing wavelength

5. **[Required]** The OADM shall be capable of supporting dynamic wavelength selection without pre-cabling being required.

6. **[Required]** The OADM shall be capable of dropping all wavelengths from each of two line side fiber connections to tributary side optics

7. **[Required]** The OADM shall be capable of adding all wavelengths to each of two line side fiber connections from tributary side optics.

8. **[Required]** The OADM shall be capable of dropping any specific wavelength, independent of other wavelengths to be dropped.

9. **[Required]** The OADM shall be capable of adding any specific wavelength, independent of other wavelengths to be added.

10. **[Required]** Vendor shall describe the hair-pinning capabilities of your OADM.

11. **[Required]** The OADM shall support wavelength regeneration, including wavelength conversion, using back-to-back transponders or through-transponders via hair-pinning.

12. **[Required]** The activation of additional services on interfaces in the OADM shall be non-service affecting to existing traffic and shall not cause any increase in bit-errors.

13. **[Required]** The deletion of active services on interfaces in the OADM shall be non-service affecting to the remaining traffic and shall not cause any increase in bit-errors.

14. **[Required]** Hardware upgrades of the OADM to support higher tributary interface density shall not disrupt operational traffic.

15. **[Required]** Hardware upgrades of the OADM to support higher line interface density shall not disrupt operational traffic.

16. **[Required]** The OADM shall provide latching capability. (Latching is the ability of the OADM to maintain its current state in the event of power failure.)

17. **[Required]** The OADM shall provide optical multicasting capability. (Multicasting is the OADM's ability to allow one input wavelength to be duplicated on multiple output tributary and line ports).

18. **[Required]** The OADM shall support dynamic per-wavelength power leveling.

19. **[Required]** The addition or deletion of a wavelength service on the OADM shall not cause an increase in BER or data loss on other wavelengths.

20. **[Required]** The OADM shall not incur increased bit errors associated with wavelength provisioning or line equalization.

21. **[Required]** The failure of an upstream line system shall not cause the OADM to increase in BER or lose data on the remaining active wavelengths.

22. **[Required]** The optical power penalty due to crosstalk for any signal passing thru a fully loaded OADM shall be < 1 dB.

23. **[Required]** The system is required to automatically redirect working paths to available spare fibers/wavelengths in the event of a primary path failure. The OADM shall not inhibit ring or linear protection switching initiated by ODXC, MSPP or other electronic device.

24. **[Required]** The OADM shall support 1+1 protection functionality with fully diverse routing. The OADM shall not inhibit ring or linear protection switching initiated by ODXC, MSPP or other electronic device.

25. **[Required]** The switching time for 1+1 protection shall be ≤ 50 ms. The OADM shall not inhibit ring or linear protection switching initiated by ODXC, MSPP or other electronic device.

26. **[Required]** The switching time for 1+1 protection shall be ≤ 20 ms. The OADM shall not inhibit ring or linear protection switching initiated by ODXC, MSPP or other electronic device.

27. **[Required]** The OADM shall support redirection of light paths via the EMS/NMS.

28. **[Required]** The OADM shall support linear protection topologies. The OADM shall not inhibit ring or linear protection switching initiated by ODXC, MSPP or other electronic device.

29. **[Required]** The OADM shall support ring protection topologies. The OADM shall not inhibit ring or linear protection switching initiated by ODXC, MSPP or other electronic device.

OADM specific physical design requirements are listed below.

1. **[Required]** The vendor shall comply with all requirements listed in General Physical Requirements of this document. The vendor shall list all discrepancies.

2. **[Required]** The OADM shall support hot swappable modular components, including but not limited to fans, switch fabric, interface ports, power supplies, and control processor.

3. **[Required]** The OADM shall support redundant fans, switching fabrics, power supplies, and control processors.

4. **[Required]** The OADM equipment shall be able to fit in either a 19” or a 23” rack with depth no greater than 32” and height no more than 84”.

5. **[Required]** The fully configured OADM (excluding the transponder shelves) shall not exceed two full 84" racks.

6. **[Required]** The fully configured OADM shall not exceed one full 84" rack.

7. **[Required]** The OADM shall not require contiguous rack locations.

8. **[Required]** The OADM weight shall be such that the device can be mountable in a standard Telco rack or secure cabinet with standard rack screws and not require unusual strength reinforced racking.

5.5.2.12 Planning Tools

To aid in network design and implementation, the vendor shall have a physical layer planning tool available that is capable of modeling the equipment capability. Additional modeling tools are described as desired functionalities to address optical transport layer and optical network layer.

5.5.2.12.1 Optical Layer (Physical) Planning Tool

1. **[Required]** The vendor shall make available a physical layer software planning tool, including all necessary documentation to aid the use of the tool.

2. **[Required]** The software planning tool shall be able to run on a standard PC.

3. **[Required]** Provide a set of flexible engineering tools that calculate the Q and OSNR due to variation of fiber characteristics, including but not limited to, fiber type, span length, span loss, and PMD.

4. **[Required]** Provide information on the physical layer planning tool, its simulation engine and give a functional overview on the use of the tool, including its capabilities and limitations.

5. **[Required]** State how the physical layer planning tool has been verified and tested to give the correct output of the optical transmission system behavior.

6. **[Required]** The vendor shall propose an optical modeling tool, herein referred to as the Tool, to support the engineering solution proposed. If the vendor is to provide the Tool, all the requirements in this section (5.5.2.12.1) shall apply.

7. **[Required]** Provide a Tool capable of simulating and verifying optical transport, wavelength routing, and grooming designs. The Tool shall address risk reduction and deployment design cost effectiveness prior to procurement, deployment and service turn-up.

8. **[Required]** The Tool shall characterize the vendor's equipment in the following categories:

    - All optical transport
    - OEO functionality
    - Alien wavelength transport capability

9. **[Required]** The Tool shall be capable of photonic simulation, analysis, and design to include, but not limited to the requirements listed in this table.

10. **[Required]** The Tool shall include the following parameters as part of the Engineering Rules for its solution:

    - Insertion Loss
    - Per span length
    - Per channel optical power
    - Chromatic dispersion
    - Chromatic dispersion slope
    - Polarization mode dispersion

11. **[Required]** The Tool shall have Graphical Views, user friendly GUIs with menu driven commands.

12. **[Required]** The Tool shall provide topology view of the network.

13. **[Required]** The Tool shall provide link and span design.

14. **[Required]** The Tool shall provide protection and failure analysis.

15. **[Required]** The Tool shall provide MTBF and availability of the equipment.

16. **[Required]** The Tool shall provide amplifier and optical regeneration system placement analysis.

17. **[Required]** The Tool shall provide optimal cost solution analysis.

18. **[Required]** The Tool shall support multi-fiber implementation analysis

19. **[Required]** The Tool shall provide simulation through "what if" scenarios. The Vendor shall list all tradeoff scenarios that the tool supports.

20. **[Required]** The Tool shall provide user constraint settings for analysis.

21. **[Required]** The Tool shall provide Automated Failure (Link and Node) Scenarios for analysis.

22. **[Required]** The Tool shall provide results through printable reports, bill of materials, etc.

5.5.2.12.2 Network Layer Planning Tool

1. **[Required]** The vendor's optical – digital switch modeling tools shall be capable of wavelength routing, digital switching, and grooming simulation, analysis, and design to include, but not limited to the requirements defined in this table.

2. **[Required]** The network planning tool shall support emulation of the equipment link state and routing algorithms.

3. **[Required]** The network planning tool shall support user constraints supported by the equipment.

4. **[Required]** The network planning tool shall support Protection/Restoration features supported by the equipment.

5. **[Required]** The network planning tool shall support MTBF and availability calculations and analysis.

6. **[Required]** The network planning tool shall support optimal cost solution modeling.

7. **[Required]** The network planning tool shall support simulation through "what if" scenarios. The vendor shall list all tradeoff scenarios that the tool supports.

8. **[Required]** The network planning tool shall support node, link, connection reports, bill of materials generations.

9. **[Required]** The network planning tool shall support automated failure (Link and Node) scenarios.

10. **[Required]** The network planning tool shall have graphical views, user friendly GUI, menu driven user interfaces.

11. **[Required]** The network planning tool shall support topology view of the network.

12. **[Required]** The network planning tool shall support Protection and Failure analysis.

13. **[Required]** The network planning tool shall support MTBF and availability analysis.

14. **[Required]** The network planning tool shall support optimal cost solution analysis.

15. **[Required]** The network planning tool shall support user constraint settings.

16. **[Required]** The network planning tool shall support traffic engineering.

17. **[Required]** The network planning tool shall support traffic variation analysis.

18. **[Required]** The network planning tool shall support results through printable reports, bill of materials.

5.5.2.13 Standards Compliance

The DISN Transport System shall comply with the most recent published version of the following standards:

1. **[Required]** G.709 Interface for the Optical Transport Network (OTN)

2. **[Required]** G.872 Architecture for Optical Transport Networks.

3. **[Required]** G.808.1 Generic Protection Switching-Linear Trail and Subnetwork Protection, G.808.2, Generic Protection Switching – Rings.

4. **[Required]** G.875 Optical Transport Network (OTN) Management Information Model for the Network Element View.

5. **[Required]** G.874.1 Optical Transport Network: Protocol-neutral management information model for the network element view.

6. **[Required]** G.874 Management aspects of the optical transport network element.

7. **[Required]** M.24otn Error Performance Objectives and Procedures for Bringing-into-Service and Maintenance of Optical Transport Networks.

8. **[Required]** G.829, Error performance events for SDH multiplex and regenerator sections.

9. **[Required]** G.828, Error performance parameters and objectives for international, constant bit rate synchronous digital paths.

10. **[Required]** G.826, End-to-end error performance parameters and objectives for international, constant bit rate digital paths and connections.

11. **[Required]** G.825, The control of jitter and wander within digital networks.

12. **[Required]** G.959.1, Optical transport network physical layer interfaces.

13. **[Required]** G.873.1 OTN – Linear Protection, G.873.2 OTN – Ring Protection.

14. **[Required]** G.8251, The control of jitter and wander within the Optical Transport Network (OTN).

15. **[Required]** G.798, Functional characteristics of optical networking equipment.

16. **[Required]** G.876 OTN Management Information Model – SNMP Implementation.

17. **[Required]** G.691, Optical interfaces for single-channel STM-64, STM-256 and other SDH systems with optical amplifiers.

18. **[Required]** G.957 Optical Interfaces for Equipment and Systems Relating to Synchronous Digital Hierarchy.

19. **[Required]** G.694.1, Spectral grids for WDM applications: DWDM frequency grid.

20. **[Required]** G.692, Optical interfaces for multi-channel systems with optical amplifiers.

21. **[Required]** G.783, Characteristics of synchronous digital network (SDH) equipment functional blocks.

22. **[Required]** G.707 Network interface for Synchronous Digital Hierarchy (SDH).

23. **[Required]** RFC 3209 RSVP-TE: Extensions to RSVP for LSP Tunnels for Control Plane Signaling.

24. **[Required]** RFC 2328 OSPF Version 2.0 or ISIS for Control Plane Routing.

25. **[Required]** GR-253 CORE, Synchronous Optical Network (SONET) Transport Systems: Common Generic Criteria.

26. **[Required]** GR-499-CORE, Transport Systems Generic Requirements (TSGR): Common Requirements.

27. **[Required]** GR-1312-CORE, Generic Requirements for Optical Fiber Amplifiers and Proprietary Dense Wavelength-Division Multiplexed Systems.

28. **[Required]** TR-NWT-000917, SONET Regenerator (SONET RGTR) Equipment Generic Criteria.

29. **[Required]** TR-NWT-000418, Generic Reliability Assurance for Fiber Optic Transport Systems.

30. **[Required]** GR-2979-CORE, Generic Requirements for Optical Add-Drop Multiplexers (OADM) and Optical Terminal Multiplexers (OTM).

31. **[Required]** GR-2854-CORE, Generic Requirements for Fiber Optic Dispersion Compensators.

32. **[Required]** ANSI T-1.105-2001, Synchronous Optical Network (SONET) - Basic Description including Multiplex Structure, Rates, and Formats.

33. **[Required]** ANSI T-1.105.01-2000, Synchronous Optical Network (SONET) - Automatic Protection.

34. **[Required]** ANSI T-1.105.02-2001, Synchronous Optical Network (SONET) - Payload Mappings.

35. **[Required]** ANSI T-1.105.03-1994, Synchronous Optical Network (SONET) - Jitter at Network Interfaces.

36. **[Required]** ANSI T-1.105.03a-1995, Supplement ANSI T-1.105.03a-1995.

37. **[Required]** ANSI T-1.105.03b-1997, Supplement ANSI T-1.105.03b-1997.

5.5.3 DISN ODXC Requirements

The requirements in this section are specific to DISN Optical Digital Cross Connects.

5.5.3.1 ODXC SONET/SDH Interface Requirements

1. **[Required]** The systems shall support SDH or SONET on any combination of ports or port cards.

2. **[Required]** It shall be possible to use any port on the systems as network-side interfaces or a tributary-side interfaces.

3. **[Required]** The network-side interfaces shall include OC-768/STM-256, OC-192/STM-64, OC-48/STM-16, and OC-12/STM-4.

4. **[Required]** The tributary-side interfaces shall include OC-192/STM-64, OC-48/STM-16, and OC-12/STM-4, OC-3/STM-1.

5. **[Conditional]** ODXC interfaces shall support OUT-1, OUT-2 and OUT-3 optical signals.

6. **[Conditional]** The network-side interfaces shall include 10 Gbps DWDM.

7. **[Required]** The network element shall provide optical interfaces for OC-768, OC-192, OC-48, OC-12, OC-3 signals consistent with the SR-1, IR-1, IR-2, LR-1, LR-2, and LR-3 application specifications of Telcordia GR-253-CORE, Sec. 4.

8. **[Conditional]** The network element shall provide optical interfaces for OUT-1, OUT-2 and OUT-3 optical signals consistent with the application specifications of ITU-T G.709.

9. **[Required]** The network element shall provide optical interfaces for STM-256, STM-64, STM-16, STM-4, STM-1 signals consistent with the application codes I-n, S-n.x, and L-n.x in ITU-T Rec. G.957. There should be no differences between single-channel optical interfaces for SONET terminations according to Telcordia GR-253-CORE and the level-comparable SDH optical interfaces specified in Rec. G.957.

10. **[Required]** The network element shall support the SR-1 interface and at least one of IR-1, IR-2, or IR-3 interfaces for OC-3 (if supported), OC-12, OC-48, OC-192 and OC-768 signals consistent with the requirements in this document.

11. **[Required]** The network element shall support the Intraoffice (I-x) interface and any Short-haul (S-n.x) interface for STM-1 (if supported), STM-4, STM-16, STM-64 and STM-256 signals consistent with the requirements in this document.

12. **[Conditional]** The OC-192 SONET/STM-64 interfaces shall support Very Short Reach (VSR) optics as defined in ITU G.693.

5.5.3.2 ODXC Ethernet Interface Requirements

1. **[Required]** The system shall provide interfaces for Gigabit Ethernet Services in conformance with the IEEE 802.3 for Ethernet LAN interfaces. The Logical Link Interworking Function (IWF) shall terminate the Media Access Control (MAC) layer of Ethernet as described in the Ethernet Standard IEEE 802.3.

2. **[Conditional]** ODXC interfaces shall include 100 Gigabit Ethernet consistent with the application specifications of IEEE 803.

3. **[Required]** The system shall provide interfaces for 10 Gigabit Ethernet Services in conformance with the IEEE 802.3 for Ethernet LAN interfaces. The Logical Link Interworking Function (IWF) shall terminate the Media Access Control (MAC) layer of Ethernet as described in the Ethernet Standard IEEE 802.3.

4. **[Required]** The Gigabit Ethernet interfaces shall accommodate Ethernet packets greater than 4470 bytes.

5. **[Required]** The 10 Gigabit Ethernet interfaces shall accommodate Ethernet packets greater than 4470 bytes.

6. **[Required]** The system shall be able to provision, monitor, detect faults on, and restore Gigabit Ethernet services in a standardized and automated fashion.

7. **[Required]** The system shall be able to provision, monitor, detect faults on, and restore 10 Gigabit Ethernet services in a standardized and automated fashion.

8. **[Required]** The system's Ethernet services shall support Virtual LANs (VLAN) for multiple rates and customer interfaces as defined by IEEE Standard 802.1Q-1998, Virtual Bridged Local Area Networks.

9. **[Required]** The system shall not (by default) perform any Layer-3 routing.

10. **[Required]** The system shall support VLAN Tagging as specified by 802.1Q.

11. **[Required]** The system shall selectively provide point-to-point Ethernet services with dedicated non-shared bandwidth without queuing or buffering of Ethernet frames.

12. **[Required]** The system shall support ITU-T G.7041/Y.1303 (2003), Generic Framing Procedure (GFP).

13. **[Required]** The system shall support ITU-T G.7043/Y.1343 (2004), Virtual Concatenation of PDH Signals.

14. **[Required]** The system shall support ITU-T G.7042/Y.1305 (2004), Link Capacity Adjustment Scheme (LCAS) for Virtual Concatenated signals.

15. **[Required]** GE VCSA Interface ITU G.7042 [TBD].

5.5.3.3 ODXC Framing Requirements

1. **[Required]** The system shall conform to the standard SONET STS-1, STS-N, and STS-Nc frame structures per GR-253, Issue 3, September 2000.

2. **[Required]** The system shall conform to the standard SDH optical interfaces, rates and formats documented in ITU-T Recommendation G.707 for each of the following optical interfaces: STM-1, STM-4, STM-16, and STM-64.

3. **[Conditional]** The system shall conform to the standard OTU optical interfaces, rates and formats documented in ITU-T Recommendation G.709 for each of the following optical interfaces: OTU-1, OTU -2 and OTU -3.

4. **[Required]** All SONET overhead bytes are to be defined, generated, and processed according to the specifications of per GR-253, Issue 3, September 2000. All SDH overhead bytes are to be defined, generated, and processed according to the specifications of ITU-T Rec. G.707.

5. **[Conditional]** All OTU overhead bytes are to be defined, generated, and processed according to the specifications of per ITU-T Recommendation G.709.

6. **[Required]** If any SONET/SDH overhead bytes are used for proprietary purposes, it shall be possible to ignore these bytes at the receive side without affecting any transmission capability described in GR-253-CORE or in ITU-T Rec. G.783, respectively.

7. **[Required]** The capability to read/write the 16-byte frame and format of ITU-T Rec. G.707 and clause 3/G.831 shall be provided for both the Section Trace (J0) and the Path Trace (J1) bytes.

8. **[Required]** The capability to read/write the 64-byte frame and format of ITU-T Rec. G.707 and clause 3/G.831 shall be provided for both the Section Trace (J0) and the Path Trace (J1) bytes.

5.5.3.4 ODXC Switch Fabric Requirements

1. **[Required]** The SONET cross connects shall have an STS-1 granularity.

2. **[Required]** The SDH cross connects shall have a Virtual Circuit (VC)-VC-3 / VC-4 granularity.

3. **[Required]** The system shall not modify the user payload. Except for internetworking functions associated with optional Ethernet Services, the system shall not perform any user protocol conversions.

4. **[Required]** The system shall not impart any errors onto the connections during cross-connects, grooming, or multiplexing.

5. **[Required]** The system shall support virtual concatenation as defined in T-1.105-2001/G.707.

6. **[Required]** No single failure in the switch fabric shall impact service. The system shall meet GR-2996 requirements for fabric availability.

7. **[Required]** The interface cards shall be capable of switching between the working and protection switch fabric in an errorless manner for manual operation, and in a hitless manner for automated operation. No bits shall be lost or corrupted with errorless switching. Bit errors are allowed with hitless switching. However, hitless switching shall not cause downstream reframing to occur.

5.5.3.5 ODXC Performance Requirements

1. **[Required]** The Switch shall meet the jitter criteria for SONET systems in GR-253, Issue 3, September 2000, Section 5.6.

2. **[Required]** The Switch shall meet the jitter criteria for SDH systems according to ITU G.825.

3. **[Required]** The Switch shall meet the interface jitter criteria specified for UNI interfaces for ITU-T Optical Transport Networks.

4. **[Required]** The jitter tolerance measured at the OC-N interface on the Switch shall meet input jitter tolerance specification documented in ANSI T-1.105.03-1994.

5. **[Required]** The jitter generation measured at a OC-N interface on the Switch shall be less than 0.01 Unit Interval (UI) Root Mean Square (RMS) when measured using a high-pass filter with 12-kiloHertz (kHz) cutoff frequency as defined in T-1.105.03-1994, section A.3.3.

6. **[Required]** The maximum delay for a full Synchronous Transport Signal (STS) passed through the Switch or for an STS add/drop from the Switch shall not exceed the values defined in GR-2996, Issue 1, January 1999, section 6.2.

7. **[Conditional]** The Switch shall perform Hair-pinning, Drop, Continue, and Drop-and-Continue Add-Drop Multiplexing (ADM) functions as specified in GR-496, Issue 1, December 1998.

8. **[Conditional]** The Switch shall provide the ability to hub or nest lower Switches in a linear or ring configuration from line-side interfaces.

5.5.3.6 General Link Protection Requirements

1. **[Required]** It shall be possible to provision any SONET port for 1+1 Automatic Protection Switching (APS), 0:1 APS, 1:N APS; 1:N Optical Protection (OP), 2-Fiber Unidirectional Path Switched Ring (UPSR) per Telcordia GR-1400-CORE, or 2/4-Fiber Bidirectional Line Switched Ring (BLSR) per Telcordia GR-1230-CORE.

2. **[Required]** It shall be possible to provision any SDH port for 1+1 APS, 0:1 APS, 1:N APS, 1+1 2/4-Fiber Unidirectional Ring, or 2-Fiber MS Shared Protection Ring per ITU-T Rec. G.841
.
3. **[Required]** When the system participates in point-to-point UPSR or BLSR protection, switching shall take place in 50 milliseconds (ms). These protection mechanisms shall be definable and selectable from the EMS, and shall offer the selection of revertive and non-revertive restoration mechanisms.

4. **[Required]** The service restoration for a protection switch shall be automatic and accomplished without human or central management system intervention.

5. **[Required]** The protection switching mechanism shall be independent among separately-managed network domains. A protection switch in one separately-managed network domain shall not propagate or relay to another separately-managed network domain.

6. **[Required]** The maximum detection time to determine if a signal's BER threshold is exceeded shall comply with GR-253, Issue 3, September 2000 and ITU-T Rec G.783.

7. **[Required]** Once a decision is made to switch, the terminal circuit pack switching shall take place within 50 ms, as described in GR-253, Issue 3, September 2000 and ITU-T Rec G.783.

8. **[Required]** Catastrophic failures on a user-definable Excessive BER (EBER) condition shall be detected by an equipment-protected circuit pack in a terminal within 10 ms as described in GR-253, Issue 3, September 2000 and ITU-T Rec G.783.

9. **[Required]** When equipped, each network element shall be compliant with Types and Characteristics of SDH Network Protection Architectures as defined in ITU-T G.841.

10. **[Required]** When equipped, each network element shall be compliant with Inter-working of SDH Network Protection Architectures as defined in ITU-T G.842.

5.5.3.7 Linear Protection Requirements

1. **[Required]** The linear switching protection mechanisms of the system shall be selectable as either revertive or non-revertive during network operation.

2. **[Required]** The SONET linear protection mechanisms of the system, including APS functions, shall conform to GR-253, Issue 3, September 2000. No proprietary APS byte definition and no proprietary linear APS protocol is allowed.

3. **[Required]** The system shall support 1+1 APS optical interface protection, Unidirectional and Bidirectional, and Revertive and Non-revertive, as per ITU G.841.

4. **[Required]** The SDH linear protection mechanisms of the system, including APS functions, shall conform to ITU-T G.841. No proprietary APS byte definition or proprietary linear APS protocol is allowed.

5. **[Required]** When the high-speed interface of a system is configured for a linear protection system, it shall support linear protection switching with adjacent equipment. The system shall support both 1+1 and 1:1 protection switching across the network as per section 5.3.2 of Telcordia GR-253 and ITU-T G.841.

6. **[Required]** When a system is configured as a 1:1 linear protection system, it shall support both unidirectional and bidirectional protection switching capabilities, as described in Telcordia GR-253 and ITU-T G.841.

7. **[Required]** The maximum length of protection switching time due to a fiber cut, signal failure, user definable EBER, or an equipment circuit pack failure in a network shall not exceed 60 ms per transmission direction, which includes 10 ms BER detection time as described in Telcordia GR-253 and ITU-T G.841.

8. **[Required]** When a system is configured as a 1:1 linear protection system, its default protection switching mode shall be revertive, i.e., the signal shall be automatically reverted to the working fibers after the fibers are repaired and the Wait To Restore (WTR) time is expired, as described in Telcordia GR-253. A 1:1 linear system shall also be optionally configurable as non-revertive.

9. **[Required]** The linear protection configuration of the system shall:
   - Have a switch completion time in both directions of not more than 50 ms.
   - Provide the Signal Fail (SF), Signal Degrade (SD), and APS initiation criteria.
   - Support the WTR feature to prevent frequent oscillations between the working and the protection lines resulting from intermittent failures as described in Telcordia GR-253.
   - Provide a minimum WTR time of 5 minutes.
   - Provide a maximum WTR time of 12 minutes as described in Telcordia GR-253

5.5.3.8 Ring Protection Requirements

1. **[Required]** When equipped, each network element shall be compliant with GR-1230-CORE, SONET Bi-directional Line-Switched Ring (BLSR) Equipment Generic Criteria.

2. **[Required]** When equipped, each network element shall be compliant with GR-1400-CORE, SONET dual-fed Uni-directional Patch Switch Ring (UPSR) Equipment Criteria.

3. **[Required]** The system shall support Multiplex Section (MS)-Shared Protection Ring (SPRING) according to ITU G.841.

4. **[Required]** The system shall support Subnetwork Connection Protection (SNCP) ring protection according to ITU G.841.

5. **[Required]** The system shall provide the option to use UPSR, two-fiber BLSR, or four-fiber BLSR as a ring protection mechanism. When the high-speed interface at a system is configured for any of these protection schemes, it shall support protection switching with other systems in the ring. The maximum length of protection switching time due to a fiber cut, signal failure, user definable EBER, or an equipment circuit pack failure in a network shall not exceed 60 ms per transmission direction, which includes 10 ms BER detection time as described in GR-1230-CORE and GR-1400-CORE.

6. **[Required]** When the system is in a SONET/SDH BLSR configuration, its automatic protection switching (APS) functions shall conform to Telcordia GR-253 and ITU-T Recommendation G.841. No proprietary APS byte definition and no proprietary ring APS protocol is allowed.

7. **[Required]** The ring protection configurations of the system shall:

   - Use standard SONET/SDH ring APS protocols to coordinate the protection switching, as documented in Telcordia GR-253 and ITU-T G.841.

   - Complete the protection switch within 50 ms when there is no extra traffic and no previous bridge requests on the ring, and the length of a ring is less than 1200 km of fiber, as described in Telcordia GR-253.

   - Support a ring size up to at least 16 nodes, as described in Telcordia GR-253.

   - Not exceed a 50 ms length of hits to service when the following ring configuration functions are performed: Ring Node Addition, Ring Node Deletion, and Ring Segmentation, as described in Telcordia GR-253. (When the system is configured as a

BLSR system, the protection switch completion time can exceed 50 ms when there is extra traffic or previous bridge requests on the ring, as described in Telcordia GR-253).

5.5.3.9 Fault Management Requirements

1. **[Required]** The equipment shall send the appropriate Alarm Indication Signal (AIS) and Remote Defect Indication (RDI) to adjacent systems, the EMS, and/or the higher-level management system after detecting signal failure or degraded conditions for a specified alarm or indication activation time, as described in T-1.231, Tables 2, 6, and 11.

2. **[Required]** The equipment shall remove the appropriate AIS and RDI after the source system has cleared the signal failure or degraded condition for a specified alarm or indication activation time, as described in T-1.231, Tables 2, 6, and 11.

3. **[Required]** Alarms shall indicate circuit-level or signal alarms, as well as alarms in the network element itself, such as Span Failure, LOS, Path Switch Complete/Fail, Laser Degradation, Card Failure, and Card Mismatch.

4. **[Required]** Standard SONET alarms shall be supported by the system, including Loss Of Signal (LOS), Loss Of Pointer (LOP), Loss Of Frame (LOF), Receive AIS (Rx AIS), Remote Defect Indication (RDI), and Remote Failure Indication (RFI).

5. **[Required]** The system shall indicate SONET timing synchronization failures. The network element shall give an alarm showing the inability to establish a Phase Locked Loop (PLL). The network element shall have the ability to monitor the Building Integrated Timing Supply (BITS) incoming references (BITS-A and BITS-B). The system shall give an alarm when there is any timing change, e.g., a switch from BITS-A to BITS-B.

6. **[Required]** Each NE shall detect, report, and clear the following signal failure events or conditions: LOS, LOF, LOP, Severely Errored Framing (SEF), AIS, and OOF (Out Of Frame), according to ANSI T-1.231-1993.

5.5.3.10 Performance Management Requirements

1. **[Required]** The system shall calculate the Performance Monitoring (PM) parameter values for each SONET/SDH layer from block errors, rather than bit errors, per ITU Recommendation G.826.

2. **[Required]** The system shall gather PM data based on overhead bits, such as Bit Interleaved Parity-Number (BIP-N), at the Section, Line, and Path layers, or on Ethernet frame overhead, as appropriate.

3. **[Required]** The system shall track performance monitoring data for appropriate service(s), e.g., SONET errors, Far-End Block Errors (FEBE), pointer adjustments; Ethernet statistics. All statistics shall be tracked in five-minute intervals, with the ability reduce intervals for testing and analysis.

4. **[Conditional]** The system shall employ tools such as Optical Spectrum Analyzers (OSA) and optical monitoring tools to verify optical power levels and detect unauthorized signals and other anomalous events on its interfaces.

5. **[Required]** The NE shall support status and configuration reporting between nodes in Multi-Ring (Mixed UPSR, BLSR, and 1+1 APS), Linear ADM, Mesh, Regenerator, and Star/Hub node configurations. The NEs shall support near-end and far-end reporting.

6. **[Conditional]** The NE shall support reporting of Resilient Packet Ring (RPR) QoS/CoS parameters.

7. **[Required]** The NE shall support reporting of trunk and port quality with user-configurable thresholds.

8. **[Required]** The NE shall support reporting of Ethernet Frames Dropped.

9. **[Required]** The system shall be able to track near-end and far-end statistics in both receive and transmit directions. The network element shall be able to track all the performance metrics defined in ITU-T Recommendation M.2101.

10. **[Required]** The system shall monitor each optical interface in accordance with ANSI T-1.231-1993. Performance monitoring parameters shall include: Severely Errored Framing Seconds (SEFS), Code Violation (CV), Errored Seconds (ES), Severely Errored Seconds (SES), Unavailable Seconds (UAS), Protection Switching Counts, and Pointer Justification.

11. **[Required]** For SONET traffic, the system shall be able to track section, line, and path errors. Further, it shall track the respective FEBEs.

12. **[Conditional]** The system shall support intermediate Path Monitoring.

5.5.3.11 EMS Requirements

1. **[Required]** The Switch EMS shall report physical layer (layer 1) statistics. Further, it shall report layer 2 errors. It shall report all quality of service (QoS) parameters defined for the Resilient Packet Ring (RPR) as described in IEEE 802.17.

2. **[Required]** The Switch EMS shall be able to track frame errors, P-Bit Parity Errors, C-Bit Parity Errors, and Far-End Block Errors (FEBE).

5.5.3.12 Standards Compliance Requirements

The Switch shall comply with the most recent published version of the following standards:

1. **[Required]** Telcordia GR-253 Synchronous Optical Network (SONET) Transport, Issue 3, September 2000.

2. **[Required]** Telcordia GR-2996 Generic Criteria for SONET Digital Cross-Connect Systems, Issue 1, January 1999.

3. **[Required]** ITU-T G.783 Switching and Cross Connects, Characteristics of Synchronous Digital Hierarchy (SDH) Equipment Functional Block.

4. **[Required]** ITU-T G.691 Optical Interfaces for Single-Channel STM-64 systems.

5. **[Required]** ITU-T G.691 Optical Interfaces for Single-Channel STM-256 systems.

6. **[Required]** ITU-T G.957 Optical interfaces for equipment and systems relating to the Synchronous Digital Hierarchy.

7. **[Required]** ITU-T G.707 network interface for Synchronous Digital Hierarchy.

8. **[Required]** ITU-T G.841, Types and Characteristics of SDH Network Protection Architectures.

9. **[Required]** ITU-T G.842, Inter-working of SDH Network Protection Architectures.

10. **[Required]** ITU Recommendation G.872 (1999), Architecture of Optical Transport Networks.

11. **[Required]** Telcordia GR-499-CORE Transport Systems Generic Requirements: Common Requirements, Issue 2, December 1998.

12. **[Required]** Telcordia GR-1244 Clocks for the Synchronized Network: Common Generic Criteria, Issue 2, December 2000.

13. **[Required]** Telcordia GR-1230-CORE SONET Bi-Directional Line-Switched Ring Equipment Generic Criteria, Issue 4, December 1998.

14. **[Required]** Telcordia GR-1400-CORE SONET Dual-Fed Unidirectional Path Switched Ring (UPSR) Equipment Generic Criteria, Issue 2, December 1999.

5.5.4 DISN Access Requirements

The requirements in this section are specific to DISN Access systems.

5.5.4.1 MSPP, M13, Sub-T-1 Mux Requirements

TBD

5.5.4.2 SONET Interface Requirements

(TBD, revisit this section, is anything less than OC-192 needed/used in the DISN/Core?)

1. **[Required]** All SONET OC-N interfaces shall be software-provisionable to SDH STM-N.

2. **[Required]** The OC-3 Optical Interface shall conform to the standard SONET rates and formats documented in ANSI T-1.105.

3. **[Required]** The OC-3 Optical Interface shall conform to Optical Parameters for Application Category Short Reach (SR)-1 per GR-253 sections 4.1 and 4.2, and Tables 4-1 through 4-11.

4. **[Required]** The OC-3 Optical Interface shall conform to Optical Parameters for Application Category Intermediate Reach (IR)-1 per GR-253 sections 4.1 and 4.2, and Tables 4-1 through 4-11.

5. **[Required]** The OC-3 Optical Interface shall conform to Optical Parameters for Application Category IR-2 per GR-253 sections 4.1 and 4.2, and Tables 4-1 through 4-11.

6. **[Required]** The OC-3 Optical Interface shall conform to Optical Parameters for Application Category Long Reach (LR)-1 per GR-253 sections 4.1 and 4.2, and Tables 4-1 through 4-11.

7. **[Required]** The OC-3 Optical Interface shall conform to Optical Parameters for Application Category LR-2 per GR-253 sections 4.1 and 4.2, and Tables 4-1 through 4-11.

8. **[Required]** The OC-3 Optical Interface shall conform to Optical Parameters for Application Category LR-3 per GR-253 sections 4.1 and 4.2, and Tables 4-1 through 4-11.

9. **[Required]** The OC-3 interfaces shall be capable of having a Multi Mode Fiber (MMF) interface option for both transmit and receive using MMF as described in ITU G.651 and ANSI 105.06.2002.

10. **[Required]** The OC-3 interfaces shall be capable of using Single Mode Fiber (SMF) as described in ITU G.652 and ANSI 105.06.2002.

11. **[Required]** The OC-12 Optical Interface shall conform to the standard SONET rates and formats documented in ANSI T-1.105.

12. **[Required]** The OC-12 Optical Interface shall conform to Optical Parameters for Application Category SR-1 per GR-253 sections 4.1 and 4.2, and Tables 4-1 through 4-11.

13. **[Required]** The OC-12 Optical Interface shall conform to Optical Parameters for Application Category IR-1 per GR-253 sections 4.1 and 4.2, and Tables 4-1 through 4-11.

14. **[Required]** The OC-12 Optical Interface shall conform to Optical Parameters for Application Category IR-2 per GR-253 sections 4.1 and 4.2, and Tables 4-1 through 4-11.

15. **[Required]** The OC-12 Optical Interface shall conform to Optical Parameters for Application Category LR-1 per GR-253 sections 4.1 and 4.2, and Tables 4-1 through 4-11.

16. **[Required]** The OC-12 Optical Interface shall conform to Optical Parameters for Application Category LR-2 per GR-253 sections 4.1 and 4.2, and Tables 4-1 through 4-11.

17. **[Required]** The OC-12 Optical Interface shall conform to Optical Parameters for Application Category LR-3 per GR-253 sections 4.1 and 4.2, and Tables 4-1 through 4-11.

18. **[Required]** The OC-12 interfaces shall be capable of having an MMF interface option for both transmit and receive using MMF as described in ITU G.651 and ANSI 105.06.2002.

19. **[Required]** The OC-12 interfaces shall be capable of using SMF as described in ITU G.652 and ANSI 105.06.2002.

20. **[Required]** The OC-48 Optical Interface shall conform to the standard SONET rates and formats documented in ANSI T-1.105.

21. **[Required]** The OC-48 Optical Interface shall conform to Optical Parameters for Application Category SR-1 per GR-253 sections 4.1 and 4.2, and Tables 4-1 through 4-11.

22. **[Required]** The OC-48 Optical Interface shall conform to Optical Parameters for Application Category IR-1 per GR-253 sections 4.1 and 4.2, and Tables 4-1 through 4-11.

23. **[Required]** The OC-48 Optical Interface shall conform to Optical Parameters for Application Category IR-2 per GR-253 sections 4.1 and 4.2, and Tables 4-1 through 4-11

24. **[Required]** The OC-48 Optical Interface shall conform to Optical Parameters for Application Category LR-1 per GR-253 sections 4.1 and 4.2, and Tables 4-1 through 4-11.

25. **[Required]** The OC-48 Optical Interface shall conform to Optical Parameters for Application Category LR-2 per GR-253 sections 4.1 and 4.2, and Tables 4-1 through 4-11.

26. **[Required]** The OC-48 Optical Interface shall conform to Optical Parameters for Application Category LR-3 per GR-253 sections 4.1 and 4.2, and Tables 4-1 through 4-11.

27. **[Required]** The OC-192 Optical Interface shall conform to the standard SONET rates and formats documented in ANSI T-1.105.

28. **[Required]** The OC-192 Optical Interface shall conform to Optical Parameters for Application Category SR-1 per GR-253 sections 4.1 and 4.2, and Tables 4-1 through 4-11.

29. **[Required]** The OC-192 Optical Interface shall conform to Optical Parameters for Application Category IR-1 per GR-253 sections 4.1 and 4.2, and Tables 4-1 through 4-11.

30. **[Required]** The OC-192 Optical Interface shall conform to Optical Parameters for Application Category IR-2 per GR-253 sections 4.1 and 4.2, and Tables 4-1 through 4-11.

31. **[Required]** The OC-192 Optical Interface shall conform to Optical Parameters for Application Category LR-1 per GR-253 sections 4.1 and 4.2, and Tables 4-1 through 4-11.

32. **[Required]** The OC-192 Optical Interface shall conform to Optical Parameters for Application Category LR-2 per GR-253 sections 4.1 and 4.2, and Tables 4-1 through 4-11.

33. **[Required]** The OC-192 Optical Interface shall conform to Optical Parameters for Application Category LR-3 per GR-253 sections 4.1 and 4.2, and Tables 4-1 through 4-11.

5.5.4.3 SDH Interface Requirements

1. **[Required]** The STM-1 Optical Interface shall conform to Optical Parameters for Application Code I-1 per G.957 Table 2.

2. **[Required]** The STM-1 Optical Interface shall conform to Optical Parameters for Application Code S-1.1 per G.957 Table 2.

3. **[Required]** The STM-1 Optical Interface shall conform to Optical Parameters for Application Code S-1.2 per G.957 Table 2.

4. **[Required]** The STM-1 Optical Interface shall conform to Optical Parameters for Application Code L-1.1 per G.957 Table 2.

5. **[Required]** The STM-1 Optical Interface shall conform to Optical Parameters for Application Code L-1.2 per G.957 Table 2.

6. **[Required]** The STM-1 Optical Interface shall conform to Optical Parameters for Application Code L-1.3 per G.957 Table 2.

7. **[Required]** The STM-1 interfaces shall be capable of having an MMF interface option for both transmit and receive using MMF as described in ITU G.651.

8. **[Required]** The STM-1 interfaces shall be capable of using SMF as described in ITU G.652.

9. **[Required]** The STM-4 Optical Interface shall conform to Optical Parameters for Application Code I-4 per G.957 Table 3.

10. **[Required]** The STM-4 Optical Interface shall conform to Optical Parameters for Application Code S-4.1 per G.957 Table 3.

11. **[Required]** The STM-4 Optical Interface shall conform to Optical Parameters for Application Code S-4.2 per G.957 Table 3.

12. **[Required]** The STM-4 Optical Interface shall conform to Optical Parameters for Application Code L-4.1 per G.957 Table 3.

13. **[Required]** The STM-4 Optical Interface shall conform to Optical Parameters for Application Code L-4.2 per G.957 Table 3.

14. **[Required]** The STM-4 Optical Interface shall conform to Optical Parameters for Application Code L-4.3 per G.957 Table 3.

15. **[Required]** The STM-4 interfaces shall be capable of having an MMF interface option for both transmit and receive using MMF as described in ITU G.651.

16. **[Required]** The STM-4 interfaces shall be capable of using SMF as described in ITU G.652.

17. **[Required]** The STM-16 Optical Interface shall conform to Optical Parameters for Application Code I-16 per G.957 Table 4.

18. **[Required]** The STM-16 Optical Interface shall conform to Optical Parameters for Application Code S-16.1 per G.957 Table 4.

19. **[Required]** The STM-16 Optical Interface shall conform to Optical Parameters for Application Code S-16.2 per G.957 Table 4.

20. **[Required]** The STM-16 Optical Interface shall conform to Optical Parameters for Application Code L-16.1 per G.957 Table 4.

21. **[Required]** The STM-16 Optical Interface shall conform to Optical Parameters for Application Code L-16.2 per G.957 Table 4.

22. **[Required]** The STM-16 Optical Interface shall conform to Optical Parameters for Application Code L-16.3 per G.957 Table 4.

23. **[Required]** The STM-64 Optical interface shall conform to ITU-T G.691 Optical Interfaces for Single-Channel STM-64, STM-256 systems.

5.5.4.4. Lambda Interface Requirements

1. **[Conditional]** The network element shall have Lambda interfaces at the 10 Gigabit rates. These shall be compatible with the DISN Transport section.

2. **[Required]** Lambda Interfaces shall be compliant with the ITU G.694.1 grid.

5.5.4.5 Electrical Interface Requirements

1. **[Conditional]** The network element shall support STS-1 (EC-1) electrical interfaces that comply with specifications and pulse masks as defined in Telcordia GR-253 Chapter 4.4 and ANSI T-1.102-1993.

2. **[Required]** The network element shall support DS-1 electrical interfaces that comply with ANSI T-1.102.

3. **[Required]** The network element shall support channelized and unchannelized DS-1 Superframe (SF) format and Extended Superframe (ESF) format as specified in ANSI T.403. The ability to read/write the ESF data link is required. The selection of format for any particular DS-1 interface shall be user-selectable.

4. **[Required]** The network element shall support unframed DS-1 electrical signals.

5. **[Required]** The network element shall support E-1 electrical interfaces shall comply with ITU-T G.711.

6. **[Required]** The network element shall support the both channelized and unchannelized E-1 as specified in ITU-T G.711.

7. **[Required]** The network element shall support DS-3 electrical tributary interfaces that comply with ANSI T-1.102-1993. The selection of format for any particular E-1 interface shall be user-selectable.

8. **[Required]** The network element shall support channelized and unchannelized DS-3 signals in either M13 or C-bit parity formats per ANSI T-1.107and T-1.404. The selection of format for any particular DS-3 interface shall be user-selectable.

5.5.4.6 Ethernet Interface Requirements

1. **[Required]** The network element shall provide interfaces for Ethernet, Fast Ethernet, and Gigabit Ethernet Services in conformance with IEEE 802.3 for Ethernet LAN interfaces.

2. **[Required]** The Logical Link Interworking Function (IWF) shall terminate the Media Access Control (MAC) layer of Ethernet as described in Ethernet Standard IEE 802.3.

3. **[Required]** Ethernet interfaces shall accommodate Ethernet packets greater than 4470 bytes.

4. **[Required]** Ethernet services shall support VLANS for multiple rates and customer interfaces as per IEEE 802.1Q.

5. **[Required]** The network element shall support transparent VLAN tagging for Ethernet on SONET/SDH service.

6. **[Required]** The network element shall not perform any Layer-3 IP routing.

7. **[Required]** The network element shall be able to provision, monitor, detect faults, and restore Ethernet services in a standardized and automated fashion.

8. **[Required]** The network element shall selectively provide QoS/CoS for Ethernet Services according to IEEE 802.1Q.

9. **[Conditional]** Available Ethernet Services shall include Resilient Packet Ring (IEEE 802.17b), Generic Framing Procedure (ITU-T G.7041/Y.1303), Link Capacity Adjustment Scheme (LCAS), and Virtual Concatenation (VCAT).

10. **[Required]** The network element shall selectively provide point-to-point Ethernet services with dedicated non-shared bandwidth without queuing or buffering Ethernet frames.

11. **[Required]** Gigabit Ethernet and 10 Gigabit Ethernet interfaces shall be auto-sensing/auto-detecting and auto configuring between incoming Gigabit Ethernet and 10 Gigabit Ethernet signals.

12. **[Required]** Ethernet and Fast Ethernet interfaces shall be auto-sensing/auto-detecting and auto configuring between incoming Ethernet and Fast Ethernet signals.

13. **[Conditional]** The network element shall have the ability to support 10 Gigabit Ethernet interfaces.

5.5.4.7 SAN Interface Requirements

1. **[Conditional]** The network element shall provide Fiber Connectivity (FICON) tributary interfaces and services as per ANSI X3.230.

2. **[Conditional]** The network element shall provide Enterprise Services Connectivity (ESCON) tributary interfaces and services as per ANSI X3.296.

5.5.4.8 Cross Connect Requirements

1. **[Required]** The network element shall cross connect with the granularity of STS-1 and VT 1.5.

2. **[Required]** The network element shall cross connect with the granularity of E-1 (not necessarily simultaneously with STS-1 and VT 1.5).

3. **[Required]** The network element shall perform Time Slot Interchange (TSI) and Time Slot Assignment (TSA) cross-connect between DS-1 interfaces, DS-3 interfaces and onto SONET VT 1.5 formatted STS containers.

4. **[Required]** The network element shall support structured AU-4 mapping for SDH applications using the ITU multiplexing structure in G.707.

5. **[Required]** The network element shall be able to map T-1, E-1, T-3, and E-3 signals into an AU-4 mapping structure as per ITU G.707.

6. **[Required]** The network element shall support VC-11, VC-12, VC-3, and VC-4 cross connect capability for SDH AU-4 based system.

7. **[Required]** The network element shall support SDH/SONET container gateway functionalities (i.e., VC-3 to STS-1 and VC-11 to VT-1.5).

8. **[Required]** The network element shall have the ability to retime signals from either VT-1.5 or DS-1 formats, as well as pass timing through the matrix directly to provide timing up to Stratum 1 via DS-1 ports.

9. **[Required]** The network element cross connects and interfaces shall be compatible with network side STS or Lambda cross connects at the DISN Switch or the DISN Transport Element.

10. **[Required]** The network element cross connects and interfaces at the network element shall be transparent to all protection switching at the DISN Switch or the DISN Transport Element.

5.5.4.9 Performance Requirements

1. **[Required]** The DISN Access element shall meet the jitter criteria for SONET systems in GR-253, Section 5.6.

2. **[Required]** The DISN Access element shall meet the jitter criteria for SDH systems according to ITU G.825 and ITU-T G.732.

3. **[Required]** The DISN Access element shall meet the interface jitter criteria specified for UNI interfaces for ITU-T Optical Transport Networks.

4. **[Required]** The jitter tolerance measured at the OC-N interface on a DISN Access element shall meet Figure A.1 input jitter tolerance specification documented in ANSI T-1.105.03-1994.

5. **[Required]** The jitter tolerance measured at the Digital Signal (DS)-3 interface on a DISN Access element shall be at least 5 Unit Interval peak-to-peak (UIpp) between 10 Hertz (Hz) and 2.3×10^{3} Hz, and at least 0.1 UIpp between 60×10^{3} and 200×10^{3} Hz as per Fig. 7-1 in TR- 499.

6. **[Required]** The jitter transfer measured between an input DS-3 interface and the corresponding output DS-3 interface on a DISN Access element (with its OC-12 or OC-3 signal looped-back) shall be less than the jitter transfer mask shown in Figure 7-4 of TR-499. (TBD is anything less than OC-192 used in the core?)

7. **[Required]** The jitter generation measured at the OC-N interface on a DISN Access element shall be less than 0.01 Unit Interval root mean square (UIrms) when measured using a high-pass filter with 12-kHz cutoff frequency as per ANSI T-1.105.03, Section A.3.3.

8. **[Required]** The jitter generation due to DS-3/STS-1 payload mapping for the DS-3 interface on a DISN Access element shall be less than 0.4 UIpp, without pointer adjustments as per ANSI T-1.105.03, Sec. 6.1.2.1.

9. **[Required]** The jitter generation due to DS-3/STS-1 payload mapping for the DS-3 interface on a DISN Access element shall be less than A1 = A0 + .3 UIpp for a single pointer adjustment as shown in Table 2 of ANSI T-1.105.03-1994.

10. **[Required]** The jitter generation due to DS-3/STS-1 payload mapping for the DS-3 interface on a DISN Access element shall be less than 1.3 UIpp for pointer adjustment bursts as shown in Table 3 of ANSI T-1.105.03-1994.

11. **[Required]** The jitter generation due to DS-3/STS-1 payload mapping for the DS-3 interface on a DISN Access element shall be less than 1.2 UIpp for phase transient pointer adjustment bursts as shown in Table 4 of ANSI T-1.105.03-1994.

12. **[Required]** The jitter generation due to DS-3/STS-1 payload mapping for the DS-3 interface on a DISN Access element shall be less than 1.3 UIpp for periodic pointer adjustments as shown in Table 6 of ANSI T-1.105.03-1994.

13. **[Required]** The jitter generation due to DS-3/STS-1 payload mapping for the DS-3 interface on a DISN Access element shall be less than 5 UIpp between 10 Hz and 500 Hz, and at least 0.1 UIpp between 8x10 3 and 40x10 3 Hz as per Figure 7-1 of TR-499.

14. **[Required]** The jitter transfer measured between an input DS-1 interface and the corresponding output DS-1 interface on a DISN Access element (with its OC-12 or OC-3 signal looped-back) shall be less than the jitter transfer mask shown in Figure 7-4 of TR-499. (TBD is anything less than OC-192 used in the core?)

15. **[Required]** The jitter generation due to DS-1/Virtual Tributary (VT)-1.5 payload mapping without pointer adjustments for the DS-1 interface on a DISN Access element shall be less than 0.7 UIpp as per ANSI T-1.105.03s, Section 6.1.1.1.

16. **[Required]** The jitter generation due to DS-1/VT-1.5 payload mapping and a single pointer adjustment for the DS-1 interface on a DISN Access element shall meet the single VT pointer adjustment Maximum Time Interval Error (MTIE) mask shown on Figure 8 of ANSI T-1X1.3/94-001R5, supplement to ANSI T-1.105.03-1994.

17. **[Required]** The jitter generation due to DS-1/VT-1.5 payload mapping and periodic pointer adjustments for the DS-1 interface on a DISN Access element shall meet the periodic VT pointer adjustment MTIE mask shown on Figure 10 of ANSI T-1X1.3/94-001R5, supplement to ANSI T-1.105.03-1994.

18. **[Required]** The maximum delay for a full STS passed through a DISN Access element (OC-N to OC-N), or for an STS add/drop shall not exceed 25 microseconds as perTR-496, (R) [3-45].

19. **[Required]** The maximum delay for a floating VT passed through an DISN Access element (OC-N to OC-N), or for a floating VT add/drop (OC-N to Low-Speed or Low-Speed to OC-N) shall not exceed 50 microseconds as per TR-496, (R) [3-46].

5.5.4.10 Equipment Redundancy Requirements

1. **[Required]** No single failure in the switch fabric shall impact service. The system shall meet GR-2996 requirements for fabric availability.

2. **[Required]** The interface cards shall be capable of switching between the working and protection switch fabric in an errorless manner for manual operation, and in a hitless manner for automated operation. No bits shall be lost or corrupted with errorless switching. Bit errors are allowed with hitless switching. However, hitless switching shall not cause downstream reframing to occur.

5.5.4.11 General Protection Requirements

1. **[Required]** It shall be possible to provision any SONET port for 1+1 Automatic Protection Switching (APS), 0:1 APS, 1:N APS; 1:N Optical Protection (OP), 2-Fiber Unidirectional Path Switched Ring (UPSR) per Telcordia GR-1400-CORE, or 2/4-Fiber Bidirectional Line Switched Ring (BLSR) per Telcordia GR-1230-CORE.

2. **[Required]** It shall be possible to provision any SDH port for 1+1 APS, 0:1 APS, 1:N APS, 1+1 2/4-Fiber Unidirectional Ring, or 2-Fiber MS Shared Protection Ring per ITU-T Rec. G.841.

3. **[Required]** When the system participates in point-to-point UPSR or BLSR protection, switching shall take place in 50 milliseconds (ms). These protection mechanisms shall be definable and selectable from the EMS, and shall offer the selection of revertive and non-revertive restoration mechanisms.

4. **[Required]** The service restoration for a protection switch shall be automatic and accomplished without human or central management system intervention.

5. **[Required]** The protection switching mechanism shall be independent among separately managed network domains. A protection switch in one separately managed network domain shall not propagate or relay to another separately-managed network domain.

6. **[Required]** The maximum detection time to determine if a signal's BER threshold is exceeded shall comply with GR-253, Issue 3, September 2000 and ITU-T Rec G.783.

7. **[Critical]** Once a decision is made to switch, the terminal circuit pack switching shall take place within 50 ms, as described in GR-253, Issue 3, September 2000 and ITU-T Rec G.783.

8. **[Required]** Catastrophic failures on a user-definable Excessive BER (EBER) condition shall be detected by an equipment-protected circuit pack in a terminal within 10 ms as described in GR-253, Issue 3, September 2000 and ITU-T Rec G.783.

9. **[Required]** When equipped, each network element shall be compliant with Types and Characteristics of SDH Network Protection Architectures as defined in ITU-T G.841.

10. **[Required]** When equipped, each network element shall be compliant with Inter-working of SDH Network Protection Architectures as defined in ITU-T G.842.

5.5.4.12 Interoperability Requirements

1. **[Required]** The DISN Access element user interfaces, software, firmware, and hardware shall be fully compatible and interoperable with protection mechanisms of the DISN Transport system, DISN Switch, and DISN Router.

2. **[Required]** DISN Access element cross-connects and interfaces shall be compatible with network-side STS or Lambda cross-connects at the DISN Switch.

3. **[Required]** Cross-connects and interfaces at the DISN Access element shall be compatible with all protection switching at the DISN Transport system, DISN Switch, and DISN Router.

5.5.4.13 Fault Management Requirements

1. **[Required]** The equipment shall send the appropriate Alarm Indication Signal (AIS) and Remote Defect Indication (RDI) to adjacent systems, the EMS, and/or the higher-level management system after detecting signal failure or degraded conditions for a specified alarm or indication activation time, as described in T-1.231, Tables 2, 6, and 11.

2. **[Required]** The equipment shall remove the appropriate AIS and RDI after the source system has cleared the signal failure or degraded condition for a specified alarm or indication activation time, as described in T-1.231, Tables 2, 6, and 11.

3. **[Required]** Alarms shall indicate circuit-level or signal alarms, as well as alarms in the network element itself, such as Span Failure, LOS, Path Switch Complete/Fail, Laser Degradation, Card Failure, and Card Mismatch.

4. **[Required]** Standard SONET alarms shall be supported by the system, including Loss Of Signal (LOS), Loss Of Pointer (LOP), Loss Of Frame (LOF), Receive AIS (Rx AIS), Remote Defect Indication (RDI), and Remote Failure Indication (RFI).

5. **[Required]** The system shall indicate SONET timing synchronization failures. The network element shall give an alarm showing the inability to establish a Phase Locked Loop (PLL). The network element shall have the ability to monitor the Building Integrated Timing Supply (BITS) incoming references (BITS-A and BITS-B). The system shall give an alarm when there is any timing change, e.g., a switch from BITS-A to BITS-B.

6. **[Required]** Each NE shall detect, report, and clear the following signal failure events or conditions: LOS, LOF, LOP, Severely Errored Framing (SEF), AIS, and OOF (Out Of Frame), according to ANSI T-1.231-1993.

7. **[Required]** The network element shall provide the following DS-3 alarms: LOS and AIS (or blue alarm). Definitions are the same as with DS-1. The network element shall be able to transmit and receive the Far-End Out Of Frame (FEOOF) alarm for those network elements that transmit them. In addition, the network element shall be able to transmit and receive Far-End Alarm and Control (FEAC) signals. The FEAC option allows the network element to display far-end alarm and status information via the FEAC channel and to transmit FEAC messages from the near-end to the far-end.

8. **[Required]** The network element shall provide the following SONET VT alarms: Include Signal Label Mismatch, Receive Unequipped, and Rx AIS. Signal label mismatch tells whether the VT payload is locked or floating. Rx unequipped indicates that the far end SONET port has not been provisioned.

9. **[Required]** The network element shall provide the following DS-1 alarms: Alarm Indication Signal (AIS) or yellow alarm, Loss Of Signal (LOS), Remote Alarm Indication (RAI)/yellow alarm, and excess zeroes. AIS is transmitted as a result of a received LOS. The RAI or yellow alarm is transmitted upstream to indicate a red alarm or LOS downstream. Alarms shall indicate which physical port is receiving or transmitting the alarm. The yellow or RAI alarm is for Extended Super Frame (ESF) circuits only. Excess zeroes alarm only applies to D-4/Super Frame circuits.

5.5.4.14 Performance Management Requirements

1. **[Required]** The network element shall perform Hairpinning and ADM functions in accordance with GR-496.

2. **[Required]** The network element shall perform Drop ADM functions in accordance with GR-496.

3. **[Required]** The network element shall perform Continue ADM functions in accordance with GR-496.

4. **[Conditional]** The network element shall perform Drop and Continue ADM functions in accordance with GR-496.

5. **[Required]** The network element shall provide the ability to hub or nest lower DISN Access elements in a linear or ring configuration from user-side interfaces.

6. **[Conditional]** The network element shall not utilize external connections for ring interconnection. Where multiple rings can be supported by a single shelf, connectivity

between rings shall be accomplished via the switch matrix. No external connection between tributary interfaces shall be used to cross-connect rings in the same bay.

7. **[Required]** The network element shall be protocol-transparent to incoming bit streams. Except for internetworking functions associated with Ethernet Services within the network element, the network element shall not perform any user protocol conversions.

8. **[Required]** The network element shall not impart any errors onto the connections during cross-connects, grooming or multiplexing.

9. **[Required]** The network element shall perform hair-pinning cross connects without affecting the line capacity rate of the network element.

10. **[Required]** The network element shall send the appropriate Alarm Indication Signal (AIS) and Remote Defect Indication (RDI) to adjacent network elements, the EMS, and/or higher-level management systems after detecting signal failure or degraded conditions for a specified alarm or indication activation time as per T1.231, Tables 2, 6 and 11.

11. **[Required]** The network element shall remove appropriate AIS and RDI after another network element has cleared the signal failure or degraded conditions for a specified alarm or indication activation time as per T1.231, Tables 2, 6 and 11.

12. **[Conditional]** The network element shall have internal local and remote terminal loop-back capability as per GR-253, (R) 6-380.

13. **[Required]** The network element shall have a local and remote service loop-back capability as per GR-253, (R) 6-389.

14. **[Required]** The network element with DS-1/E-1 line terminations shall provide both DS-1/E-1 terminal and service loop-back capabilities as per GR-253, (O) 6-397.

15. **[Required]** The network element with DS-3 line terminations shall provide both DS-3 terminal and service loop-back capabilities as per GR-253, (O) 6-397.

5.5.4.15 EMS Requirements

1. **[Required]** The DISN Access EMS shall report physical layer (layer 1) statistics. Further, it shall report layer 2 errors. It shall report all quality of service (QoS) parameters defined for the Resilient Packet Ring (RPR) as described in IEEE 802.17
.

2. **[Required]** The DISN Access EMS shall be able to track frame errors, P-Bit Parity Errors, C-Bit Parity Errors, and Far-End Block Errors (FEBE).

5.5.4.16 Standards Compliance Requirements

1. **[Required]** Telcordia GR-253, Synchronous Optical Network (SONET) Transport, Issue 3, September 2000.

2. **[Required]** Telcordia GR-2996, Generic Criteria for SONET Digital Cross-Connect Systems, Issue 1, January 1999.

3. **[Required]** ITU-T G.783, Characteristics of Synchronous Digital Hierarchy (SDH) Equipment Functional Block for VC-3/4 Switching and Cross Connects.

4. **[Required]** ITU-T G.957, Optical Interfaces for Equipment and Systems Relating to the Synchronous Digital Hierarchy.

5. **[Required]** ITU-T G.707, Network Interface for Synchronous Digital Hierarchy.

6. **[Required]** ITU-T G.841, Types and Characteristics of SDH Network Protection Architectures.

7. **[Required]** ITU-T G.842, Inter-working of SDH Network Protection Architectures.

8. **[Required]** ITU Recommendation G.872 (1999), Architecture of Optical Transport Networks.

9. **[Required]** Telcordia GR-499-CORE Transport Systems Generic Requirements: Common Requirements, Issue 2, December 1998.

5.5.5 DISN Router Requirements

The DISN employs a variety of makes and models of routers. The integration of these routers into the DISN architecture is dependent on capabilities such as backplane capacity and available interfaces. It is customary to assign names to such routers to depict their placement in the architecture. Examples would be Provider (P) routers and Provider Edge (PE) routers. Typically, the higher backplane routers, which also support high bandwidth but low port density interfaces, are used in the core of the DISN. However, as technologies evolve, no specific make or model of router should be limited to a particular place in the architecture. Such decisions will be made by the engineers who design the network. As such, the routers that are required for the DISN fall into categories of small, medium, and large. Each of these routers may support a

variety of interface types and numbers. The size of the routers is indicative of certain characteristics such as backplane capacity and packet forwarding capability. The specific bandwidth capacity for these routers and their packet forwarding capabilities is TBD.

5.5.5.1 Interface Requirements

The interfaces specified below do not have to be supported by all routers but must be supported by at least one (and preferably more than one) router. The decision on which interface to use with which chassis will be decided during the design phase, upgrade, or technical refresh of future networks or existing networks as appropriate.

5.5.5.1.1 POS Interface Requirements

1. **[Required]** The Core Network network element shall support OC-3c/STM-1 Packet Over SONET (POS) interfaces.

2. **[Required]** OC-3c/STM-1 POS interfaces shall be configurable to support either SONET or Synchronous Digital Hierarchy (SDH) framing.

3. **[Required]** OC-3c/ STM-1 POS interfaces shall conform to ANSI T1.105-2001.

4. **[Required]** OC-3c/ STM-1 POS interfaces shall conform to Telcordia GR-253 (sections 3, 4, and 5).

5. **[Required]** OC-3c/ STM-1 POS interfaces shall conform to ITU-T G.707, and ITU-T G.957.

6. **[Required]** OC-3c/ STM-1 POS interfaces shall provide the standard SONET STS-1, STS-N, and STS-Nc frame structures defined in ANSI T1.105-2001.

7. **[Required]** OC-3c/STM-1 POS interfaces shall provide the standard SDH AU-3, AU-4, and AU-4-Xc frame structures defined in ITU-T G.707.

8. **[Required]** The definition, generation, and function of the OC-3c/ STM-1 POS interface SONET overhead and pointer processing shall follow standards defined in ANSI T1.105-2001.

9. **[Required]** The definition, generation, and function of the OC-3c/ STM-1 SDH interface SDH overhead and pointer processing shall follow standards defined in ITU-T G.707.

10. **[Required]** OC-3c/ STM-1 POS interfaces shall ignore the value contained in unused bits/bytes.

11. **[Required]** OC-3c/STM-1 POS interfaces shall support point-to-point frame relay encapsulation for link layer framing of packets as defined by IETF RFC 2427.

12. **[Required]** OC-3c/STM-1 POS interfaces shall support Point-to-Point Protocol (PPP) for link layer framing of packets as defined by IETF RFC 1662 and 2615.

13. **[Required]** OC-3c/STM-1 POS interfaces shall support High Level Data Link Control (HDLC) for link layer framing of packets.

14. **[Required]** OC-3c/ STM-1 POS interfaces shall allow separate Maximum Transmission Unit (MTU) sizes for unlabeled network layer packets and labeled MPLS packets.

15. **[Required]** OC-3c/STM-1 POS interfaces shall support an MTU size of at least 4470 bytes.

16. **[Required]** OC-3c/STM-1 POS interfaces shall support appropriate in-band routing and control protocols, such as ISIS, RSVP, and BGP.

17. **[Required]** OC-3c/ STM-1 POS interfaces shall support the transport of IPv6 packets.

18. **[Required]** OC-3c/STM-1 POS interfaces shall clock transmitted data based on internal source clock.

19. **[Required]** OC-3c/STM-1 POS interfaces shall clock transmitted data based on external source clock recovered from the received line.

20. **[Required]** The network element shall support OC-12c/ STM-4 POS interfaces.

21. **[Required]** OC-12c/STM-4 POS interfaces shall be configurable to support either SONET or Synchronous Digital Hierarchy (SDH) framing.

22. **[Required]** OC-12c/ STM-4 POS interfaces shall conform to ANSI T1.105-2001.

23. **[Required]** OC-12c/ STM-4 POS interfaces shall conform to Telcordia GR-253 (sections 3, 4, and 5).

24. **[Required]** OC-12c/ STM-4 POS interfaces shall conform to ITU-T G.707, and ITU-T G.957.

25. **[Required]** OC-12c/ STM-4 POS interfaces shall provide the standard SONET STS-1, STS-N, and STS-Nc frame structures defined in ANSI T1.105-2001.

26. **[Required]** OC-12c/STM-4 POS interfaces shall provide the standard SDH AU-3, AU-4, and AU-4-Xc frame structures defined in ITU-T G.707.

27. **[Required]** The definition, generation, and function of the OC-12c/ STM-4 POS interface SONET overhead and pointer processing shall follow standards defined in ANSI T1.105-2001.

28. **[Required]** The definition, generation, and function of the OC-12c/ STM-4 POS interface SDH overhead and pointer processing shall follow standards defined in ITU-T G.707.

29. **[Required]** OC-12c/ STM-4 POS interfaces shall ignore the value contained in unused bits/bytes.

30. **[Required]** OC-12c/STM-4 POS interfaces shall support point-to-point frame relay encapsulation for link layer framing of packets as defined by IETF RFC 2427.

31. **[Required]** OC-12c/STM-4 POS interfaces shall support Point-to-Point Protocol (PPP) for link layer framing of packets as defined by IETF RFC 1662 and 2615.

32. **[Required]** OC-12c/STM-4 POS interfaces shall support High Level Data Link Control (HDLC) for link layer framing of packets.

33. **[Required]** OC-12c/ STM-4 POS interfaces shall allow separate Maximum Transmission Unit (MTU) sizes for unlabeled network layer packets and labeled MPLS packets.

34. **[Required]** OC-12c/STM-4 POS interfaces shall support an MTU size of at least 4470 bytes.

35. **[Required]** OC-12c/STM-4 POS interfaces shall support appropriate in-band routing and control protocols, such as ISIS, RSVP, and internal BGP.

36. **[Required]** OC-12c/ STM-4 POS interfaces shall support the transport of IPv6 packets.

37. **[Required]** OC-12c/STM-4 POS interfaces shall clock transmitted data based on internal source clock.

38. **[Required]** OC-12c/STM-4 POS interfaces shall clock transmitted data based on external source clock recovered from the received line.

39. **[Required]** The network element shall support OC-48c/ STM-16 POS interfaces.

40. **[Required]** OC-48c/STM-16 POS interfaces shall be configurable to support either SONET or Synchronous Digital Hierarchy (SDH) framing.

41. **[Required]** OC-48c/STM-16 POS interfaces shall conform to ANSI T1.105-2001.

42. **[Required]** OC-48c/STM-16 POS interfaces shall conform to Telcordia GR-253 (sections 3, 4, and 5).

43. **[Required]** OC-48c/STM-16 POS interface shall conform to ITU-T G.707, and ITU-T G.957.

44. **[Required]** OC-48c/STM-16 POS interfaces shall provide the standard SONET STS-1, STS-N, and STS-Nc frame structures defined in ANSI T1.105-2001.

45. **[Required]** OC-48c/STM-16 POS interfaces shall provide the standard SDH AU-3, AU-4, and AU-4-Xc frame structures defined in ITU-T G.707.

46. **[Required]** The definition, generation, and function of the OC-48c/ STM-16 POS interface SONET overhead and pointer processing shall follow standards defined in ANSI T1.105-2001.

47. **[Required]** The definition, generation, and function of the OC-48c/ STM-16 POS interface SDH overhead and pointer processing shall follow standards defined in ITU-T G.707.

48. **[Required]** OC-48c/ STM-16 POS interfaces shall ignore the value contained in unused bits/bytes.

49. **[Required]** OC-48c/STM-16 POS interfaces shall support point-to-point frame relay encapsulation for link layer framing of packets as defined by IETF RFC 2427.

50. **[Required]** OC-48c/STM-16 POS interfaces shall support Point-to-Point Protocol (PPP) for link layer framing of packets as defined by IETF RFC 1662 and 2615.

51. **[Required]** OC-48c/STM-16 POS interfaces shall support High Level Data Link Control (HDLC) for link layer framing of packets.

52. **[Required]** OC-48c/ STM-16 POS interfaces shall allow separate Maximum Transmission Unit (MTU) sizes for unlabeled network layer packets and labeled MPLS packets.

53. **[Required]** OC-48c/STM-16 POS interfaces shall support an MTU size of at least 4470 bytes.

54. **[Required]** OC-48c/STM-16 POS interfaces shall support appropriate in-band routing and control protocols, such as ISIS, RSVP, and BGP.

55. **[Required]** OC-48c/ STM-16 POS interfaces shall support the transport of IPv6 packets.

56. **[Required]** OC-48c/STM-16 POS interfaces shall clock transmitted data based on internal source clock.

57. **[Required]** OC-48c/STM-16 POS interfaces shall clock transmitted data based on external source clock recovered from the received line.

58. **[Required]** The network element shall support OC-192c/ STM-64 POS interfaces.

59. **[Required]** OC-192c/STM-64 POS interfaces shall be configurable to support either SONET or Synchronous Digital Hierarchy (SDH) framing.

60. **[Required]** OC-192c/ STM-64 POS interfaces shall conform to ANSI T1.105-2001.

61. **[Required]** OC-192c/ STM-64 POS interfaces shall conform to Telcordia GR-253 (sections 3, 4, and 5).

62. **[Required]** OC-192c/ STM-64 interfaces shall conform to ITU-T G.691.

63. **[Required]** OC-192c/ STM-64 POS interfaces shall provide the standard SONET STS-1, STS-N, and STS-Nc frame structures defined in ANSI T1.105-2001.

64. **[Required]** OC-192c/STM-64 POS interfaces shall provide the standard SDH AU-3, AU-4, and AU-4-Xc frame structures defined in ITU-T G.707.

65. **[Required]** The definition, generation, and function of the OC-192c/ STM-64 POS interface SONET overhead and pointer processing shall follow standards defined in ANSI T1.105-2001.

66. **[Required]** The definition, generation, and function of the OC-192c/ STM-64 POS interface SDH overhead and pointer processing shall follow standards defined in ITU-T G.707.

67. **[Required]** OC-192c/ STM-64 POS interfaces shall ignore the value contained in unused bits/bytes.

68. **[Required]** OC-192c/STM-64 POS interfaces shall support point-to-point frame relay encapsulation for link layer framing of packets as defined by IETF RFC 2427.

69. **[Required]** OC-192c/STM-64 POS interfaces shall support Point-to-Point Protocol (PPP) for link layer framing of packets as defined by IETF RFC 1662 and 2615.

70. **[Required]** OC-192c/STM-64 POS interfaces shall support High Level Data Link Control (HDLC) for link layer framing of packets.

71. **[Required]** OC-192c/ STM-64 POS interfaces shall allow separate Maximum Transmission Unit (MTU) sizes for unlabeled network layer packets and labeled MPLS packets.

72. **[Required]** OC-192c/STM-64 POS interfaces shall support an MTU size of at least 4470 bytes.

73. **[Required]** OC-192c/STM-64 POS interfaces shall support appropriate in-band routing and control protocols, such as ISIS, RSVP, and BGP.

74. **[Required]** OC-192c/STM-64 POS interfaces shall support the transport of IPv6 packets.

75. **[Required]** OC-192c/STM-64 POS interfaces shall support Very Short Reach (VSR) optics as defined by the Optical Internetworking Forum (OIF).

76. **[Required]** OC-192c/STM-64 POS interfaces shall clock transmitted data based on internal source clock.

77. **[Required]** OC-192c/STM-64 POS interfaces shall clock transmitted data based on external source clock recovered from the received line.

78. **[Conditional]** The network element shall support OC-768c/STM-256 POS interfaces.

5.5.5.1.2 ATM Interface Requirements

1. **[Required]** The network element shall support OC-12c/STM-4 Asynchronous Transport Mode (ATM) interfaces.

2. **[Required]** OC-12c/STM-4 ATM interfaces shall be configurable to support either SONET or Synchronous Digital Hierarchy (SDH) framing.

3. **[Required]** OC-12c/ STM-4 ATM interfaces shall conform to ANSI T1.105-2001.

4. **[Required]** OC-12c/ STM-4 ATM interfaces shall conform to Telcordia GR-253 (sections 3, 4, and 5).

5. **[Required]** OC-12c/ STM-4 ATM interfaces shall conform to ITU-T G.707 and ITU-T G.957.

6. **[Required]** OC-12c/ STM-4 ATM interfaces shall provide the standard SONET STS-1, STS-N, and STS-Nc frame structures defined in ANSI T1.105-2001.

7. **[Required]** OC-12c/STM-4 ATM interfaces shall provide the standard SDH AU-3, AU-4, and AU-4-Xc frame structures defined in ITU-T G.707.

8. **[Required]** The definition, generation, and function of the OC-12c/ STM-4 ATM interface SONET overhead and pointer processing shall follow standards defined in ANSI T1.105-2001.

9. **[Required]** The definition, generation, and function of the OC-12c/ STM-4 ATM interface SDH overhead and pointer processing shall follow standards defined in ITU-T G.707.

10. **[Required]** OC-12c/ STM-4 ATM interfaces shall ignore the value contained in unused bits/bytes.

11. **[Required]** OC-12c/STM-4 ATM interfaces shall provide segmentation and reassembly (SAR) of IP packets for transport over AAL5 as defined by IETF RFC 2684.

12. **[Required]** OC-12c/STM-4 ATM interfaces shall support the ATM Forum User Network Interface (UNI).

13. **[Required]** OC-12c/STM-4 ATM interfaces shall support the ATM Forum User Network Interface (UNI) 4.1.

14. **[Required]** OC-12c/STM-4 ATM interfaces shall support the ATM Forum Integrated Local Management Interface (ILMI)**.**

15. **[Required]** OC-12c/STM-4 ATM interfaces shall support F5 Operation, Administration, and Maintenance (OAM).

16. **[Required]** OC-12c/STM-4 ATM interfaces shall allow separate Maximum Transmission Unit (MTU) sizes for unlabeled network layer packets and labeled MPLS packets.

17. **[Required]** OC-12c/STM-4 ATM interfaces shall support appropriate in-band routing and control protocols, such as ISIS, RSVP, and BGP.

18. **[Required]** OC-12c/ STM-4 ATM interfaces shall support the transport of IPv6 packets.

19. **[Required]** OC-12c/STM-4 ATM interfaces shall clock transmitted data based on internal source clock.

20. **[Required]** OC-12c/STM-4 ATM interfaces shall clock transmitted data based on external source clock recovered from the received line.

21. **[Required]** The network element shall support OC-48c/STM-16 ATM interfaces.

22. **[Required]** OC-48c/STM-16 ATM interfaces shall be configurable to support either SONET or Synchronous Digital Hierarchy (SDH) framing.

23. **[Required]** OC-48c/STM-16 ATM interfaces shall conform to ANSI T1.105-2001.

24. **[Required]** OC-48c/STM-16 ATM interfaces shall conform to Telcordia GR-253 (sections 3, 4, and 5).

25. **[Required]** OC-48c/STM-16 ATM interfaces shall conform to ITU-T G.707 and ITU-T G.957.

26. **[Required]** OC-48c/STM-16 ATM interfaces shall provide the standard SONET STS-1, STS-N, and STS-Nc frame structures defined in ANSI T1.105-2001.

27. **[Required]** OC-48c/STM-16 ATM interfaces shall provide the standard SDH AU-3, AU-4, and AU-4-Xc frame structures defined in ITU-T G.707.

28. **[Required]** The definition, generation, and function of the OC-48c/ STM-16 ATM interface SONET overhead and pointer processing shall follow standards defined in ANSI T1.105-2001.

29. **[Required]** The definition, generation, and function of the OC-48c/STM-16 ATM interface SDH overhead and pointer processing shall follow standards defined in ITU-T G.707.

30. **[Required]** OC-48c/ STM-16 ATM interfaces shall ignore the value contained in unused bits/bytes.

31. **[Required]** OC-48c/STM-16 ATM interfaces shall provide segmentation and reassembly (SAR) of IP packets for transport over AAL5 as defined by IETF RFC 2684.

32. **[Required]** OC-48c/STM-16 ATM interfaces shall support the ATM Forum User Network Interface (UNI).

33. **[Required]** OC-48c/STM-16 ATM interfaces shall support the ATM Forum User Network Interface (UNI) 4.1.

34. **[Required]** OC-48c/STM-16 ATM interfaces shall support the ATM Forum Integrated Local Management Interface (ILMI)**.**

35. **[Required]** OC-48c/STM-16 ATM interfaces shall support F5 Operation, Administration, and Maintenance (OAM).

36. **[Required]** OC-48c/STM-16 ATM interfaces shall allow separate Maximum Transmission Unit (MTU) sizes for unlabeled network layer packets and labeled MPLS packets.

37. **[Required]** OC-48c/STM-16 ATM interfaces shall support appropriate in-band routing and control protocols, such as ISIS, RSVP, and BGP.

38. **[Required]** OC-48c/ STM-16 ATM interfaces shall support the transport of IPv6 packets.

39. **[Required]** OC-48c/STM-16 ATM interfaces shall clock transmitted data based on internal source clock.

40. **[Required]** OC-48c/STM-16 ATM interfaces shall clock transmitted data based on external source clock recovered from the received line.

41. **[Required]** The network element shall support OC-192c/STM-64 ATM interfaces.

42. **[Required]** OC-192c/STM-64 ATM interfaces shall be configurable to support either SONET or Synchronous Digital Hierarchy (SDH) framing.

43. **[Required]** OC-192c/ STM-64 ATM interfaces shall conform to ANSI T1.105-2001.

44. **[Required]** OC-192c/ STM-64 ATM interfaces shall conform to Telcordia GR-253 (sections 3, 4, and 5).

45. **[Required]** OC-192c/STM-64 ATM interfaces shall conform to ITU-T G.691.

46. **[Required]** OC-192c/STM-64 ATM interfaces shall provide the standard SONET STS-1, STS-N, and STS-Nc frame structures defined in ANSI T1.105-2001.

47. **[Required]** OC-192c/STM-64 ATM interfaces shall provide the standard SDH AU-3, AU-4, and AU-4-Xc frame structures defined in ITU-T G.707.

48. **[Required]** The definition, generation, and function of the OC-192c/STM-64 ATM interface SONET overhead and pointer processing shall follow standards defined in ANSI T1.105-2001.

49. **[Required]** The definition, generation, and function of the OC-192c/STM-64 ATM interface SDH overhead and pointer processing shall follow standards defined in ITU-T G.707.

50. **[Required]** OC-192c/STM-64 ATM interfaces shall ignore the value contained in unused bits/bytes.

51. **[Required]** OC-192c/STM-64 ATM interfaces shall provide Segmentation And Reassembly (SAR) of IP packets for transport over AAL5 as defined by IETF RFC 2684
.

52. **[Required]** OC-192c/STM-64 ATM interfaces shall support the ATM Forum User Network Interface (UNI).

53. **[Required]** OC-192c/STM-64 ATM interfaces shall support the ATM Forum UNI 4.1.

54. **[Required]** OC-192c/STM-64 ATM interfaces shall support the ATM Forum Integrated Local Management Interface (ILMI)**.**

55. **[Required]** OC-192c/STM-64 ATM interfaces shall support F5 Operation, Administration, and Maintenance (OAM).

56. **[Required]** OC-192c/ STM-64 ATM interfaces shall allow separate Maximum Transmission Unit (MTU) sizes for unlabeled network layer packets and labeled MPLS packets.

57. **[Required]** OC-192c/STM-64 ATM interfaces shall support appropriate in-band routing and control protocols, such as ISIS, RSVP, and BGP.

58. **[Required]** OC-192c/STM-64 ATM interfaces shall support the transport of IPv6 packets.

59. **[Required]** OC-192c/STM-64 ATM interfaces shall support Very Short Reach (VSR) optics as defined by the Optical Internetworking Forum (OIF).

60. **[Required]** OC-192c/STM-64 ATM interfaces shall clock transmitted data based on internal source clock.

61. **[Required]** OC-192c/STM-64 ATM interfaces shall clock transmitted data based on external source clock recovered from the received line.

5.5.5.1.3 Ethernet Interface Requirements

1. **[Required]** The network element shall support Gigabit Ethernet interfaces.

2. **[Required]** Gigabit Ethernet interfaces shall comply with IEEE 802.3-2002.

3. **[Required]** Gigabit Ethernet interfaces shall allow separate Maximum Transmission Unit (MTU) sizes for unlabeled network layer packets and labeled Multi Protocol Label Switching (MPLS) packets.

4. **[Required]** Gigabit Ethernet interfaces shall support an MTU size of at least 4470 bytes.

5. **[Required]** Gigabit Ethernet interfaces shall support modular, interchangeable optics for short reach applications over standard multi-mode fiber optic cable and extended reach applications over standard single-mode fiber optic cable.

6. **[Required]** Gigabit Ethernet interfaces shall support appropriate in-band routing and control protocols, such as ISIS, RSVP, and BGP.

7. **[Required]** The network element shall support 10 Gbps Ethernet interfaces.

8. **[Required]** 10 Gbps Ethernet interfaces shall comply with IEEE Std 802.3ae-2002.

9. **[Required]** 10 Gbps Ethernet interfaces shall support VLAN and priority tagging as defined by IEEE Std 802.1Q-1998.

10. **[Required]** 10 Gbps Ethernet interfaces shall allow separate Maximum Transmission Unit (MTU) sizes for unlabeled network layer packets and labeled MPLS packets.

11. **[Required]** 10 Gbps Ethernet interfaces shall support an MTU size of at least 4470 bytes .

12. **[Required]** 10 Gbps Ethernet interfaces shall support appropriate in-band routing and control protocols, such as ISIS, RSVP, and BGP.

13. **[Required]** 10 Gbps Ethernet interfaces shall support the transport of IPv6 packets.

5.5.5.1.4 Packet Ring Requirements

1. **[Required]** The network element shall support packet ring technology interfaces, e.g., IEEE 802.17 Resilient Packet Ring Working Group.

2. **[Required]** The network element shall support OC-12c/STM-4 packet ring interfaces**.**

3. **[Required]** The network element shall support OC-48c/STM-16 packet ring interfaces**.**

4. **[Required]** The network element shall support OC-192c/STM-64 packet ring interfaces**.**

5.5.5.2 IPv6 Requirements

The IPv6 requirements for routers must be compliant with the requirements specified in the DoD IPv6 Profile version 2.0, and UCR 2008 Section 5.3.5, IPv6 Requirements.

5.5.5.3 Performance Requirements

1. **[Required]** The switch fabric shall be non-blocking while operating at maximum full-duplex rate and bandwidth in a fully loaded chassis.

2. **[Required]** Interfaces shall forward at maximum rate for all packet sizes, including 40-byte IPv4 packets, while offering simultaneous services such as access control list filtering, policy routing, and packet marking.

3. **[Required]** Neither internal nor external control plane signaling shall be interrupted by fully loaded data forwarding.

4. **[Required]** Packet loss within the DISN Router, for reasons other than congestion, lack of route, or external corruption shall be less than 0.1% under full load.

5. **[Required]** Packet processing latency within the DISN Router, not including serialization delay related to the reception and transmission of an entire packet, shall be less than 15 microseconds for a 40-byte packet. (TBD, revisit)

6. **[Required]** The network element shall introduce less than 1.9 microseconds of jitter for all packet sizes while fully loaded. (TBD, revisit)

7. **[Required]** The network element shall support a minimum of 15,000 forwarding cache entries defined as the tuple of group, inbound interface, and outbound interface list. (TBD, revisit)

8. **[Required]** The network element shall support 10,000 multicast groups with a minimum of 150,000 forwarding cache entries.

9. **[Required]** The network element shall support QoS-aware multicast over Diffserv as discussed in IETF draft-bianchi-qos-multicast-over-diffserv.

10. **[Conditional]** The network element shall be ready to accept 40 Gbps interfaces without chassis replacement, including POS, Ethernet, and G.709**.**

5.5.5.4 ISIS Requirements

1. **[Required]** The network element shall implement the Integrated Intermediate System to Intermediate System (ISIS) routing protocol as specified in IETF RFC 1195 and RFC 1142.

2. **[Required]** The implementation of the ISIS protocol on the Provider network element shall interoperate with the implementation of the ISIS protocol on the Provider Edge network element.

3. **[Required]** The network element shall be able to authenticate ISIS routing updates using the HMAC-MD5 algorithm as specified in IETF draft-ietf-isis-hmac.

4. **[Required]** The network element shall support the ISIS Extensions for Traffic Engineering as specified in IETF draft-ietf-isis-traffic.

5. **[Required]** The network element shall support the Extended IS reachability TLV (22) with Sub-TLV TE Default Metric (18) as specified in IETF draft-ietf-isis-traffic.

6. **[Required]** The network element shall support the Extended IP reachability TLV (135) with the up/down bit as specified in IETF draft-ietf-isis-traffic.

7. **[Required]** The network element shall support the Traffic Engineering Network element ID TLV (134) as specified in IETF draft-ietf-isis-traffic.

8. **[Required]** The network element shall support the ISIS Extended IS reachability TLV (22) with Sub-TLV Administrative Group (3) as defined in IETF draft-ietf-isis-traffic.

9. **[Required]** The network element shall support the ISIS Extended IS reachability TLV (22) with Sub-TLV IPv4 Interface Address (6) as specified in IETF draft-ietf-isis-traffic.

10. **[Required]** The network element shall support the ISIS Extended IS reachability TLV (22) with Sub-TLV IPv4 Neighbor Address (8) as specified in IETF draft-ietf-isis-traffic.

11. **[Required]** The network element shall support the ISIS Extended IS reachability TLV (22) with Sub-TLV IPv4 Maximum Link Bandwidth (9) as specified in IETF draft-ietf-isis-traffic.

12. **[Required]** The network element shall support the ISIS Extended IS reachability TLV (22) with Sub-TLV Reservable Link Bandwidth (10) as specified in IETF draft-ietf-isis-traffic.

13. **[Required]** The network element shall support the ISIS Extended IS reachability TLV (22) with Sub-TLV Unreserved Bandwidth (11) (eight values for priorities 0 through 7) as specified in IETF draft-ietf-isis-traffic.

14. **[Required]** The network element shall be compatible with known ISIS Type-Length-Value (TLV) Code Points as defined in RFC 3359 i.e. the network element should only use the code points specified in the RFC for the purpose specified in IETF RFC 3359.

15. **[Required]** The network element shall be able to restart the ISIS routing process and initiate database synchronization without cycling adjacencies through a down state as described in IETF draft-ietf-isis-restart.

16. **[Required]** The network element shall be able to treat an Ethernet interface that is directly connected to a neighboring network element as a point-to-point circuit with regard to ISIS routing as specified in IETF draft-ietf-isis-igp-p2p-over-lan.

17. **[Required]** The network element shall be able to reduce the flooding of redundant LSPs in ISIS topologies as specified in IETF RFC 2973.

18. **[Required]** The network element shall be able to dynamically exchange ISIS hostnames as specified in IETF RFC 2763.

19. **[Required]** The network element shall be able to eliminate ISIS reliance on reliable protocols at the link layer for point-to-point links as specified in IETF RFC 3373.

20. **[Required]** The core router shall be able to support two new TLVs, a reachability TLV and an interface address TLV to distribute the necessary IPv6 information throughout a routing domain, as specified in draft-ietf-isis-ipv6 (TBD, revisit).

21. **[Required]** The core router shall be able to support three new TLVs, and two new sub-TLVs of the Extended IS Reachability TLV that allow a CSPF algorithm to calculate traffic engineered routes using IPv6 addresses, as specified in draft-ietf-isis-ipv6-te. (TBD, revisit)

22. **[Required]** The network element shall recognize ISIS TLVs defined for Generalized MPLS traffic engineering links as specified in the IETF draft-ietf-isis-gmpls-extensions.

23. **[Required]** The network element shall act as an ISIS level 1 network element.

24. **[Required]** The network element shall act as an ISIS level 2 network element.

25. **[Required]** The network element shall act as an ISIS level 1/ level2 network element.

26. **[Required]** The network element shall be able to perform incremental Shortest Path First (SPF) calculations, rather than a full calculation, after minor changes in the network topology.

27. **[Required]** The network element shall begin to forward packets on the new route within 20 milliseconds of receiving a Link State PDU (LSP) that causes the network element to change the SPF route.

28. **[Required]** The network element shall be able to apply filter/access lists to the control plane including route policy to control ISIS route leaking.

29. **[Required]** The network element shall be able to maintain a minimum of 1,000 prefixes in the ISIS database.

30. **[Conditional]** The network element shall be able to maintain a minimum of 10,000 prefixes in the ISIS database.

31. **[Required]** The network element shall support a minimum of 10 ISIS neighbors (adjacencies).

32. **[Conditional]** The network element shall support a minimum of 50 ISIS neighbors (adjacencies).

33. **[Conditional]** The network element shall support traffic load distribution over at least four equal-cost nearest-neighbor links between network elements while maintaining per-flow packet sequence order.

34. **[Conditional]** The network element shall support multiple independent instances of ISIS to offer alternate topologies for different services.

5.5.5.5 OSPF Requirements

1. **[Required]** The network element shall support the Open Shortest Path First (OSPF) link state protocol as defined by IETF RFC 2328.

2. **[Required]** The network element shall support OSPF for IPv6 as defined in IETF RFC 2740.

5.5.5.6 BGP Requirements

1. **[Required]** The network element shall support the Border Gateway Protocol (BGP), Version 4 as specified in IETF RFC 1771, and 1772 for the exchange of network reachability information with external networks (EBGP) and the distribution of external network reachability with internal neighbors (IBGP).

2. **[Required]** The network element shall support the Multi-Protocol BGP (MP-BGP) Sub-Address Family Identifier (SAFI) for multicast addresses as specified in IETF RFC 2858 and the IETF draft-ietc-idr-rfc2858bis.

3. **[Required]** The network element shall support MP-BGP SAFI for global unicast IPv6 Addresses as specified in IETF RFC 2858 and IETF draft-ietf-idr-rfc2858bis.

4. **[Required]** The network element shall support MP-BGP SAFI for MPLS Layer 3 VPN-IPv4 as specified in IETF RFC 2858 and 2547, IETF draft-ietf-idr-rfc2858bis and IETF draft-ietf-ppvpn-rfc2547bis.

5. **[Required]** The implementation of the BGP-4 / MP-BGP protocol on the Provider network element shall interoperate with the implementation of the BGP-4 / MP-BGP protocol on the Provider Edge network element.

6. **[Required]** The network element shall be able to authenticate BGP routing information using an MD5 Signature as specified in IETF RFC 2385 and 2385bis.

7. **[Required]** The network element shall be able to reduce routing oscillations by dampening updates associated with unstable routes as specified in IETF RFC 2439.

8. **[Required]** Enhancements to BGP-4 protocol to mitigate against the persistent BGP route oscillations introduced in particular configurations that use route reflection or confederation in conjunction with the MULTI_EXIT_DEC attribute as documented in IETF RFC 3345.

9. **[Required]** The network element shall be able to tag routes on ingress and egress for common group identification and administration using the Communities attribute as specified in IETF RFC 1997.

10. **[Required]** The network element shall support the Extended Community Attribute that extends the range of the Community Attribute and adds a Type field for structure of the community space as specified in the IETF draft-ietf-idr-bgp-ext-communities.

11. **[Required]** The network element shall be able to distribute an MPLS label with a route in the same Update message as specified in IETF RFC 3107.

12. **[Required]** The network element shall be able to act as a BGP route reflector as specified in IETF RFC 2796.

13. **[Required]** The network element shall be able to act as a MP-BGP route reflector.

14. **[Required]** The network element shall be able to participate as a BGP network element within a confederation of autonomous systems that is represented as a single autonomous system to BGP peers external to the confederation as specified in IETF RFC 3065.

15. **[Required]** The network element shall be able to negotiate capabilities with a BGP neighbor by sending and receiving the optional Capabilities parameter as specified in IETF RFC 3392.

16. **[Required]** The network element shall be able to request and respond to requests for re-advertisement of the BGP neighbor outbound routing information base (Adj-RIB-Out) as specified in IETF RFC 2918.

17. **[Required]** The network element shall be able to restart the BGP routing process and initiate database synchronization with neighbors while preserving forwarding state as specified in IETF draft-ietf-idr-restart.

18. **[Required]** The network element shall be able to apply policy to affect route acceptance and forwarding based on prefix.

19. **[Required]** The network element shall be able to apply policy to affect route acceptance and forwarding based on community string.

20. **[Required]** The network element shall be able to apply policy to affect route acceptance and forwarding based on address family.

21. **[Required]** The network element shall be able to apply policy to affect route acceptance and forwarding based on Autonomous System (AS) path.

22. **[Required]** The network element shall be able to apply policy to affect route acceptance and forwarding based on BGP next-hop.

23. **[Required]** The network element shall be able to apply policy to affect route acceptance and forwarding based on multi-exit discriminator.

24. **[Required]** The network element shall be able to apply policy to affect route acceptance and forwarding based on local preference.

25. **[Required]** The network element shall be able to perform eBGP multihop to allow two non-directly connected peers to exchange eBPG.

26. **[Required]** The network element shall support the BGP TTL Security Hack as specified in IETF draft-gill-btsh.

27. **[Required]** The network element shall be able to logically group neighbors with similar policy attributes to avoid Routing Information Base (RIB) duplication.

28. **[Required]** The network element shall support multiple configurable network element IDs (RID) and corresponding routable source address, e.g., multiple loopback interfaces each with unique address or single loopback with multiple addresses, to separate and uniquely identify each unicast, multicast, and VPN address family supported.

29. **[Required]** The network element shall stabilize its BGP routing table without requiring intervention or assistance after a full system or routing restart.

30. **[Required]** The network element shall support a minimum of 200,000 best path BGP entries that are unique from each other in prefix/subnet.

31. **[Conditional]** The network element shall support a minimum of 400,000 best path BGP entries that are unique from each other in prefix/subnet in addition to 600,000 routes that provide alternate paths to those prefixes/subnets.

32. **[Required]** The network element shall support 100 distinct internal neighbors that are not logically grouped to optimize memory or update processing.

33. **[Conditional]** The network element shall support 200 distinct internal neighbors that are not logically grouped to optimize memory or update processing.

34. **[Required]** The network element shall support 100 distinct external neighbors that are not logically grouped to optimize memory or update processing.

35. **[Conditional]** The network element shall support 200 distinct external neighbors that are not logically grouped to optimize memory or update processing.

5.5.5.7 MPLS Requirements

1. **[Required]** The network element shall act as a Multi Protocol Label Switching (MPLS) Label Switching Router (LSR) by forwarding inbound labeled packets based on the contents of the packet MPLS header and performing label swapping (inbound packet label pop and outbound packet label push) as defined in IETF RFC 3031.

2. **[Required]** The network element shall act as an MPLS Label Edge Router (LER) by pushing a label onto packets when at the Label Switched Path (LSP) ingress and popping a label off packets when at the LSP egress
.
3. **[Required]** The network element shall possess encoding capabilities to produce a valid MPLS-labeled packet from a given label stack and a network layer packet as defined by IETF RFC 3032, section 2.1.

4. **[Conditional]** The network element shall support label stacks consisting of at least three labels.

5. **[Conditional]** The network element shall support load sharing between multiple LSPs with the same ingress and egress LERs.

5.5.5.8 RSVP Requirements

1. **[Required]** The network element shall use extensions to Resource Reservation Protocol (RSVP) to establish MPLS Label Switched Paths (LSP) and enable constraint-based routing traffic engineering as defined by IETF RFC 3209.

2. **[Required]** The implementation of the RSVP protocol on the Provider network element shall interoperate with the implementation of the RSVP protocol on the Provider Edge network element.

3. **[Required]** The network element shall authenticate the integrity of RSVP requests for MPLS LSPs as defined by IETF RFC 2747 and updated by RFC 3097, RSVP Cryptographic Authentication (Updated Message Type Value)

4. **[Required]** The network element shall support the Summary Refresh Message to reduce the processing overhead requirements of RSVP refresh messages as defined by IETF RFC 2961.

5. **[Required]** The network element shall support the Bundle Message to reduce the processing overhead requirements of RSVP refresh messages as defined by IETF RFC 2961.

6. **[Required]** The network element shall be able to dynamically signal and enforce different bandwidth constraints for different classes of traffic that are transported over separately routed constraint-based LSPs as defined by IETF draft-ietf-tewg-diff-te-protocol.

7. **[Required]** The network element shall support Forwarding Adjacencies (FA) and hierarchal or nested label switched paths as described in IETF draft-ietf-mpls-lsp-hierarchy.

8. **[Required]** The network element shall support extensions to RSVP for Generalized MPLS (GMPLS) as specified in IETF draft-ietf-mpls-bundle.

9. **[Required]** The network element shall support protocols for requesting and accepting resources from other physical and link layer network elements and signaling Generalized MPLS (GMPLS) traffic engineered links between nodes as defined by IETF draft-ietf-ccamp-lmp and Optical Internetworking Forum (OIF) User Network Interface (UNI) 1.0.

10. **[Required]** The network element shall support the bundling of multiple component links into a single logical traffic engineered bundled link as specified in IETF draft-ietf-mpls-bundle.

11. **[Required]** The network element shall be able to locally repair an RSVP-TE LSP within 20 milliseconds of downstream link or node failure by rerouting the LSP traffic around the failure as specified in IETF draft-ietf-mpls-rsvp-lsp-fastreroute and IETF draft-ietf-mpls-recovery-frmwrk.

12. **[Required]** The network element acting as an ingress MPLS Label Edge Network element shall reroute data traffic to a secondary pre-signaled LSP in less than 20 ms upon indication of the primary LSP failure.

13. **[Required]** The network element shall support 10,000 bi-directional traffic engineered LSPs acting as an intermediate LSR.

14. **[Required]** The network element shall be able to originate 500 traffic engineered LSPs and terminate the same number.

5.5.5.9 LDP Requirements

1. **[Required]** The network element shall support the Label Distribution Protocol (LDP) for MPLS downstream-unsolicited label distribution as defined by IETF RFC 3036.

2. **[Required]** The implementation of the LDP shall interoperate with the implementation of the LDP on approved network elements.

5.5.5.10 DiffServ Requirements

1. **[Required]** The network element shall support Differentiated Services (Diffserv) in accordance with IETF RFC 2474 and 3140.

2. **[Required]** The network element shall support the Diffserv Expedited Forwarding (EF) per-hop-behavior and code point assignment as defined by IETF RFC 3246.

3. **[Required]** The network element shall support the Diffserv Assured Forwarding (AF) per-hop-behavior classes and code point assignments as defined by IETF RFC 2597.

4. **[Required]** The network element shall support Differentiated Services over MPLS by mapping the Diffserv code points of packets received into MPLS EXP-Inferred LSPs (E-LSP) as defined by IETF RFC 3270.

5. **[Required]** The network element shall support Differentiated Services over MPLS by mapping DiffServ code points of packets received into Label-Only-Inferred LSPs (L-LSPs) as defined by IETF RFC 3270.

6. **[Conditional]** The network element shall support the 16-bit encoding mechanism for the identification of differentiated services Per Hop Behaviors in protocol messages, including both code points defined by standards action and code points not defined by standards action, as specified in IETF RFC 3140.

5.5.5.11 Intserv Requirements

1. **[Required]** The network element shall support Integrated Services (Intserv) using RSVP for user signaled per-flow QoS requirements and for reservation of resources as defined by IETF RFC 2205 and 2210.

2. **[Required]** The network element shall provide Intserv Controlled Load service, which offers a customer service with a low average delay with limited packet loss as defined by IETF RFC 2211.

3. **[Required]** The network element shall provide Intserv Guaranteed service, which offers customers a precisely bounded maximum delay with no packet loss as defined by IETF RFC 2212.

4. **[Required]** The network element shall support preemption priority policy for signaled policy based admission protocols such as RSVP used to establish MPLS LSPs as an alternate preemption mechanism to Diffserv as defined by IETF RFC 3181.

5.5.5.12 Congestion Control Requirements

1. **[Required]** The network element shall provide congestion control based on the EXP field in the MPLS header for E-LSP packets.

2. **[Required]** The network element shall provide congestion control based on the MPLS label for L-LSP packets.

3. **[Required]** The network element shall provide congestion control based on the Differentiated Services Code Point (DSCP) for IPv4 packets.

4. **[Required]** The network element shall provide congestion control based on the Traffic Class field for IPv6 packets.

5.5.5.13 Queuing Requirements

1. **[Required]** The network element shall queue packets based on the EXP field in the MPLS header for E-LSP packets.

2. **[Required]** The network element shall queue packets based on the MPLS label for L-LSP packets.

3. **[Required]** The network element shall queue packets based on the DSCP for IPv4 packets.

4. **[Required]** The network element shall queue packets based on the Traffic Class field for IPv6 packets.

5.5.5.14 Multicast Requirements

1. **[Required]** The network element shall support Protocol Independent Multicast-Sparse Mode (PIM-SM) as defined by IETF RFC 2362 and draft-ietf-pim-sm-v2-new.

2. **[Required]** The network element shall support the bootstrap network element (BSR) mechanism for PIM-SM as defined by IETF draft-ietf-pim-sm-bsr.

3. **[Required]** The network element shall be capable of performing the Rendezvous Point (RP) function for PIM-SM.

4. **[Required]** The network element shall support multiple Rendezvous Points (RP) in a single domain for load sharing and redundancy as defined by IETF RFC 3446.

5. **[Required]** The network element shall enhance inter-domain multicast via Multicast Source Discovery Protocol (MSDP) as defined by IETF draft-ietf-msdp-spec.

6. **[Required]** The network element shall support the Generic Routing Encapsulation (GRE) tunneling protocol as defined by IETF RFC 2784 for the transport of multicast traffic.

7. **[Required]** The network element shall be able to perform a Reverse Path Forwarding (RPF) check on a GRE tunnel interface.

8. **[Required]** The network element shall support Source-Specific Multicast (SSM) and its assigned address range as defined by IETF draft-ietf-ssm-overview and draft-ieft-ssm-arch, Section 5, Network element Requirements.

9. **[Required]** The network element shall support the Border Gateway Multicast Protocol (BGMP) as defined by IETF draft-ietf-bgmp-spec.

10. **[Required]** The network element shall provide multicast routing for native IPv6 packets.

5.5.5.15 Equipment Redundancy Requirements

1. **[Required]** The network element shall support at least one redundant component for every N components that are required for full operation (1:N redundancy protection) for all service affecting components.

2. **[Required]** The network element shall support redundant switch fabric elements and schedulers.

3. **[Required]** The network element shall recover to its pre-failure forwarding performance level within 50 ms after the failure of a single switch fabric element or scheduler.

5.5.5.16 Management Requirements

1. **[Required]** The network element shall support the Internet Group Management Protocol, version 3 (IGMPv3) for IPv4 multicast management and multicast group membership reporting to neighboring multicast network elements as defined by IETF RFC 3376.

2. **[Required]** The network element shall support Multicast Listener Discovery (MLD) version 2 for IPv6 multicast network elements to discover the presence of multicast listeners as defined by IETF draft-vida-mld-v2.

3. **[Required]** The network element shall support administratively scoped addresses (239/8) and multicast administrative boundaries as described in RFC 2365.

5.5.6 DISN Transport Timing and Synchronization Requirements

5.5.6.1 DISN Switch Timing and Synchronization Requirements

1. **[Required]** The DISN Switch shall generate timing to other network elements connected to it. The DISN Switch shall transport timing across the DISN to other network elements. The DISN Switch shall recover timing from network elements connected to it and transport that timing reference across the DISN to other network elements connected to distant DISN Switches.

2. **[Required]** The DISN Switch shall be able to use timing from several timing reference sources.

3. **[Required]** The DISN Switch shall be capable of accepting its timing reference from collocated Building Integrated Timing Supply (BITS) sources or via a line interface from a SONET network element that is being timed from an upstream BITS. It shall also be capable of providing timing to collocated network elements by means of external Digital Signal (DS)-1 timing leads.

4. **[Required]** The DISN Switch shall conform to the Telcordia GR-1244-CORE, Issue 2, December 2000 and GR-253, Issue 3, September 2000 requirements for network timing and synchronization.

5. **[Required]** The DISN Switch shall be compliant with ITU-T G.811 Timing characteristics of primary reference clocks.

6. **[Required]** The system shall be capable of accepting external timing from a BITS system that is traceable to a Stratum 1 Primary Reference Source, as defined in GR-436 and ANSI T-1.101-1999.

7. **[Required]** The DISN Switch shall be capable of receiving two (primary and secondary) external BITS sources. It shall be capable of switching between the primary and secondary source, and the switch shall not cause any errors to be imparted on data traffic.

8. **[Required]** Two sets of duplicated clock hardware (i.e., four-fold clock redundancy) that can independently provide system timing shall be provided. Each set shall consist of two physically separate clock systems. The clock system shall be implemented in such a way that any clock failure, including a loss of a single clock shelf, shall not result in any loss of data traversing the DISN Switch.

9. **[Required]** Neither manual nor autonomous protection switching of clock reference sources or clock units, including manual removal of the active clock unit, shall cause any error on any traffic signal.

10. **[Required]** The system shall be capable of slaving each interface to a specific timing source, such as a BITS source, an internal stratum 3E clock, or the timing recovered from any selected port.

11. **[Required]** The system shall be capable of receiving a BITS clock signal formatted as electrical T-1, AMI formatted ESF with Sync Status Messaging.

12. **[Required]** The system shall provide for the External timing mode as defined in Telcordia GR-253, Issue 3, September 2000, Section 5.4.

13. **[Required]** The system shall provide for the Line timing mode as defined in Telcordia GR-253, Issue 3, September 2000, Section 5.4.

14. **[Required]** The system shall provide for the Loop timing mode as defined in Telcordia GR-253, Issue 3, September 2000, Section 5.4.

15. **[Required]** The system shall provide for the Internal timing mode as defined in Telcordia GR-253, Issue 3, September 2000, Section 5.4.

16. **[Required]** The system shall provide for the Through timing mode as defined in Telcordia GR-253, Issue 3, September 2000, Section 5.4.

17. **[Required]** The system internal clock shall conform to Telcordia GR-253, Issue 3, September 2000, standards for Stratum 3E and higher sources.

18. **[Required]** The system internal clock shall conform to Telcordia GR-253, Issue 3, September 2000, Section 5.4 for Free Run Accuracy, Holdover, Pull-In/Hold In, Wander, Jitter, Phase Transients, Input Tolerance, and Transition from Self-Timing to Normal Timing Modes.

19. **[Required]** The system shall be capable of meeting or exceeding the wander and transient specifications defined in GR-1244-CORE, Issue 2, December 2000.

20. **[Required]** The system shall provide an error-free transition (i.e., no payload errors) between external and internal timing.

21. **[Required]** The physical interface for the external timing references shall be DS-1 or E-1, terminated and transformer coupled, and compliant with ANSI T-1.101-1999 and ITU-T G.703/G.704, respectively.

22. **[Required]** The system shall provide Synchronization Status Messages (SSM) in accordance with GR-253, Issue 3, September 2000, Section 5.4 to preclude and detect timing loops within the SONET network.

23. **[Required]** The system shall conform to the timing message generation, validation, and reaction characteristics detailed in Telcordia GR-253, Issue 3, September 2000, Section 5.4.

5.5.6.2 DISN Access Element Timing and Synchronization Requirements

1. **[Required]** The DISN Access element shall be capable of accepting its timing reference via a line interface from a SONET network element that is being timed from an upstream BITS as defined in Telcordia GR-253 Sections 5.4.

2. **[Required]** The DISN Access element shall be capable of accepting its timing reference via a line interface from an SDH network element that is being timed from an upstream Building Integrated Timing Supply (BITS).

3. **[Required]** The DISN Access element shall conform to the Telcordia GR-1110 requirements for network timing and synchronization.

4. **[Required]** The DISN Access element shall be compliant with ITU-T G.811, Timing Characteristics of Primary Reference Clocks.

5. **[Required]** The DISN Access element shall be capable of accepting two (Primary and Secondary) external timing sources from a BITS system that is traceable to a Stratum 1 Primary Reference Source as defined in GR 000436, ANSI TI.101, and GR-253 Sections 5.4.

6. **[Required]** The DISN Access element shall be capable of providing timing to collocated network elements by means of external DS-1 timing leads.

7. **[Required]** The DISN Access element shall be capable of slaving each interface to a specific timing source, such as a BITS, internal Stratum 3E Clock, or the timing recovered from any selected port.

8. **[Required]** The DISN Access element shall be capable of receiving a BITS clock signal formatted as electrical T-1, AMI formatted ESF with Sync Status Messaging.

9. **[Required]** The DISN Access element shall be capable of receiving a BITS clock signal formatted as electrical E-1 75 or 120 ohms according to ITU G.732.

10. **[Required]** The DISN Access element shall be able to provide a selectable timing option, which will generate timing on DS-1s across the DISN to users connected to other DISN Access elements.

11. **[Required]** The DISN Access element shall be able to provide a selectable timing option, which recovers timing from users connected to the DISN Access element, and transport that timing reference across the DISN to other users connected to the distant DISN Access elements.

12. **[Required]** The DISN Access element shall support the Loop timing mode as defined in Telcordia GR-253, September 2000, Section 5.4.

13. **[Required]** The DISN Access element shall support the Internal timing mode as defined in Telcordia GR-253, September 2000, Section 5.4.

14. **[Required]** The DISN Access element shall support the Through timing mode as defined in Telcordia GR-253, September 2000, Sections 5.4.

15. **[Required]** The DISN Access element's internal clock shall conform to Telcordia GR-253 standards for SONET Minimum Clock (SMC) applications for Stratum 3 and higher sources as per GR-253 Section 5.4.

16. **[Required]** The DISN Access element's internal clock shall conform to Telcordia GR-253, Issue 3 September 2000, Section 5.4 for Free Run Accuracy, Holdover, Pull-In/Hold In, Wander, Jitter, Phase Transients, Input Tolerance, and Transition from Self-Timing to Normal Timing Modes.

17. **[Required]** The network element shall meet or exceed the wander and transient specifications as defined in GR-1244-CORE December 2000.

18. **[Required]** The DISN Access element shall support errorless transitions between external timing and internal timing. An event is errorless if no Severely Errored Seconds (SES) is incurred by the event.

19. **[Required]** The physical interface for the external timing references shall be DS-1 or E-1, terminated and transformer-coupled, and compliant with ANSI T-1.101 or ITU-T G.703/G.704, respectively.

20. **[Required]** The DISN Access element shall provide Synchronization Status Messages (SSM) in accordance with GR-253 Section 5.4 in order to preclude and detect timing loops within the SONET network.

21. **[Required]** The DISN Access element shall conform to the timing message generation, validation, and reaction characteristics detailed in Telcordia GR-253 Section 5.4.

22. **[Required]** Two sets of duplicated clock hardware (i.e., four-fold clock redundancy) that can independently provide system timing shall be provided. Each set shall consist of two physically separate clock systems. The clock system shall be implemented in such a way that any clock failure, including a loss of a single clock shelf, shall not result in any traffic outage.

23. **[Required]** Neither manual nor autonomous protection switching of clock reference sources or clock units, including manual removal of the active clock unit, shall cause any error on any traffic signal.

24. **[Required]** The network element shall provide appropriate alarms and proper responses when the frequencies of the incoming signals differ in magnitude from their nominal frequency by more than 20 parts per million (ppm).

5.5.7 DISN Transport Encryption for Overseas Connections (TBD)

TBD

5.5.8 DISN Transport OSS (TBD)

TBD

5.6 GENERIC ENCRYPTION DEVICE REQUIREMENTS

5.6.1 Introduction

This Section presents a system overview of End Cryptographic Units (ECUs) encryption products, e.g. High Assurance Internet Protocol Encryptor (HAIPE) and Link Encryptor Family (LEF). Subordinate Sub-Sections of UCR 2008, Section 5.6, provide the Core interoperability requirements applicable to each HAIPE and LEF cryptographic device. The requirements are extracted from the Generic Cryptographic Interoperability Requirements Document (GCIRD), Version 1.3 dated 07 January 2008. The GCIRD was developed by Subject Matter Experts (SMEs) and provides Department of Defense (DoD) vetted requirements critically needed for Joint Interoperability Test Command (JITC) testing and certification of Information Assurance (IA) products developed under the Commercial Communications Security (COMSEC) Evaluation Program (CCEP). The development of the GCIRD was requested by the Joint Staff.

Interoperability and Supportability needs are addressed in the Chairman of the Joint Chiefs of Staff Instruction, CJCSI 6212.01D, Interoperability and Supportability of Information Technology (IT) and National Security Systems (NSS). CJCSI 6212.01D establishes policies and procedures for developing, coordinating, reviewing, and approving interoperability and supportability needs, as well as certifying that those needs have been met. The GCIRD provides a set of standards to address interoperability engineering and testing of CCEP products. The purpose of the GCIRD is to provide a coordinated and testable set of requirements to ensure interoperability certification of modernized (ECUs).

The GCIRD establishes interoperability requirements to guide product development so that they can achieve Joint interoperability certification. The scope of these requirements is limited to National Security Agency (NSA) approved CCEP products and other COMSEC products not covered by traditional capabilities documents intended for DoD. The GCIRD is a dynamic document and will be maintained and updated on an annual basis or as required by the Joint Services Cryptographic Modernization Working Group (JSCMWG) Cryptographic Products Testing Integrated Product Team (CPT IPT). At the same time as the GCIRD is updated, this section of the UCR will be updated to remain consistent with the GCIRD.

5.6.2 Encryption Products Overview

ECUs are components of information systems that provide security services, which may include confidentiality, identification & authentication, integrity, and non-repudiation, to the overall system. Typically, the ECU is integrated with other components to provide the overall security required for the system. As such, neither the ECU nor the encryption function provided is a stand-alone system. Figure 5.6-1 illustrates the use of the ECU in a system.

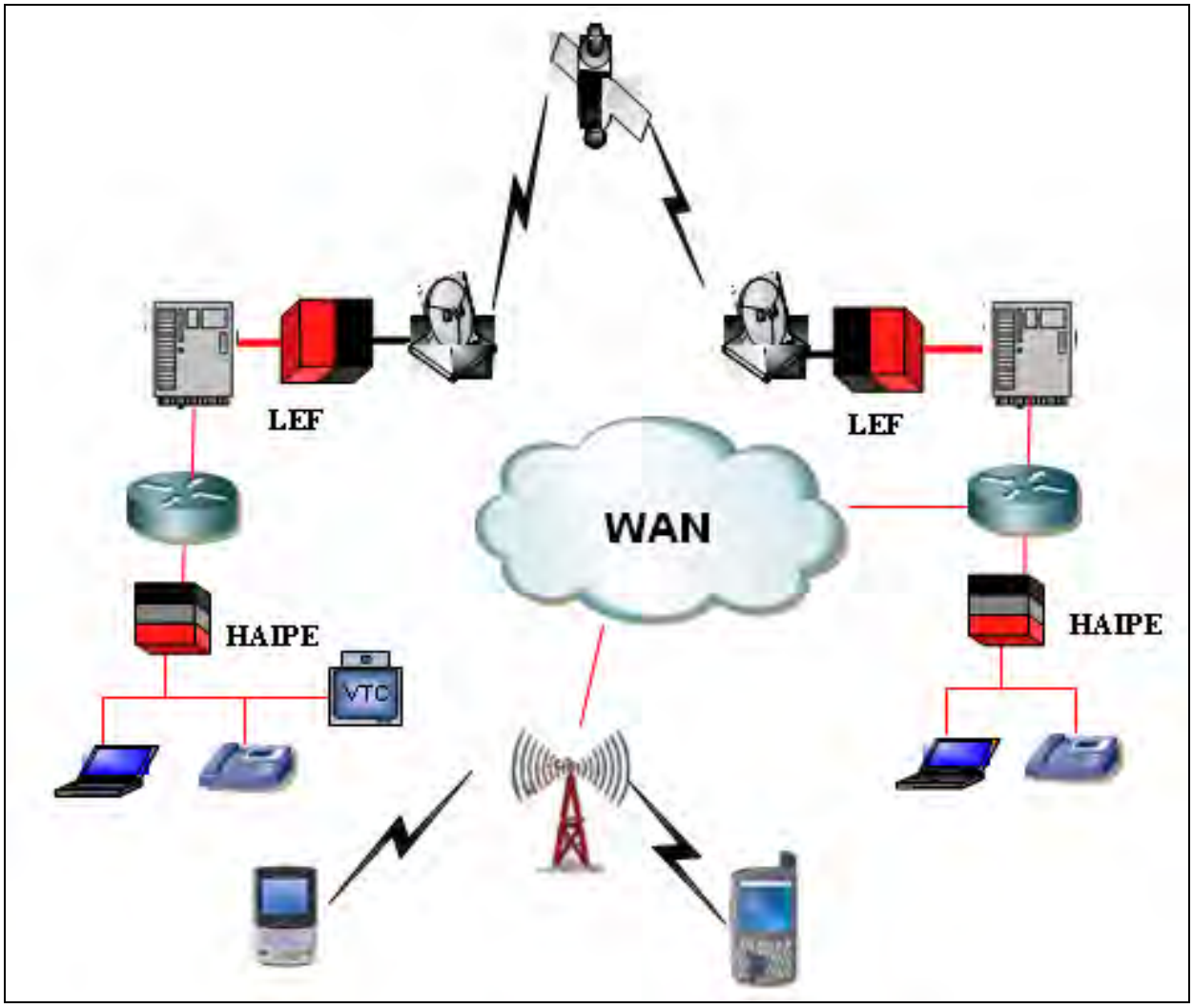


Figure 5.6-1. ECU Overview Diagram

A HAIPE is a programmable Internet Protocol (IP) Information Security (INFOSEC) device with traffic protection, networking, and management features that provide Information Assurance (IA) services for IPv4 and IPv6 networks. HAIPE(s) that are version 3.x compliant meet the DoD mandate for IPv6 compatibility and the goals of the Cryptographic Modernization Initiative (CMI), and are a key component of the GIG Vision. The HAIPE device is designed to provide confidentiality, integrity, and authentication services for IP traffic for tactical and strategic network applications. The HAIPE enables secure transmission across Wide Area Networks (WANs) via IP packet encryption to compatible destination network security devices where decryption takes place. Figure 5.6-2 provides an example of HAIPE implementation within a WAN.

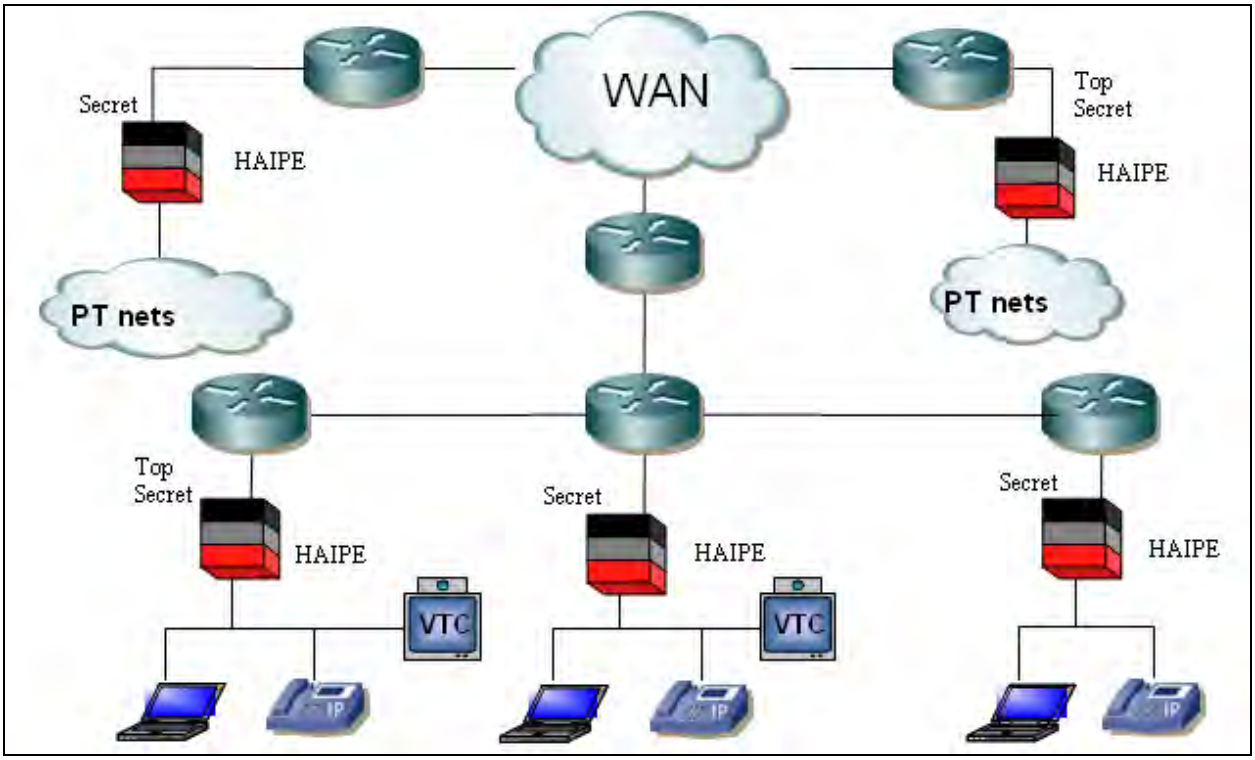


Figure 5.6-2. Example HAIPE Application Diagram

Design requirements are captured and promulgated in the High Assurance Internet Protocol Encryptor Interoperability Specification (HAIPE IS). The HAIPE IS provides interoperability requirements for the following interconnections:

- (U//FOUO) HAIPE Device to HAIPE Device
- (U//FOUO) HAIPE Device to Key Management Infrastructure (KMI)
- (U//FOUO) HAIPE Device to Security Management Infrastructure (SMI)
- (U//FOUO) HAIPE Device to Network Component Infrastructure (NCI)

HAIPE compliancy, a.k.a., "HAIPE Interoperability Certification" is granted by the NSA for a COMSEC device that complies with HAIPE IS v3.0.x. Whereas JITC Interoperability Certification deals with interoperability as defined by CJCSI 6212.01D, it is important to note that JITC certification will not be granted until the device is Type-1 certified by NSA. HAIPE compliance is met by meeting the requirements in the Networking Core and Traffic Protection Core Specifications, plus the three classified cryptography specifications (Suite A, Suite B, and Legacy), and any Extension Specifications. In HAIPE IS 3.1.x, the Networking Core and Traffic Protection Core Specifications have been combined into a single Core Specification.

Link Encryptor Family (LEF) ECUs provide data security for the U.S. military, U.S. Government, Allied Forces and Coalition security environments. Current LEF devices include

Link and Bulk Encryptors. The LEF's primary mission is to protect classified and sensitive digital data in a multitude of network environments: point-to-point, netted, broadcast, or high-speed trunk. The LEF ECU provides the means for encryption and decryption using Suite A and Suite B data security while providing advanced key management features that support the current key distribution system and the Key Management Infrastructure (KMI) initiatives.

LEF ECUs are backward compatible with their legacy family members of equipment to the degree necessary to support continuous operations. Although LEF requirements will vary based on implementation, JITC interoperability testing is still required. Additional testing may be required based on individual Services requirements.

The LEF Specification establishes the detailed cryptographic requirements and basic functional, performance, and security requirements of the Cryptographic Modernization (CM) version of the LEF link/bulk ECUs. It is the intent of this section to incorporate the appropriate LEF specification requirements to provide a sufficiently detailed baseline set of requirements while also allowing vendors design flexibility as to the form, fit, and additional functionality of the resulting ECUs. Figure 5.6-3 illustrates the use of the LEF in a system.

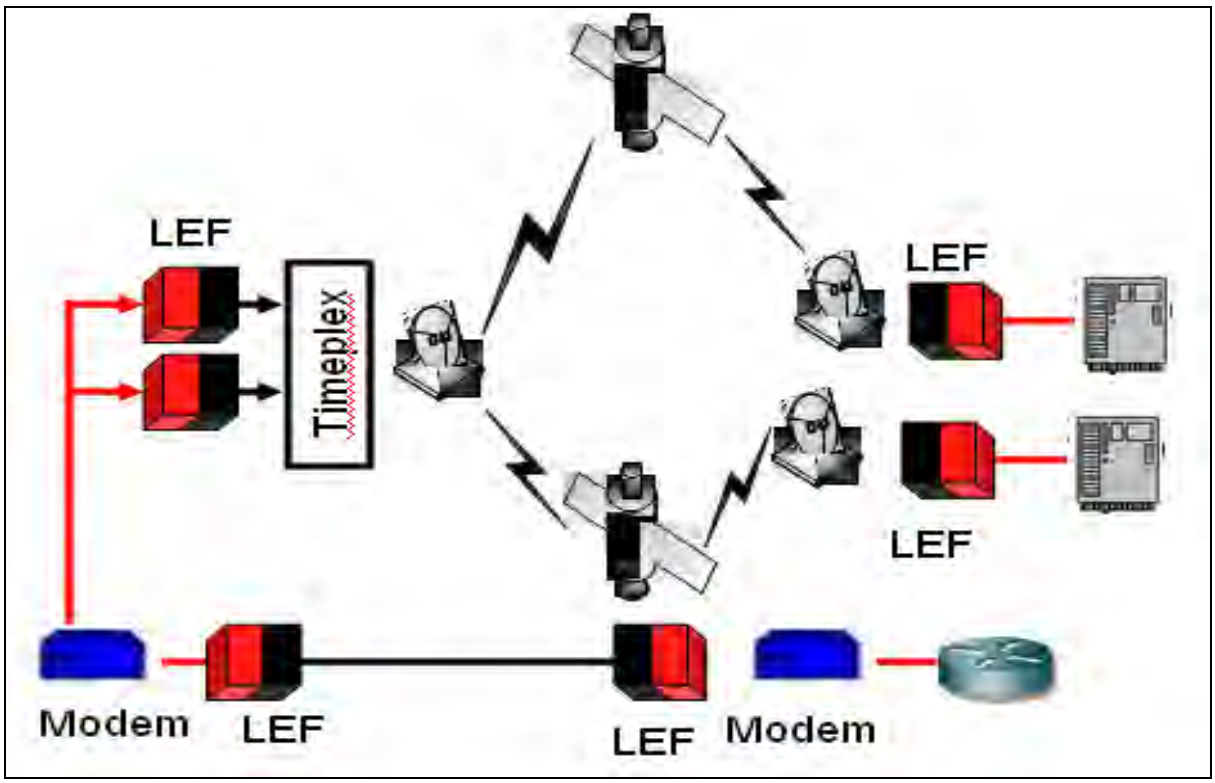


Figure 5.6-3. Example LEF Application Diagram

5.6.3 Minimum Requirements

The following sub-sections present minimum ECU requirements organized by operational capability category.

5.6.3.1 Flexible and Robust Security

[Required: HAIPE and LEF] ECUs shall have the capability to be loaded and configured with legacy algorithms and modes in order to provide legacy-interoperable encryption services with 90% reliability as specified in the Generic Cryptographic Interoperability Requirements Database (ID0215).

[Required: HAIPE and LEF] ECUs shall have an inherent IA capability to ensure information and process integrity (during storage, processing, transmission, and presentation) to prevent unauthorized or unintended changes with 90% reliability as specified in the Generic Cryptographic Interoperability Requirements Database (ID0249).

5.6.3.2 Interfaces

[Required: HAIPE and LEF] ECUs shall be capable of loading and accepting KEYMAT from NSA approved key fill devices with 90% reliability as specified in the Generic Cryptographic Interoperability Requirements Database (ID0295).

[Required: HAIPE and LEF] ECUs shall include a DS-101 cryptographic fill port interface IAW EKMS 308 with 90% reliability as specified in the Generic Cryptographic Interoperability Requirements Database (ID0149).

[Required: LEF] LEF ECUs shall implement data interfaces that conform to the EIA-530 standard. Additional details associated with the interface parameters are defined in the Generic Cryptographic Interoperability Requirements Database (ID0635).

[Required: LEF] LEF ECUs shall implement data interfaces that conform to the RS-232 standard Additional details associated with the interface parameters are defined in the Generic Cryptographic Interoperability Requirements Database (ID0661).

5.6.3.3 Operational Management

[Required: HAIPE and LEF] ECUs shall recover last known, good operational state/settings after loss of primary power with 90% reliability as specified in the Generic Cryptographic Interoperability Requirements Database (ID0210).

[Conditional: HAIPE and LEF] ECUs should have the capability to provide data to management devices to generate user defined high-level operational status reports with 90% reliability.

If a HAIPE or LEF implements this feature, it shall perform as specified in the Generic Cryptographic Interoperability Requirements Database (ID0377).

[Required: HAIPE] HAIPE(s) shall not preclude operation over low bandwidth networks as low as 2.4 kB/s with 90% reliability as specified in the Generic Cryptographic Interoperability Requirements Database (ID0237).

[Conditional: HAIPE] HAIPEs should have the capability to execute the In-Line Network Encryptor (INE) Management command and control function with 90% reliability.

If a HAIPE implements this feature, it shall perform as specified in the Generic Cryptographic Interoperability Requirements Database (ID0320).

[Conditional: HAIPE] HAIPEs should have the capability to execute the Backup Remote Management (RM) command and control function with 90% reliability.

If a HAIPE implements this feature, it shall perform as specified in the Generic Cryptographic Interoperability Requirements Database (ID0325).

[Required: LEF] LEF ECUs shall be capable of operating with legacy Time Division Multiple Access (TDMA) architectures for networked data exchange with 90% reliability as specified in the Generic Cryptographic Interoperability Requirements Database (ID0029).

[Required: LEF] LEF ECUs shall be able to automatically recover security connections after loss of power on one end or both ends of a channel with 90% reliability as specified in the Generic Cryptographic Interoperability Requirements Database (ID0639).

5.6.3.4 Zeroization

[Required: HAIPE and LEF] ECUs shall prevent the accidental deletion of all loaded operational key with 90% reliability as specified in the Generic Cryptographic Interoperability Requirements Database (ID0591).

5.6.3.5 Maintainability and Serviceability

[Required: HAIPE and LEF] New software releases shall, as a minimum, be backward compatible with the previous NSA certified version of software with 90% reliability as specified in the Generic Cryptographic Interoperability Requirements Database (ID0214).

[Required: LEF] LEF ECUs shall provide autophase if interoperable with KG-84C with 90% reliability as specified in the Generic Cryptographic Interoperability Requirements Database (ID044).

5.6.3.6 Data Recovery

[Required: HAIPE] HAIPE(s) shall be able to recover security associations after loss of power on one end or both ends of the link with 90% reliability as specified in the Generic Cryptographic Interoperability Requirements Database (ID0211).

5.6.3.7 External Interfaces

[Required: HAIPE] HAIPE(s) shall adhere to standard commercial interfaces (e.g., Ethernet, Fast Ethernet, Gigabit Ethernet, or 10 Gigabit Ethernet). Additional details associated with the interface parameters are defined in the Generic Cryptographic Interoperability Requirements Database (ID0223).

[Required: HAIPE] HAIPE(s) devices shall be compatible with network components such as routers and hosts in common usage within the GIG IA architecture with 90% reliability as specified in the Generic Cryptographic Interoperability Requirements Database (ID0226).

5.6.3.8 Programmability

[Required: HAIPE] HAIPE(s) shall be capable of being reprogrammed with updated cryptographic software and algorithms with 90% reliability as specified in the Generic Cryptographic Interoperability Requirements Database (ID0450).

5.6.3.9 Performance

[Required: HAIPE] HAIPE(s) shall operate over connections to satellite links that experience delays of up to two seconds aggregate with 90% reliability as specified in the Generic Cryptographic Interoperability Requirements Database (ID0235).

[Required: HAIPE] HAIPE(s) shall not preclude operation over degraded networks that exhibit Bit Error Rates (BER) as low as 10^2.with 90% reliability as specified in the Generic Cryptographic Interoperability Requirements Database (ID0236).

5.6.3.10 Network Operations

[Required: HAIPE] When subjected to 70% or greater of rated throughput, HAIPE(s) shall maintain secure communications without interruption (i.e. without reboot) with 90% reliability as specified in the Generic Cryptographic Interoperability Requirements Database (ID0166).

5.6.3.11 Key Management

[Required: LEF] LEF ECUs shall have Over-The-Air-Rekey (OTAR) capability with 90% reliability as specified in the Generic Cryptographic Interoperability Requirements Database (ID0022).

5.6.4 Operational Control over Features and Capabilities Management

The GCIRD augments CCEP required documentation such as the product/system specific Telecommunications Security Requirements Document (TSRD) and Information Assurance Security Requirements (IASRD).

5.6.5 General GCIRD Specification Language

The GCIRD uses non-UCR 2008 terminology to define the weighting factors incorporated into the ECU requirement specifications. This differs from the language used in UCR 2008, Section 5.1.4, General Requirement Language. The following mapping from GCIRD to UCR terminology is presented in the following paragraphs:

- The term “SHALL” designates the most important weighting level; that is, mandatory. In UCR 2008, Section 5.6, this requirement has been mapped to the term “REQUIRED”.

- The term “SHOULD” designates requirements, which are requested but are not mandatory. In UCR 2008, Section 5.6, this requirement has been mapped to the term “CONDITIONAL.”

5.6.6 Relationships Among Unified Capabilities Requirements Documents

The following assumptions, dependencies, and references pertain to the ECU products described throughout Section 5.6 and amplify the relationships among Unified Capabilities Requirements Documents discussed in UCR 2008, Section 5.1.5.

5.6.6.1 Assumptions and Dependencies

The following identifies all assumptions and dependencies developed by the Ad Hoc Working Group (AHWG) regarding external factors that may affect interoperability and acquisition processes supported by the GCIRD.

- Policy (i.e. CJCSI 6212) will be modified as appropriate.
- DoD Testing community, to include respective Service Test Commands, will accept and use the GCIRD.
- Department of Defense Architecture Framework (DoDAF) products and NR-KPP will be addressed in the JCIDS documentation of systems utilizing CCEP products.
- The GCIRD is a living document managed by a CPT IPT established under charter and authority of the JSCMWG and updated/changed yearly or as required.
- Secure Communications Interoperability Protocol (SCIP) products are covered elsewhere in UCR 2008.

5.6.6.2 Applicable Documents

The GCIRD provides interoperability requirements for product development and Joint interoperability certification. The scope of these requirements is limited to approved NSA CCEP products and other COMSEC products not covered by traditional capabilities documents intended for DoD. The GCIRD and underlying database will also serve as a cryptographic requirements reference document readily available to the Testing Community, Program Managers across DoD, and Commercial Vendors. This document identifies the core interoperability requirements for cryptographic products and those unique requirements common to individual cryptographic families.

The GCIRD is for use by all DoD Components (including COCOMs, Services, and Agencies) and commercial vendors to aid in development of ECUs. It applies to development of new

cryptographic products as well as major hardware and software upgrades for existing CryptoMod compliant products. The GCIRD applies to cryptographic equipment/devices procured for installation in the Global Information Grid (GIG). For Joint interoperability testing and certification, this document takes precedence over the explicit or implicit requirements of subsidiary or reference documents, standards, and specifications unless applicable validated JCIDS documents already exist.

Tables 5.6-1 through 5.6-6 provide a detailed listing of the applicable government and non-government documents. These tables were extracted from the DRAFT GCIRD, Version 1.3 dated 07 January 2008.

Table 5.6-1. Core Government Documents

DOC ID	NAME	DATE
NSA/CSS POLICY NUMBER 3-9	Cryptographic Modernization Initiative Requirements For Type 1 Cryptographic Products	28 Mar 2003
CM MA ICD	Cryptographic Modernization Mission Area Initial Capabilities Document	14 Aug 04
MIL-STD-1275D	Department Of Defense Interface Standard Characteristics Of 28 Volt Dc Electrical Systems In Military Vehicles	29 Aug 2006
MIL-STD-961E	Department Of Defense Standard Practice Defense And Program-Unique Specifications Format And Content	1 Aug 2003
MIL-STD-167-1A	Department Of Defense Test Method Standard Mechanical Vibrations Of Shipboard Equipment	2 Nov 2005
MIL-HDBK-502	DoD Handbook Acquisition Logistics	30 May 1997
EKMS 217	EKMS Benign Techniques Specification RevG	21 Dec 2001
EKMS 322B	EKMS FIREFLY Specification (SECRET)	5 Apr 2002
EKMS 218	Generic Rekey Front End System Requirements	13 Dec 2001
MIL-STD-1399C (NAVY)	Interface Standard For Shipborne Systems	2 Feb 1988
DODD 4630.5	Interoperability and Supportability of Information Technology (IT) and National Security Systems (NSS)	5 May 2004
CJCSI 6212.01D	Interoperability And Supportability Of Information Technology And National Security Systems	8 Mar 2006
CJCSI 3170.01E	Joint Capabilities Integration And Development System	11 May 2005
EKMS 308	Key Distribution Functional Standard RevD SCN-2	23 Mar 2004
	KMI CI-2 CDD	17 Feb 2005
MIL-HDBK-5400	Military Handbook Airborne General Guidelines For Electronic Equipment	30 Nov 1995
MIL-HDBK-454A	Military Handbook General Guidelines For Electronic Equipment	3 Nov 2000
MIL-S-901D (NAVY)	Military Specification Requirements For Shock Tests, H.I. (High-Impact) Shipboard Machinery, Equipment, And Systems	17 Mar 1989
CNSSI 4009	National Information Systems Security INFOSEC Glossary	Sep 2000
DODI 5000.2	Operation of the Defense Acquisition System	12 May 2003

DOC ID	NAME	DATE
CJCSM 3170.01B	Operation Of The Joint Capabilities Integration And Development System	11 May 2005
	P^3 Generation & Distribution Specification for Foreign Interoperability In-Line Network Encryptors (INE), v2	20 Oct 2005
DODI 4630.8	Procedures for Interoperability and Supportability of Information Technology (IT) and National Security Systems (NSS)	30 Jun 2004
NIST SP 800-56A	Recommendation for Obtaining Assurances for Digital Signature Application	Apr 2006
MIL-HDBK-217F	Reliability Prediction of Electronic Equipments	28 Feb 1995
CNS 4005	Safeguarding Communications Security Facilities and Materials	Aug 1997
KMI 3003	Sender Intermediary Receiver (SIR) Model	29 Oct 2005
	TECOM Test Operations Procedure (TOP) 1-2-511	29 Dec 1989
DODD 5000.1	The Defense Acquisition System	24 Nov 2003

Table 5.6-2. HAIPE Government Documents

DOC ID	NAME	DATE
	HAIPE (Version 1.35) Remote Manager Test Plan v1.1	22 Feb 2006
	HAIPE Interoperability Specification (IS) 1.3.5	11 May 2004
	HAIPE Interoperability Specification 3.1.0	31 Dec 2006
	HAIPE IS 3.1 Auto Security Association Extension	31 Dec 2006
	HAIPE IS 3.1 Gateway Extension	31 Dec 2006
	HAIPE IS 3.1 Generic Discovery Client Extension	31 Dec 2006
	HAIPE IS 3.1 Implicit Peer Enclave Prefix Discovery Extension	31 Dec 2006
	HAIPE IS 3.1 Legacy Discovery Extension	31 Dec 2006
	HAIPE IS 3.1 Legacy Encapsulating Security Payload Extension	31 Dec 2006
	HAIPE IS 3.1 Reachability Extension	31 Dec 2006
	HAIPE IS 3.1 Remote Configuration and Monitor Extension	31 Dec 2006
	HAIPE IS 3.1 Remote Provisioning Authority Extension	31 Dec 2006
	HAIPE IS 3.1 Remote Provisioning Extension	31 Dec 2006
DISA/JITC	High Assurance Internet Protocol Encryptor (HAIPE) Interoperability Test Plan	Mar 2006
DISA/JITC	High Assurance Internet Protocol Encryptor (HAIPE) Interoperability Test Report	Aug 2006
	TRADOC Futures Center Reliability And Maintainability (R&M) ANALYSIS For The High Assurance Internet Protocol Encryptor (HAIPE)	22 Aug 2005

Table 5.6-3. LEF Government Documents

DOC ID	NAME	DATE
	KIV-7M Encryption Device Release 1.0 Interoperability Assessment Plan	Jul 2006
	LEF Key Specification, Rev E.	1 Nov 06
	LEFCIS Classified Appendix	9 May 2006
NSA 03-01A	Link Encryptor Family (LEF) Cryptographic Interoperability Specification Version 2.1.0	9 May 2006
	TRADOC Futures Center Reliability And Maintainability (R&M) ANALYSIS For The Link Encryptor Family (LEF)	22 Aug 2005

Table 5.6-4. Core Non-Government Documents

DOC ID	NAME	DATE
ANSI/EIA-310-D-92	Cabinets, Racks, Panels and Associated Equipment. American National Standards Institute (ANSI) / Electronic Industries Association (EIA) Standard	Sep 1992
ITU P.Imp563	Implementers' Guide for ITU-T Recommendation P.563	
RFC 3647	Internet X.509 Public Key Infrastructure Certification Policy and Certification Practices Framework	Nov 2003
ITU-T Recommendation P.800.1	Mean Opinion Score (MOS) Terminology	Mar 2003
ITU-T Recommendation P.800	Methods for subjective determination of transmission quality (formerly P.80)	1996
ITU-T Recommendation P.563,	Single-ended method for objective speech quality assessment in narrow-band telephony applications.	2004
ASME Y14.35M	This Standard defines the practices for revising drawings and associated documentation and establishes methods for identification and recording revisions. The revision practices of this Standard apply to any form of original drawing and associated documentation.	8 Dec 1997
ASME Y14.24	This Standard defines the types of engineering drawings most frequently used to establish engineering requirements. It describes typical applications and minimum content requirements. Drawings for specialized engineering disciplines (e.g., marine, civil, construction, optics, etc.) are not included in this Standard.	1 Jan 1999
ASME Y14.100	This Standard establishes the essential requirements and reference documents applicable to the preparation and revision of engineering drawings and associated lists. It is essential that this Standard be used in close conjunction with ASME Y14.24, ASME Y14.34M, and ASME Y14.35M.	1 Jan 2004

DOC ID	NAME	DATE
ASME Y14.34M	This Standard establishes the minimum requirements for the preparation and revision of parts lists, application lists, data lists, and index lists. In addition, this Standard presents certain options that may be into incorporated into parts lists, data lists, index lists, application lists, indentured data lists, and wire lists at the discretion of the design activity.	1 Jan 1996
	Universal Serial Bus (USB) Specification Version 2.0	7 Dec 2000
RFC 4108	Using CMS to Protect Firmware Packages	Aug 2005

Table 5.6-5. HAIPE Non-Government Documents

DOC ID	NAME	DATE
RFC 3414	User-based Security Model for SNMP V3	Dec 2002
RFC 3415	View-based Access Control Model SNMP	Dec 2002

Table 5.6-6. LEF Non-Government Documents

DOC ID	NAME	DATE
EIA-530	Electronics Industries Alliance (EIA) Standard For The Interconnection Of DTE and DCE Employing Serial Binary Data Interchange with Control Information Exchanged on Separate Control Circuits	
RS-232	Recommended Standard 232 for Serial Binary Data Signals Connecting Between a DTE and a DCE	

THIS PAGE INTENTIONALLY LEFT BLANK

5.7 INSTANT MESSAGING, CHAT AND PRESENCE/AWARENESS

5.7.1 Introduction

Presence/Awareness, Instant Messaging, and Chat features and capabilities listed in this section are not required for all products on the APL, but may be offered as a part of a unified capabilities offering. The definitions for Instant Messaging (IM), Chat, and Presence/Awareness are found in Section A1, Definitions, Abbreviations, Acronyms, and References.

5.7.2 Presence/Awareness, IM and Chat Standards

The DISR mandated standard for Presence/Awareness, IM, and Chat is Extensible Messaging and Presence Protocol (XMPP). XMPP is both a client-to-server and server-to-server protocol. DoD's mandate of this protocol within the DISR has three primary justifications:

1. The XMPP is lower bandwidth than SIP/SIMPLE based systems and its bandwidth efficiency increases its feasibility of deployment further to the edge within bandwidth constrained tactical deployments.

2. The XMPP is an extensible standard which ensures future flexibility.

3. Many IM and Chat vendors currently offer XMPP natively or offer a bridge or gateway to XMPP.

The core XMPP protocol is defined by Request for Comment (RFC) 3920 and RFC 3921. A wide variety of applications can be built on top of the core Extensible Markup Language (XML) streaming layer. The first such application is IM and Presence/Awareness. The basic IM and Presence/Awareness extensions specified in RFC 3921 address the requirements of RFC 2779, as well as the contact list functionality expected in IM and presence/awareness systems. RFC 3921 also makes it possible to separate the messaging and Presence/Awareness functionality if desired, although most deployments offer both.

5.7.3 Routing and Addressing

Basic routing for Enterprise Presence/Awareness, IM and Chat use the DNS to locate connection points or servers when configured in a federated manner. Entity identification shall use uniform IDs as outlined in RFC 4622.

[Required: FY12] Systems that provide Presence/Awareness, IM and/or Chat shall use uniform IDs as defined in RFC 4622.

The recipient's username or entity ID is unique to each server; and the server name is the hostname to the right of a user's XID. This ID associates the client with a particular server similar to an email format where "entity@server" uniquely defines each entity in the federation.

Using the addressing scheme outlined above insures that any system offering Presence/ Awareness, IM, and/or Chat is capable of federating to other Presence/Awareness, IM, and/or Chat systems.

Figure 5.7.3-1 illustrates routing of XMPP-based Presence/Awareness, IM and Chat messages. Messages are not sent directly between clients, but are instead sent from a sender's client to his server and his server delivers the message to recipient's server which then delivers the message to the recipient's client. If the recipient is not online when the message is received, if a queuing function is enabled on the server, the server will queue the message for delivery for when the user comes back online.

Although only the basic message routing is described above, additional security measures such as server certificates and the use of TLS over port 5222 may be required for authentication.

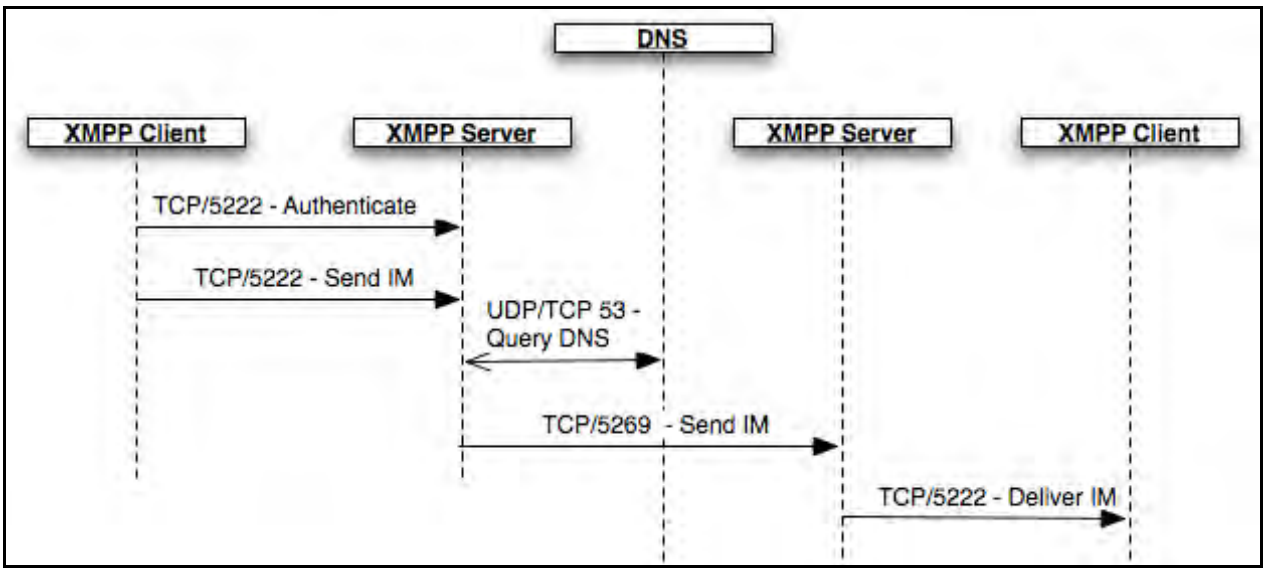


Figure 5.7.3-1. Routing of XMPP-based Presence/Awareness, IM, and Chat Messages

5.7.4 Ports and Protocols

[Required: FY12] Systems implementing XMPP-based Presence/Awareness, IM, and Chat shall use port 5222 for client communications.

[Required: FY12] Systems implementing XMPP-based Presence/Awareness, IM, and Chat shall use port 5269 for server communication.

NOTE: Systems that implement XMPP-based Presence/Awareness, IM, and Chat can secure their systems using TLS over port 5222.

5.7.5 Standards Requirements

5.7.5.1 Instant Messaging and Chat

The IM feature allows users on different computers or devices to send and receive one-to-one ad-hoc text message exchanged over a network in real-time. The Chat feature allows two or more users operating on different computers or devices to exchange real time text messages chat or messaging room.

[Required: FY12] IM and Chat system capabilities shall comply with the DISR. As of the publication of UCR 2008, the following standards and extensions apply to IM and Chat and are contained in the Messaging & Presence Family section of the DISR:

- RFC 3920: XMPP Core
- RFC 3921: XMPP IM
- XEP-0030: Service Discovery
- XEP-0004: Data Forms
- XEP-0016: Privacy Lists
- XEP-0033: Extended Stanza Addressing (ESA)
- XEP-0071: XHTML-IM
- XEP-0077: In-Band Registration
- XEP-0045: Multi-User Chat
- XEP-0068: Field Standardization for Data Forms
- XEP-0082: Jabber Date and Time Profiles
- XEP-0128: Service Discovery Extensions
- XEP-0115: Entity Capabilities
- XEP-0138: Stream Compression
- RFC 4422: Simple Authentication and Security Layer (SASL) Authentication
- XEP-0191: Simple Communications Blocking

The File Sharing part of XEP-0117 shall not be implemented.

These standards are mandated and additionally specified in the DISR under the Messaging & Presence Family of standards.

For client and server standards testing purposes, XEP-0211 (Client Standard) and XEP-0212 (Server Standards) are mandatory. These standards contain the set of RFC and XEP extensions that will be tested for basic XMPP compliance.

XMPP servers may be configured, when possible in the implementation to use XEP-0138: (Stream Compression) to optimize bandwidth usage. Additionally, XMPP Servers, especially ones in tactical or low-bandwidth environments, may set limits on the amount of Chat room history that is sent to the client on connection or reconnection to a chat room. This is a configuration recommendation and does not apply to a specific IETF standard.

Additional standards marked as conditional, to include Privacy Lists, Simple Communications Blocking, Extended Stanza Addressing, XHTML-IM, Field Standardization for Data Forms, Entity Capabilities, and Simple Authentication and Security Layer may be implemented in IM and Chat Client, Server, or Presence/Awareness servers. These standards are called out as conditional but desired by the DoD.

Table 5.7.5-1 is a summary of the standards that are required and conditional in accordance with the DISR.

Table 5.7.5-1. Required and Conditional Standards for Presence/Awareness, IM, and Chat

IETF STANDARD	IM CLIENT	IM SERVER	CHAT CLIENT	CHAT SERVER	PRESENCE/ AWARENESS
RFC 3920: XMPP Core	R	R	R	R	R
RFC 3921: XMPP IM	R	R	R	R	R
XEP-0030: Service Discovery	R	R	R	R	C
XEP-0004: Data Forms			R	R	
XEP-0016: Privacy Lists	C	C	C	C	
XEP-0033: Extended Stanza Addressing (ESA)	C	C	C	C	
XEP-0071: XHTML-IM	C		C		
XEP-0077: In-Band Registration	R	R	R	R	
XEP-0045: Multi-User Chat	NA	NA	R	R	NA
XEP-0068: Field Standardization for Data Forms			R	R	
XEP-0082: Jabber Date and Time Profiles			R	R	
XEP-0128: Service Discovery Extensions			R	R	
XEP-0115: Entity Capabilities	C		C		
XEP-0138: Stream Compression	C	C	C	C	C

IETF STANDARD	IM CLIENT	IM SERVER	CHAT CLIENT	CHAT SERVER	PRESENCE/ AWARENESS
RFC 4422: Simple Authentication and Security Layer (SASL) Authentication		C		C	
XEP-0191: Simple Communications Blocking		C		C	
XEP-0211: XMPP Basic Client 2008	R	N/A	R	N/A	R
XEP-0212: XMPP Basic Server 2008	N/A	R	N/A	R	R

5.7.5.2 Presence/Awareness

[Required: FY12] If Presence/Awareness is provided, the system shall provide the functionality in accordance with the RFC 3920 and 3921.

Although these RFCs cover features other than mere Presence/Awareness, only Presence/ Awareness capabilities need to be implemented to comply. Presence/Awareness may be embedded in telephony, email/calendar, office productivity applications, as well as traditional IM/Chat clients.

Systems providing Presence/Awareness capabilities may provide user profile information. A user's presence profile may also contain optional information that can be controlled by local policy. Specifically, Presence may include the following:

- Account identification
- Virtual Locations of User
- Geographic Location of User
- Email Address of User
- Telephony usage
- Calendar availability of User

5.7.6 Security Requirements for Presence/Awareness, IM, and Chat

[Required] All IM and Chat systems shall adhere to the *Instant Messaging Security Technical Implementation Guide, Version 1 Release 2. (February 2008).*

Where the UCR 2008 requirements differ from the current IM STIG, the IM STIG specification shall apply.

[Required: FY12] The XMPP-based Presence/Awareness, IM, and Chat servers shall restrict their XMPP user directory searches to only users that have accounts on that server.

[Required: FY12] The XMPP servers and or systems connecting via gateway shall prohibit in-band registration or anonymous use.

[Required: FY12] The XMPP server systems shall allow an operator to create all users.

[Required: FY12] The Multi-User-Chat (MUC) rooms shall support a configurable parameter to deny anonymous access.

[Required: FY12] The MUC rooms shall prevent users from changing their username or nicknames.

[Required: FY12] The XMPP servers shall not initiate or forward XMPP TCP/5222 and TCP/5223 (legacy XMPP SSL XMPP client-to-server) outbound packets.

NOTE: This is the XMPP client-to-server connection. All outbound connections should be XMPP server-to-server. Inbound connections may allow for both server to server and client-to-server.

[Required: FY12] The IM and Chat systems shall be configurable to disable Peer-to-Peer (P2P) communications.

NOTE: This requirement is not applicable if P2P application has been authorized for use by the DAA.

[Required: FY12] All Presence/Awareness, IM, and Chat servers shall encrypt all server-to-server communications.

[Required: FY12] All IM traffic (client-to-server and server-to-client) shall use FIPS 140-2 (level 1) cryptographic modules.

[Required: FY12] All Presence/Awareness, IM, and Chat servers shall be capable of using DoD PKI certificates for authentication as defined in UCR 2008 Section 5.4, IA Requirements.

[Required: FY12] All Presence/Awareness, IM, and Chat servers shall be capable of logging all user and system events.

[Required: FY12] Chat servers shall be capable of logging virtual room entrance events, virtual room exit events, and virtual meeting tools used.

[Required: FY12] IM and Chat servers shall store system logs offline.