

TABLE OF CONTENTS

<u>SECTION</u>	<u>PAGE</u>
SECTION 6 UNIQUE CAPABILITIES AND REQUIREMENTS.....	1469
SECTION 6.1 UNIQUE TACTICAL REQUIREMENTS.....	1469
6.1.1 Introduction.....	1469
6.1.1.1 Purpose.....	1469
6.1.1.2 Applicability	1469
6.1.1.3 Definitions	1470
6.1.2 Circuit-Switched-Based Deployable Network Designs and Components	1470
6.1.2.1 Switching System Arrangements.....	1470
6.1.2.2 Tactical Voice Quality	1470
6.1.3 Deployable Voice Exchanges	1470
6.1.3.2 Deployable Voice Exchange Requirements	1472
6.1.3.3 Preset Conferencing.....	1472
6.1.3.4 Tactical Routing and Numbering.....	1472
6.1.3.5 Announcements	1473
6.1.3.6 DVX Network Traffic Management Operating System (NTMOS).....	1473
6.1.3.7 Data Quality	1474
6.1.3.8 Configuration Management	1474
6.1.3.9 Line Timing Mode	1474
6.1.4 Tactical-Network Element Requirements.....	1474
6.1.4.1 Tactical Network Element General Requirements	1474
6.1.4.2 Tactical Network Element Time Division Multiplexing Requirements	1476
6.1.4.3 Tactical Network Element Internet Protocol Requirements	1476
6.1.4.4 Encapsulated Time Division Multiplexing Requirements	1477
6.1.4.5 Carrier Group Alarms	1477
6.1.4.6 Long-Local Requirements	1477
6.1.4.7 Proprietary IP Trunk Requirements.....	1478
6.1.4.8 Secure Call Handling.....	1478
6.1.4.9 Voice Packet Multiplexing	1479
6.1.5 Tactical Local Area Networks	1479
6.1.5.1 Overview.....	1479
6.1.6 Deployed Cellular Voice Exchange System (DCVX) Requirements.	1479
6.1.6.1 Introduction and Purpose	1479

FOR OFFICIAL USE ONLY

Unified Capabilities Requirements 2008

Table of Contents

6.1.6.2	Applicability	1480
6.1.6.3	Policy and Reference Documents	1480
6.1.6.4	DCVX System Overview.....	1481
6.1.6.4.1	DCVX Components	1481
6.1.6.5	DCVX Operation	1482
6.1.6.5.1	Subtended Deployment Connection	1482
6.1.6.5.2	Direct DSN Deployment Connection	1482
6.1.6.5.3	Networked DCVX Deployment.....	1484
6.1.6.5.4	Stand-Alone DCVX Deployment	1484
6.1.6.6	General Description of Cellular Mobile Features and technologies	1485
6.1.6.6.1	Priority Access Service (PAS)/Wireless Priority Service (WPS)	1485
6.1.6.6.2	DOD GSM Cellular Band.....	1485
6.1.6.6.3	Precedence and Preemption	1486
6.1.6.6.4	Code Division Multiple Access (CDMA) Mobile Systems.....	1487
6.1.6.6.5	Global System for Mobile Communications (GSM) Mobile Systems	1487
6.1.6.6.6	Secure Communications Interoperability Protocol (SCIP).....	1487
6.1.6.7	DCVX Requirements Terminology	1487
6.1.6.8	DCVX General Requirements	1487
6.1.6.8.1	Coverage and Signaling Strength.....	1487
6.1.6.8.2	Protocol/Format	1488
6.1.6.8.3	MOS and Measuring Methodology	1489
6.1.6.8.4	Availability	1489
6.1.6.8.5	Encryption.....	1489
6.1.6.8.6	Calling Features	1490
6.1.6.8.6.1	Call Waiting Feature Requirement.....	1490
6.1.6.8.6.2	Three-Way Calling (TWC) Requirement.....	1490
6.1.6.8.6.3	Conference Calling	1491
6.1.6.8.7	Roaming.....	1491
6.1.6.8.8	Precedence and Preemption	1491
6.1.6.8.9	Precedence Capability Terminal Device Activation/deactivation.....	1492
6.1.6.8.10	Precedence and Preemption Calling Features.....	1492
6.1.6.8.10.1	Precedence CW.....	1492

	6.1.6.8.10.2	Precedence TWC	1493
	6.1.6.8.10.3	Precedence Conference Calling.....	1494
	6.1.6.8.10.4	Voice Mail	1494
6.1.6.8.11	Management Capabilities for Terminal Devices.....		1495
6.1.6.9	Terminal Device Specific Requirements		1495
	6.1.6.9.1	Terminal Device Requirements	1495
	6.1.6.9.2	Terminal Device Signaling	1496
	6.1.6.9.3	Terminal Device Frequency Band Support..	1496
	6.1.6.9.4	Terminal Device Encryption.....	1496
	6.1.6.9.5	Terminal Device Battery Requirements.....	1497
	6.1.6.9.6	Terminal Device Secure Call Handling	1497
	6.1.6.9.7	Terminal Device display/alerting features ...	1497
6.1.6.10	Base Station Subsystem (BSS) Specific Requirements		1498
	6.1.6.10.1	Signaling	1498
	6.1.6.10.2	Strength.....	1498
	6.1.6.10.3	Protocol/Format	1498
	6.1.6.10.4	Coverage	1498
	6.1.6.10.5	Preemption	1499
6.1.6.11	Deployed Mobile Switching Center (DMSC) Specific Requirements		1499
	6.1.6.11.1	Visitor Location Register	1499
	6.1.6.11.2	Home Location Register	1499
	6.1.6.11.3	Equipment Identity Register	1500
	6.1.6.11.4	Terminal Device Authentication Center	1500
	6.1.6.11.5	Mobile Switching Office Functions and Features	1500
	6.1.6.11.5.1	MSO MLPP Trunks and Interfaces.....	1500
	6.1.6.11.5.2	Non-MLPP Networks Support.....	1502
	6.1.6.11.5.3	Call Handling	1502
6.1.6.12	Security		1502
6.1.6.13	DCVX Network Traffic Management Operating System (NTMOS).....		1502
6.1.6.14	Submission of Wireless Systems to UCCO for DSN Connection Request		1503

THIS PAGE INTENTIONALLY LEFT BLANK

**SECTION 6
UNIQUE CAPABILITIES AND REQUIREMENTS**

UCR 2008 Section 6 contains requirements that are unique to Tactical Systems (Section 6.1) and Classified Systems (Section 6.2). The unique requirements are modifications to, or additions to the overall requirements defined in UCR 2008, Section 5.

THIS PAGE INTENTIONALLY LEFT BLANK

SECTION 6.1 UNIQUE TACTICAL REQUIREMENTS

6.1.1 Introduction

This section of UCR 2008 defines unique tactical requirements. UCR 2008 Section 5.1 provides the general definition of requirements terminology used. Tactical requirements that are common to strategic requirements for Deployable Voice Exchange (DVX) systems are set forth in UCR 2008 Section 5.2. The DVX requirements specified in this section supersede any similar requirements specified in UCR 2008 Section 5.2.

This section was created by the Executive Agent for Theater Joint Tactical Networks (EA-TJTN) to identify the tactical requirements in consonance with responsibilities assigned by the Assistant Secretary of Defense for National Information Infrastructure (ASD (NII)). In addition, the U.S. Military Communications-Electronics Board (MCEB) tasked the Theater Joint Tactical Networks Configuration Control Board (TJTNCB) to develop tactical interoperability requirements as certification criteria for joint networked-communications systems. In pursuing acquisition initiatives, combatant commander (COCOMs), military services, and defense agencies shall use this section as a guideline for the purchase of Commercial Off-The-Shelf (COTS) equipment, as well for the development of systems that need to interface in deployed networks. The tactical networked-communications community of the DoD shall adhere to this section in order to comply with DoDI 8100.3, “DoD Voice Networks.”

6.1.1.1 Purpose

The purpose of this section is to define the unique tactical requirements that are not contained in UCR 2008 Section 5.2 and the strategic requirements that need to be modified in order to support tactical users. This section consolidates interoperability certification requirements to the maximum extent possible and incorporates them as part of requirements for the overarching Global Information Grid (GIG) in support of network-centric warfare. This section provides guidance for satisfying the certification requirements for tactical voice systems employed as part of an Operational Area Network (OAN), which is the deployed extension of the GIG. This section also defines other UCR elements applicable to the tactical community, and serves as a ready-reference to be used by the Joint Interoperability Test Command (JITC) when writing the tactical annex to the Generic Switch Test Plan (GSTP).

6.1.1.2 Applicability

The requirements in UCR 2008 Section 5.2 apply to DVX, COTS (DVX-C), DVX – Legacy (DVX-L), and Tactical Network Elements (T-NEs) as expanded and modified in this section. The expanded and modified requirements for DVX-C specified in this section take precedence

Section 6.1 – Unique Tactical Requirements

over requirements defined in UCR 2008 Section 5.2. The requirements further delineated in this section apply to network elements (NEs), LANs when used in deployed tactical environments, and Deployed Cellular Voice Exchange (DCVX) Systems.

6.1.1.3 Definitions

Definitions and Acronyms are provided in UCR 2008 Section A1, Acronyms, Abbreviations, Glossary and references.

6.1.2 Circuit-Switched-Based Deployable Network Designs and Components

6.1.2.1 Switching System Arrangements

[Figure 6.1-1](#) depicts how a DVX typically connects into the overall DSN system design. The figure does not stipulate all connections and components that may be applicable.

Both the Private Branch Exchange (PBX) Type 1 and PBX Type 2 are subordinate switches that can be used in the deployed environment subtended to a DVX switch consistent with authorization from the appropriate connection approval authority. A DVX also may be subordinate to another DVX switch.

6.1.2.2 Tactical Voice Quality

The desired objective for tactical voice quality is a Mean Opinion Score (MOS) of 4.0 or greater, but it is realized that the network may operate under less than ideal conditions. The requirements provided in the following paragraphs are the minimally acceptable values under the conditions specified. The MOS calculation will assume the use of G.729 with 20 ms samples for the purpose of SLAs.

6.1.3 Deployable Voice Exchanges

The DVX is either a deployable commercial switch (DVX-C) or tactical legacy system (DVX-L). The DVXs have End Office (EO) and Tandem switch (TS) capabilities which includes Military Unique Features (MUFs), which are not limited to Multilevel Precedence and Preemption (MLPP). A DVX has the technical capability to connect to the DSN via a Standardized Tactical Entry Point (STEP)/Teleport location or directly to a DSN TS, MFS, EO switch, or Small End Office (SMEO) switch. Typically, a DVX does not:

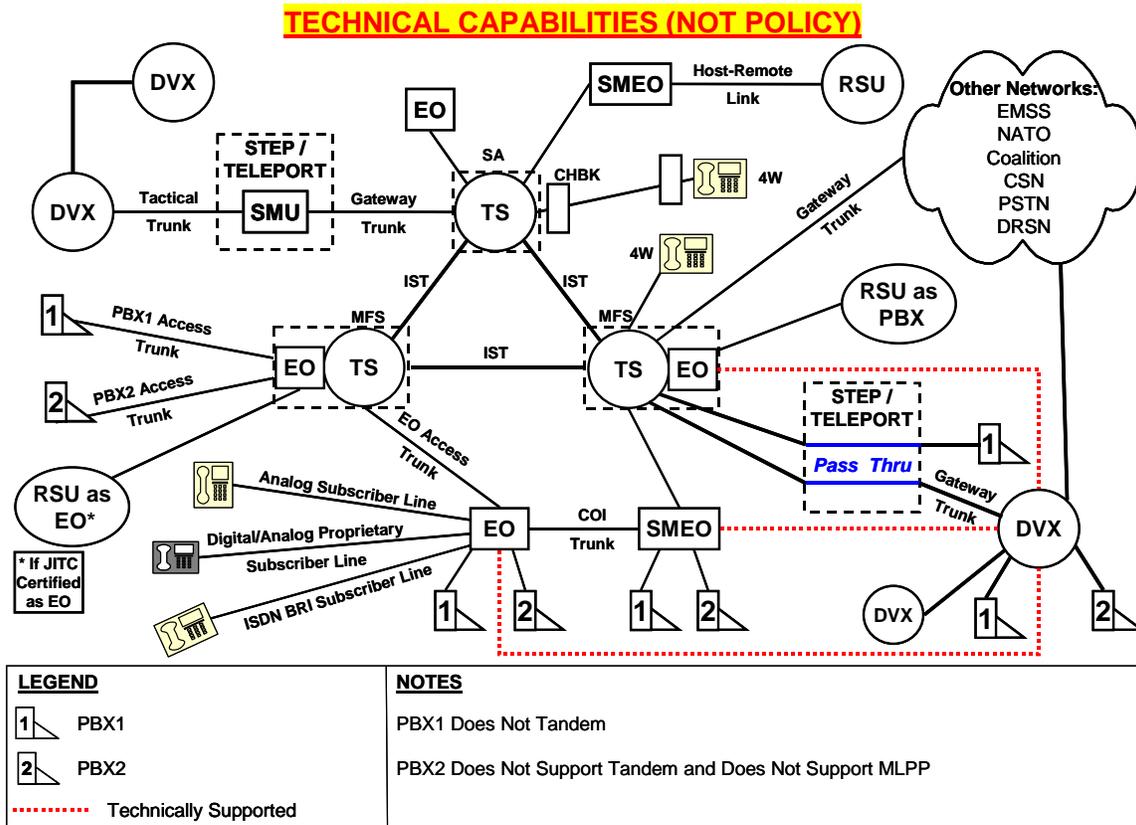


Figure 6.1-1. DSN Design with DVX Components

- Provide full DSN Network Traffic Management control capability.
- Support Common Channel Signaling System Number 7 (CCS7) signaling.
- Support the Communications Assistance to Law Enforcement Act (CALEA).

A DVX offers only limited performance reporting, and is not intended to be a permanent part of the DSN infrastructure. Rather, it is intended to fulfill an operational need as long as the mission requirement exists.

The DVX-L is a Government-deployable legacy voice switching system, such as the Common Baseline Circuit Switch (CBCS) and Unit Level Circuit Switch (ULCS) that shall meet the requirements contained in the current edition of Chairman of the Joint Chiefs of Staff Manual (CJCSM) 6231.02, “Manual for Employing Joint Tactical Communications Systems, Joint Voice Communications Systems,” 1 August 1998. Detailed functional descriptions are provided in the TM 11-5805-681-12 series, “Operator’s and Organizational Maintenance Manual for Central Office, Telephone, Automatic AN/TTC-39(V)2”; or Reference Guide for Nodal Manager, “ESOP and Global Edition,” Version 5.0, September 2001, or Reference Guide for Nodal Manager, “THDSN and SSS Edition,” Version 5.0, September 2001.

Section 6.1 – Unique Tactical Requirements

6.1.3.2 Deployable Voice Exchange Requirements

The technical requirements specified in UCR 2008 Section 5.2, lists the specific requirements of the DVX(s). These requirements are similar to the SMEO requirements in UCR 2008 Section 5.2 in most instances. The specific DVX (i.e., DVX-C and DVX-L) technical requirements are delineated in UCR 2008, Section 5.2 with the following exceptions:

6.1.3.3 Preset Conferencing

[Required: DVX-C, DVX-L] The DVX shall meet all preset conferencing requirements contained in UCR 2008 Section 5.2.1.6, Conferencing, and associated subparagraphs with the following exceptions:

1. The DVX shall provide four (4) separate bridges with each bridge having the capacity for one (1) originator and three (3) conferees.
2. Each bridge shall have the capability to function as the “Primary,” or “Secondary,” or “Alternate” bridge that interconnects to other bridges, which supports up to a maximum of ten (10) conferees using all four (4) 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 three (3) switch address numbers per bridge. Such address numbers could be a combination of subscriber lines and other conference bridge access numbers.
4. The number assignments shall be made in accordance with the DSN World Wide Dialing and Numbering Plan (WWDNP), Defense Information Systems Agency Circular (DISAC) 310-255-1, “DSN User Services Guide,” and the Global Block Numbering Plan, as appropriate.

6.1.3.4 Tactical Routing and Numbering

[Required: DVX-C, DVX-L] The switch shall be equipped and operationally capable of the dialing format for User Dialing Format to Coalition Forces as defined in Standard NATO Agreement (STANAG 4214), “International Rating and Directory for Tactical Communications Systems,” Edition 3, Version T, 07 January 2005, or current edition.

[Conditional: DVX-C, DVX-L] The switch outpulsing digit format for integrated services digital network (ISDN) basic rate interface (BRI) signaling (i.e., NI-1/2 and American National Standards Institute (ANSI) T1.619a) shall utilize the UCR SMEO ISDN BRI requirement, as stated in UCR 2008 Section 5.2, Table 5.2.12-3, BRI Access, Call Control, and Signaling.

6.1.3.5 Announcements

[**Conditional: DVX-L**] The Precedence Access Limitation Announcement (PALA) as shown in UCR 2008 Table 5.2.2-1 Announcements is required to meet draft version, STANAG 4214, “International Rating and Directory for Tactical Communications Systems,” Edition 3, Version T, 07 January 2005, or current edition.

6.1.3.6 DVX Network Traffic Management Operating System (NTMOS)

[**Required: DVX-C, DVX-L**] The DVX switching systems shall provide network management data to the administering network management console via one of the three following physical interfaces:

1. Ethernet/Transmission Control Protocol (TCP)/IP (Institute of Electrical and
2. Electronics Engineers (IEEE) 802.3).
3. Serial (RS-232)/Asynchronous.
4. Serial/Synchronous (X.25 and/or BX.25 Variant).

All network management data that is collected, and configurable features and functions shall, at a minimum, be accessible through one of these interfaces. The DSN switch shall 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 shall be transmitted to the network management console in such a method as to allow for storage, recovery, and transfer of the information to or from digital media storage, and to allow for printing and/or screen display using methods, such as American Standard Code for Information Interchange (ASCII), binary, or hexadecimal data.

The data channels shall be used for and, as such, shall be capable of providing:

1. Alarm/Log Data
2. Performance Data (e.g., traffic data)
3. Accounting Data (e.g., Call Detail Recording (CDR))
4. Switch access (to perform switch data fill administration and network controls)

Section 6.1 – Unique Tactical Requirements

6.1.3.7 Data Quality

[Required: DVX-L] The DVX-L switching systems shall meet the data quality and data presentation requirements for R-1 through R-6 Reports identified in the TM 11-5805-681-12 series, “Operator’s and Organizational Maintenance Manual for Central Office, Telephone, Automatic AN/TTC-39(V)2”; and/or Reference Guide for Nodal Manager, “ESOP and Global Edition,” Version 4.0, January 1998. The collection shall meet the 15, 30, or 60 minute and daily reporting requirements.

6.1.3.8 Configuration Management

[Required: DVX-L] Configuration management shall be provided in accordance with (IAW) UCR 2008 Section 5.2.8.4.

6.1.3.9 Line Timing Mode

[Required: DVX-C, DVX-L] The DVX shall support line timing modes as defined in UCR 2008 Section 5.2.10.1.1 and Telcordia Technologies GR-1244-Core, “Clocks for the Synchronized Network: Common Generic Criteria,” Issue No. 1, 3 May 2005, except for the Proprietary Internet Protocol Trunk (PIPT) IP interface as described in UCR 2008 [Section 6.1.4.7](#), Proprietary IP Trunk Requirements.

6.1.4 Tactical-Network Element Requirements

[Required] The T-NEs shall meet all network element requirements specified in UCR 2008 Section 5.2.12.5, DSN Strategic Network Element Generic Requirements, except as modified by the following paragraphs. The T-NEs shall be tested under a simulated tactical environment using the OAN architecture framework and the following parameters:

1. Inclusion of satellite-based transmission links
2. A random bit error rate (BER) of 1×10^{-5}

6.1.4.1 Tactical Network Element General Requirements

[Conditional] The T-NEs may include voice compression, as specified in UCR 2008 Section 5.2.12.5.5.1, General Requirements, to include the following additional compression standard: International Telecommunications Union – Telecommunication (ITU-T) Recommendation G.723.

[Conditional] Network element latency requirements for various codecs are defined in UCR 2008 Section 5.2.12.5, DSN Strategic Network Element Generic Requirements. The T-NE allows for one additional codec, G.723.1. The latency introduced by a single T-NE utilizing the G.723.1 codec shall be less than 90 ms. The latency introduced by a pair of T-NEs utilizing the G.723.1 codec shall be less than 180 ms.

[Required] Voice calls placed through a set of T-NEs shall support a minimum MOS of 3.6 or better as measured in any 5-minute interval using the Perceptual Speech Quality Measure (PSQM) testing standard.

[Required] The introduction of a T-NE shall not cause the E2E digital bit error rate to degrade by more than 0.03 percent over an 8-hour period. This value does not include the application of Forward Error Correction (FEC) but is the minimum acceptable value for tactical transmission before FEC is applied.

[Required] The T-NE (when implemented in pairs) shall apply error correction to correct the errors interjected by the transport network between the two T-NEs such that the resulting bit error rate level of the external facing T-NE interface shall be better than 1×10^{-5} as measured over an 8 hour period.

[Required] The T-NE shall allow a minimum modem transmission speed of 2.4 kbps per second (kbps) across the associated network element(s).

[Required] The T-NE shall allow a minimum facsimile transmission speed of 9.6 kbps across the associated network element(s).

[Required] The network element shall assure congestion within 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:

1. A dynamic load control signal (e.g., contact closure) shall be provided to the DSN switch in accordance with UCR 2008 Section. 5.2.12.5.5.1.1.2 Congestion Control.
2. A software capability in limiting the provisioning the input and/or output interfaces such that makes congestion impossible even under the worst congestion scenario.
3. Congestion is not possible in the network element by nature of its functioning (e.g., a TDM multiplexer or transcoder).

6.1.4.2 Tactical Network Element Time Division Multiplexing Requirements

[Conditional] The T-NE shall support at least one of the interfaces listed in UCR 2008 Section 5.2.12.5, DSN Strategic Network Element Generic Requirements. To be certified for use, TDM interfaces shall meet the interface requirements for that specified interface. For interfaces provided, congestion control shall be provided as specified in UCR 2008 Section 5.2.12.5.5.1, General Requirements.

6.1.4.3 Tactical Network Element Internet Protocol Requirements

Figure 6.1-2 shows how IP can be used to provide transport for both T-NEs and Virtual Tactical Network Elements (VT-NEs).

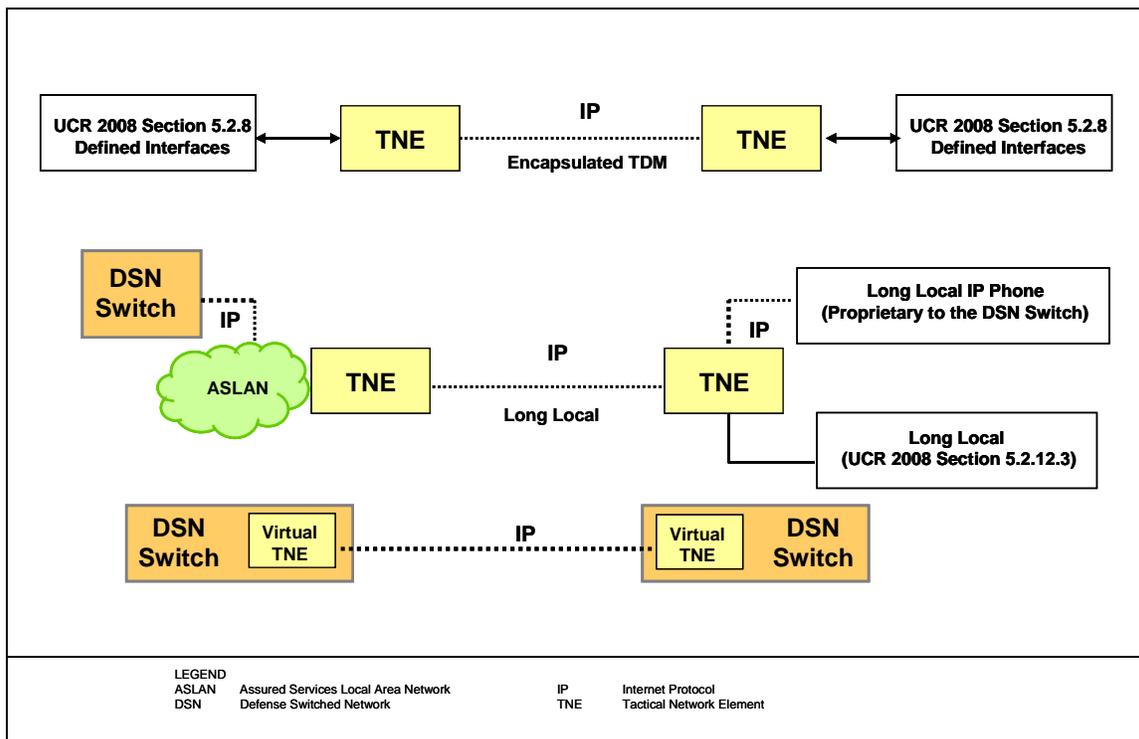


Figure 6.1-2. T-NE Connectivity Using IP Transport

[Conditional] The T-NEs may use IP as a means to transport voice communications between T-NEs. Interfaces supporting IP shall meet the appropriate specifications for that physical interface as stipulated in the latest DoD IT Standards Registry (DISR) Baseline Release. The IP transport of voice services across T-NEs shall be accomplished through any one of three methods: encapsulated TDM, long local, or PIPT.

[Required] For any IP transport methods used, T-NEs using IP interfaces shall meet the following parameters:

1. The addition of T-NEs shall meet the latency criteria specified in UCR 2008 [Section 6.1.4.1](#), Tactical Network Elements General Requirements.
2. The addition of a T-NE shall not cause jitter measured from ingress to egress to increase by more than 5 ms averaged over any 5-minute period.
3. The addition of a T-NE shall not cause packet loss measured from ingress to egress to increase by more than 0.05 percent averaged over any 5-minute period.

6.1.4.4 Encapsulated Time Division Multiplexing Requirements

The T-NEs that employ encapsulated TDM shall meet all the following requirements.

[Required] The T-NE shall use either differentiated services or integrated services to provide preferential treatment over IP transport.

[Required] The T-NE shall provide an IP bandwidth reservation/allocation mechanism to allow for the user-specified allocation of bandwidth to support the full non-blocking voice services requirement.

[Required] The T-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-to-End Requirements, and a capability to limit the provisioning of input and output interfaces such that congestion is impossible under the worst transport congestion scenario.

6.1.4.5 Carrier Group Alarms

[Required] The T-NE shall be able to propagate Carrier Group Alarms (CGAs) in accordance with UCR 2008 Section 5.2.6, System Interfaces, upon physical loss of the ingress TDM interface. Voice switching systems, DSN or DVX, shall receive the proper CGAs from the T-NE upon loss of the IP transport link between T-NEs.

6.1.4.6 Long-Local Requirements

The T-NEs that provide a long local shall meet all the following requirements:

Section 6.1 – Unique Tactical Requirements

[Required: T-NE] The T-NE shall provision features and functions to support the long-local device.

[Required: T-NE] The T-NE shall allocate enough bandwidth to support the long-local device to ensure assured services and non-blocking requirements are met.

6.1.4.7 Proprietary IP Trunk Requirements

[Conditional] Virtual T-NEs that employ PIPT shall meet all the requirements specified in the following paragraphs:

[Conditional] The DVX Virtual T-NE may use Proprietary IP signaling for this solution, and this interface shall support E2E ANSI T1.619a features and functions IAW UCR 2008 Section 5.2.2.7 (i.e., Precedence, Preemption, MLPP Service Domain, Look Forward for Busy, Network Identifiers, and Coding Standard). The PIPT shall meet the appropriate specifications for IP voice signaling method protocols (i.e., H.323, SIPv2), as stipulated in the latest DISR Baseline Release to establish the virtual IP trunk session. Until a complete set of standards exists for MLPP over IP, initially vendors may implement proprietary protocols across the PIPT to ensure the complete MLPP functionality as detailed in UCR 2008 Section 5.2.2.7, ISDN MLPP PRI, is provided to the DSN IP telephony subscriber.

[Conditional] For DVX Virtual T-NE switches that do not support MLPP, this interface shall support end-to-end ISDN PRI NI 1/2 features and functions (i.e., Bearer, Calling Number Delivery, etc.). The PIPT shall meet the appropriate specifications for IP voice signaling method protocols (i.e., H.323, SIPv2), as stipulated in the latest DISR Baseline Release to establish the virtual IP trunk session.

6.1.4.8 Secure Call Handling

[Conditional] The T-NE when equipped with a modem relay-like capability to more efficiently process secure (Secure Telephone Unit, Third Generation [STU-III] or Secure Communications Interoperability Protocol (SCIP)) calls may be through either a V.150.1 implementation or via proprietary methods.

If the T-NE implements V.150.1, it shall be compliant with the NSA SCIP-215 “U.S. SCIP) over IP Implementation Standard and Minimum Essential Requirements (MER) Publication,“ Revision 2.0, October 3, 2007.

[Required] The secure call shall complete successfully 85 percent of the time when used in the tactical environment.

6.1.4.9 Voice Packet Multiplexing

[Conditional] A T-NE that is equipped with voice packet multiplexing, where individual small IP voice packets (either from the same or multiple sources) may be combined into a single larger IP packet. The T-NE shall be configurable to allow the operator to specify the maximum latency and/or packet size to provide flexibility in the actual implementation. The intent is to allow the system to trade off additional latency incurred by this process for the gain in packet processing efficiency.

6.1.5 Tactical Local Area Networks

6.1.5.1 Overview

Tactical Operations Centers (TOCs) and other deployed enclaves operate under austere conditions, rely on a tactical power supply/grid, and may be restrictive in the size, weight, and packing requirements. The Tactical LAN and the backbone and transmission components operate from the same tactical power source. It is extremely difficult to approach the availability and power backup requirements mandated on the strategic infrastructure with its commercial-grade power supply and relatively fixed operating environment.

The ASLAN requirements defined in UCR 2008 Section 5.3.1 represent the optimal LAN design and tactical users are encouraged to implement their requirements whenever possible. However, operational realities often preclude the deployment of highly redundant components and multiple backup power sources.

6.1.6 Deployed Cellular Voice Exchange System (DCVX) Requirements

6.1.6.1 Introduction and Purpose

The following sections describe the requirements that shall be met by all Deployed DCVX systems in order for them to be certified and used in the OAN tier of the Global GIG. Requirements are defined at the system level as well as for the various components that make up the cellular system, including protocol requirements. The DCVX is a cellular system with military-unique features and therefore is not the same as commercially deployed Mobile Cellular Systems (MCS).

It is recognized that not all components may be needed for a specific application. The requirements discussed in this Section are similar to those of the SMEO, DVX, or PBX1 and dependent on the network configuration and specific authorized gateway connection.

Section 6.1 – Unique Tactical Requirements

6.1.6.2 *Applicability*

The requirements within this section are applicable to:

1. All DCVX systems that connect directly or indirectly to the DISN voice systems including the DSN, DRSN Secure Phone Gateways, and/or commercial PSTN.
2. Procured or leased cellular systems that connect to any DISN service gateway. Commercial cellular services are not allowed to be connected to DISN service gateways.
3. Procured or leased cellular systems using leased cellular frequencies that connect to any DISN service gateway.

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 a conflict, the explicit requirements of UCR 2008 take precedence over the explicit or implicit requirements of any other requirements document except for those requirements specified in the documents listed in [Section 6.1.6.3](#), Policy and Reference Documents.

6.1.6.3 *Policy and Reference Documents*

The following policy and instruction documents will, in conjunction with UCR2008, be used as basis for APL certification:

1. Policy for the use of commercial wireless devices, services, and technologies in the DoD GIG, as outlined in DoD Directive 8100.2. This directive further promotes joint interoperability using open standards throughout DoD for commercial wireless services, devices, and technological implementations.
2. Wireless Priority Service (WPS) Industry Requirements for the Full Operating Capability (FOC) for CDMA-Based Systems – Home Location Register (HLR), Issue 1, June 4, 2004.
3. The WPS Industry Requirements for the FOC for GSM-Based Systems – Issue 2, January 2004.
4. 3G TS 24.067 V3.0.0 (1999-05), 3RD Generation Partnership Project; Technical Specification Group core Network; enhanced MLPP (eMLPP) – Stage 3.

6.1.6.4 DCVX System Overview

DCVX systems provide wireless mobile communication services with military-unique features and draw their strategic services by means of approved DoD authorized gateway switching systems only. The DCVX can be connected to a DVX-C or connected directly to the DSN via tactical communications as described in CJCSM 6231.01b. DCVX systems may also be interconnected with other cellular telephone systems, excluding commercial systems unless the commercial system is procured or leased for DoD usage and is operating in isolated mode from other commercial cellular systems. The DCVX may also be connected to both the DSN and the systems described above simultaneously to E2E MUF such as MLPP.

The DCVX, when placed in a joint tactical environment will have the capability to connect to DSN and between other DCVXs and DVXs, via tactical voice, using UCR-defined protocols such as ISDN PRI, MLPP PRI (T1.619a) and/or CCS7. The CCS7 over IP using IETF SIGTAN may be used only in connecting DCVXs together on DoD IP Networks within the Tactical OAN. However, only ISDN PRI may connect to the commercial PSTN and/or other Non-Government networks. A DCVX system may also be configured to interconnect at the network transmission level with other DCVX systems to provide roaming capability outside the local home base cellular network for supported Terminal Devices.

Cellular Terminal Devices, often referred to as Mobile Subscribers Cellular Handsets, PDAs, Blackberries, and any other user cellular end item devices commercial or government developed, may connect to commercial cellular systems when operating outside the transmission range of the DCVX.

Additionally, the Cellular Terminal Devices may have the capability to interface with other wireless networks (IEEE 802.11, and IEEE 802.16) and Commercial Cellular Service when not supported by a DCVX. Actual employment of this additional Cellular Terminal Device capability will be by Command approval only in the OAN.

6.1.6.4.1 DCVX Components

The DCVX is comprised of three major components with multiple subcomponents and/or devices:

1. Terminal Device(s)
 - a. Cellular /Mobile Handset
 - b. PDA
 - c. Blackberry
 - d. Government Developed Terminal

Section 6.1 – Unique Tactical Requirements

- e. Other Commercial Cellular Devices
2. Base Station Subsystem (BSS)
 - a. Base Transceiver Station (BTS)
 - b. Base Station Controller (BSC)
 - c. Cell Tower(s) with Radio Transceiver(s)
3. Deployed Mobile Switching Center (DMSC)
 - a. Mobile Switching Office (MSO)
 - b. Home Location Register (HLR)
 - c. Visitor Location Register (VLR)
 - d. Authentication Center (AUC)
 - e. Equipment Identity Register (EIR)

6.1.6.5 DCVX Operation

The DCVX functions and provides mobile cellular services similar to standard commercial cellular systems with the addition of MUFs. It is based on a two-way cellular radio system that interconnects cell phones with other cell phones and landline stations. When employed, the DCVX will provide full mobile cellular coverage in designated deployed environments; this includes training, exercise, and operational missions within COCOM AORs or specific geographic areas. User voice, data and related communications via Terminal Devices will be similar to landline wired DSN or commercial services. Except for the inherent characteristics of radio transmission, basic service features between the two systems will be similar and transparent to the users. The DCVX, after full mature architectural implementation, will function as a wireless adjunct and extension of the joint OAN tier of the GIG. The following configurations, illustrated in [Figure 6.1-3](#), define the operational deployment options of a DCVX.

6.1.6.5.1 Subtended Deployment Connection

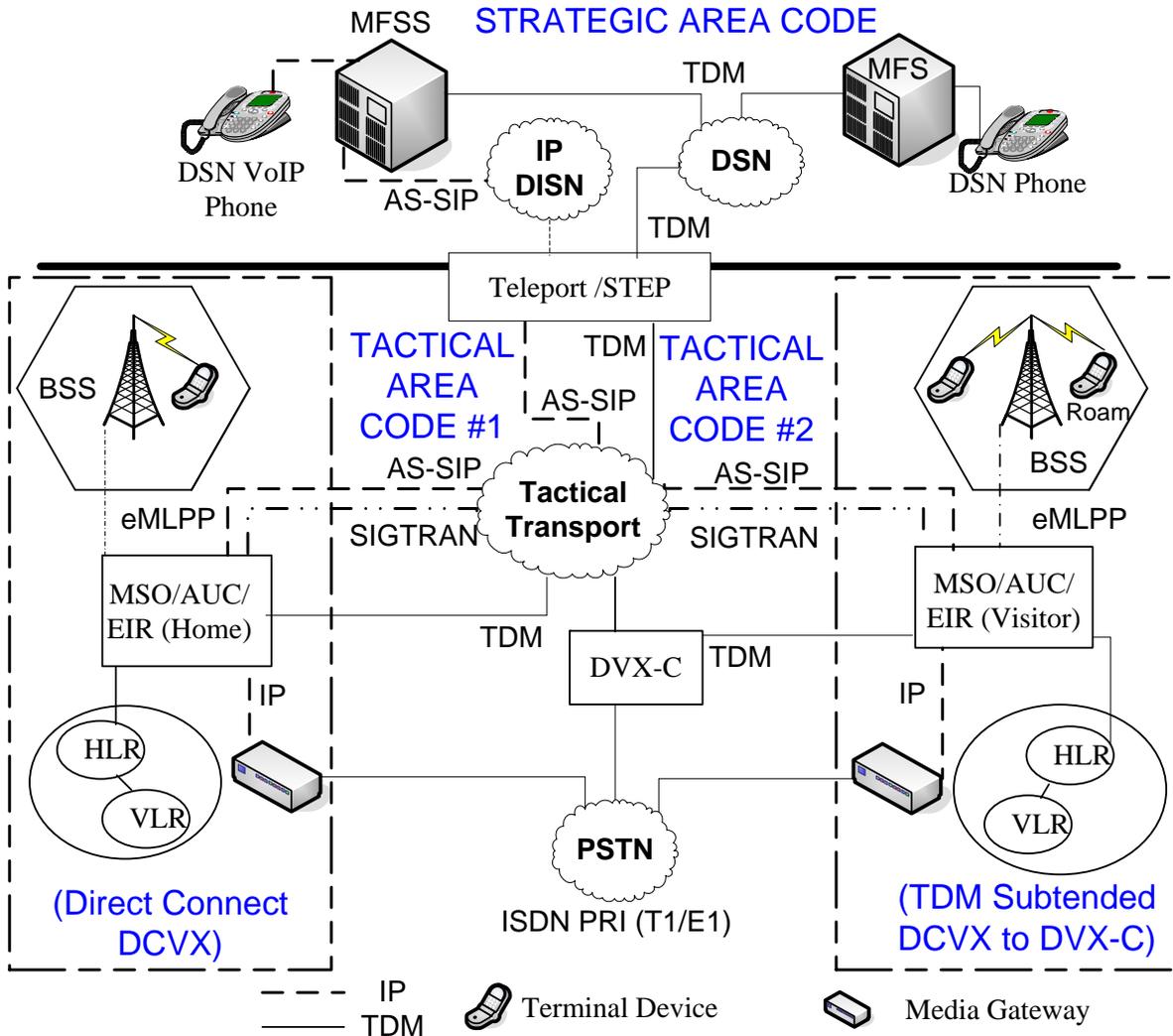
For a “Subtended Deployed Connection”, the DCVX will only interface with DSN voice services utilizing an existing authorized gateway switch, i.e. DVX-C, to connect to the tactical transport network; with the one or more of the following interfaces:

- ISDN PRI (T1/E1)
- MLPP ISDN PRI (T1/E1) [**Conditional**]

6.1.6.5.2 Direct DSN Deployment Connection

For a Direct DSN connection, the DCVX will use the “Direct Connection” configuration to the tactical transport network with one or more of the following interfaces:

**DCVX DSN Connection & Tactical Cellular Roaming
(Direct Connect & Subtended)**



AUC – Authentication Center
 EIR – Equipment Identity Register
 BSS – Base Station Subsystem
 HLR - Home Location Register
 MFS - Multi-Function Switch
 MFSS - Multi-Function Softswitch
 MSO – Mobile Switching Office
 VLR - Visitor Location Register

eMLPP- enhanced Multi-Level Precedence and Pre-emption

Time Division Multiplexed (TDM)
 ISDN PRI - ANSI T1.619, and ITU Q.955.3
 MLPP Pri - ANSI T1.619a & ITU Q.735.3
 CCS7 - ANSI T1.100 Series
Internet Protocol (IP)
 AS-SIP - Assured Service-SIP
 SIGTRAN – IETF RFC 2719+ (OAN Only)

*Note: DCVX can connect either via TDM or IP to the DSN, but not both simultaneously.
 Only ISDN PRI connections allowed to PSTN and/or Non-Government Networks.

Figure 6.1-3 Deployed Cellular Voice Exchange Generic Design

Section 6.1 – Unique Tactical Requirements

- ISDN PRI (T1/E1)
- MLPP ISDN PRI (T1/E1) [Conditional]
- CCS7 [Conditional]
- IP AS-SIP (Signaling and associated bearer channel) [Conditional]

DCVX can directly connect to the DSN by either TDM or IP, but not both simultaneously.

6.1.6.5.3 Networked DCVX Deployment

When a DCVX is deployed in a Networked DCVX configuration, a large deployed unit or multiple deployed units within the tactical OAN may be connected with one or more HLR routing tables configured to support cellular Terminal Device roaming capabilities per the interconnections previously described.

For Networked DCVXs within the Tactical OAN in support of Terminal Device roaming capability, the DCVX configuration to the tactical transport network will be with one or more of the following interfaces:

- ISDN PRI (T1/E1)
- MLPP ISDN PRI (T1/E1) [**Conditional**]
- CCS7 [Conditional]
- IP AS-SIP (Signaling and associated bearer channel) [**Conditional**]
- SIGTRAN (CCS7 over IP) [**Conditional**]

The extent of Terminal Device roaming capability will dependent upon the number and type of interconnections made between the DCVXs within the Tactical OAN and switch lookup routing table updates in the DCVXs themselves.

For all connection variations, the DVCX will connect to the PSTN and/or other Non-Government Networks via TDM ISDN PRI (T1/E1) only.

6.1.6.5.4 Stand-Alone DCVX Deployment

When a DCVX is used in standalone configuration, the only area served is a deployed unit establishing a Joint Task Force (JTF) and its C4 infrastructure. There is no DSN or PSTN access and no roaming beyond the deployed local network unit cell towers of its area of operation. The DCVX operates solely in an isolated mode.

6.1.6.6 General Description of Cellular Mobile Features and technologies

6.1.6.6.1 Priority Access Service (PAS)/Wireless Priority Service (WPS)

Priority access service provides the logical means for authorized mobile users to queue to the front and obtain priority access to the next available channel in a wireless call path. The goal of the WPS is to provide an E2E OAN-wide wireless priority communications capability to key military personnel during natural or man-made disasters. WPS is an enhancement to basic cellular service. The full WPS capability can provide priority handling from mobile call origination, through the network, and all the way to the call destination.

WPS is invoked by keying a special access number (*272) prior to the destination number on cellular instruments that have been class-marked for the WPS feature. A WPS user may be assigned one of five priority levels (1, 2, 3, 4, or 5), with 1 being the highest priority level and 5 being the lowest. Each priority level has user-qualifying criteria that may track that for MLPP in DSN.

When a WPS call is queued for a radio traffic channel – from a cellular user – and no channel is available, the call is queued according to (1) highest PAS priority first, and (2) queue entry time (earliest call first) within the same priority. If the queue for the call sector is full, and the caller's priority is determined to be higher than the level of the lowest priority caller in the queue, then the most recent WPS entry shall be removed, with the new WPS call request queued in accordance with (1) and (2) above.

6.1.6.6.2 DOD GSM Cellular Band

The dedicated DoD Global System for Mobile (GSM) band is from 1755 MHz to 1835 MHz, which is a subset of the commercial DCS-1800 Band. The remaining overnment-owned frequency ranges are 1755 MHz to 1785 MHz for the Uplink and 1805 MHz to 1850 MHz for the Downlink. There are no non-DoD regulatory challenges associated with the use of this GSM band. The band has been approved for exclusive DoD use and is not authorized for use by any other entity. This band will be utilized for both voice and data applications to support unique DoD requirements.

It is understood that the band benefits are only effective in a CONUS environment however, the DoD GSM may be utilized OCONUS with specific host country(s) authorization. The normal DoD frequency allocation process shall be followed to allow system operation within this band and CC/S/A planners must ensure that an alternative solution is available prior to deployment as part of the planning process.

Section 6.1 – Unique Tactical Requirements

6.1.6.6.3 Precedence and Preemption

Precedence and Preemption can only be implemented in a DoD network. This service has two parts- precedence and preemption. Precedence involves assigning a priority level to a call (wireless or wired). Preemption involves the seizing of a communications channel that is in use by a lower precedence level caller, in the absence of an idle channel. In the DCVX, Precedence and Preemption capability is conditional. Precedence and Preemption may be provided by enacting eMLPP or a vendor proprietary version that performs Precedence and Preemption in the DCVX between the Terminal Device and the Cellular Switch. The eMLPP is a cellular version of MLPP. In either version, precedence will be invoked by keying defined digits prior to dialing the destination number on cellular instruments that have been class-marked for this service. Precedence will function jointly in combination with WPS, and will perform E2E as an adjunct to regular MLPP service on the wired DSN. However, in either provided versions, if available in the DCVX, eMLPP or vendor proprietary, the connection to the DSN will be MLPP PRI (T1.619a) and/or CCS7 or AS-SIP.

Mobile systems, as currently designed, provide a maximum of seven (7) priority levels. The two highest levels (A and B) are reserved for network internal use, (e.g., for emergency calls or the network related service configurations for specific voice broadcast or voice group call services). The second highest level (B) can be used for network internal use or optionally, depending on regional requirements, for subscription. These two levels (A and B) can only be used locally, i.e., in the domain of one DCVX. The other five priority levels are offered for subscription and can be applied globally (e.g., on inter switch trunks) if supported by all related network elements, and also for interworking with ISDN networks providing the MLPP service. The seven eMLPP priority levels and their respective mapping to MLPP are defined as follows:

- A** highest, for network internal use
- B** for network internal use or, optionally, for subscription
- 0** for subscription: Flash-Override
- 1** for subscription: Flash
- 2** for subscription: Immediate
- 3** for subscription: Priority
- 4** lowest, for subscription: Routine

Levels A and B shall be mapped to level 0 for priority treatment outside of the DCVX area in which they are applied. The vendor proprietary version will support the 5 Precedence levels as specified for DSN MLPP.

6.1.6.6.4 *Code Division Multiple Access (CDMA) Mobile Systems*

Mobile CDMA technology uses spread spectrum telecommunications techniques in which a signal is transmitted in a bandwidth considerably greater than the frequency content of the original information. The latest technology today is based on 3G that allows high and fast bandwidth is generically called Evolution-Data Optimized (EVDO or EV-DO). This capability supports data usage of the Terminal Device to allow data connections to DoD networks and future possible use of VoIP softphone on Terminal Devices when connected to Commercial Networks for extension of DSN single number presence.

6.1.6.6.5 *Global System for Mobile Communications (GSM) Mobile Systems*

Early technology for GSM allowed the use for Time Division Multiple Access (TDMA) technology. TDMA allows several users to share the same frequency. It is the most popular standard for mobile phones in the world. The ubiquity of the GSM standard makes international roaming very common with "roaming agreements" between mobile phone operators. The latest GSM standard is based on an open standard that is developed by the 3rd Generation Partnership Project (3GPP).

6.1.6.6.6 *Secure Communications Interoperability Protocol (SCIP)*

SCIP is the NSA approved secure voice and data encryption protocol used by DoD, US Government agencies, and civilian authorities. SCIP is also used by NATO and Coalition partners to provide secure voice interoperability between the US and authorized foreign entities. Application of SCIP is described in detail within UCR 2008 Section 5.2.12.6, DoD Secure Communications Devices.

6.1.6.7 *DCVX Requirements Terminology*

Requirements terminology is defined in UCR 2008 Section 5.1.4 General Requirement Language.

6.1.6.8 *DCVX General Requirements*

6.1.6.8.1 *Coverage and Signaling Strength*

[Required] The signal strength shall not be less than the current GSM and CDMA authorized international standards and specifications. GSM and CDMA technology are spectrum based, therefore GSM/CDMA band, coverage, signal strength, and power are the basis for planned "Area of Support." Environment, weather, geography, topography, and adjacent spectrums are

FOR OFFICIAL USE ONLY

Unified Capabilities Requirements 2008

Section 6.1 – Unique Tactical Requirements

elements that must be considered when applying the basis for “Area of Support.” For testing purposes the generic set of parameters presented in [Table 6.1-1](#), shall be utilized for JITC certification either by testing and/or as determined by JITC.

Table 6.1-1. Current Cellular Systems Parameters

DCVX (DMSC, BSS) GSM/GPRS	
Bands	As provided by Standards and/or DoD GSM Cellular Band (e.g. 450 MHz , 850Mhz, 900Mhz, and 1900Mhz)
Specification on Coverage	As provided by Standards: (e.g. ITU-R 2.5G, 3G,3GSM, GSM Edge (www.itu.int/publications)
Distance Transmit/ Receive	Up to 25 miles depending on topology / manmade structures, and frequencies also determine coverage parameters.
DCVX(DMSC, BSS) CDMA	
Bands	As provided by Standards (e.g. 450 MHz , 700Mhz, 800Mhz, 850Mhz, 900Mhz, 1700Mhz, 1800Mhz, 1900Mhz and 2100Mhz)
Specification on coverage	As provided by Standards: (e.g. Telecommunication Industry Association, IS95, 3GPP2, IMT-2000, CDMA 1XRTT, CDMA2000) (www.tiaonline.org)
Distance Transmit/ Receive	Up to 32 miles depending on topology / manmade structures, and frequencies also determine coverage parameters.
Terminal Device	
Bands	As provided by Standards [CDMA/GSM] and/or DoD GSM Cellular (e.g. 450 MHz , 700Mhz, 800Mhz, 850Mhz, 900Mhz, 1700Mhz, 1800Mhz, 1900Mhz and 2100Mhz)
CDMA Specification	As provided by Standards: (e.g. CDMA(IS95), CDMA 2000, CDMA 1XRTT and CDMA 1xEVDO),
GSM Specification	As provided by Standards: (e.g. GSM (GSM 02.07 Tech. Spec.(ver.7.1.0 Rel. 1998)), 2.5G, 3G, 3GSM, GSM Edge)
Distance Transmit/ Receive	Up to 8 mi depending on topology / manmade structures, and frequencies also determine coverage parameters.

6.1.6.8.2 Protocol/Format

[Required] The DCVX shall support at least one or more of the following protocols:

- GSM/GPRS (2.5G, 3G,3GSM, GSM Edge),
- WCDMA
- CDMA2000
- CDMA 1XRTT

- UMTS
- EVDO (or EV-DO)

6.1.6.8.3 *MOS and Measuring Methodology*

[Required] DCVX shall support the minimum MOS scores as defined in Section 5.3.3, Network Infrastructure E2E performance requirement or better as measured in any 5-minute interval using P.862 testing standard. The baseline test environment shall be while operating in an open air-clear obstruction line-of-site environment with the specific requirements as outlined in [Table 6.1-1](#). Based on the results, the estimated MOS performance range will be extrapolated and provided in the vendor LoC based on the Base Station Antenna operating at or near full power mode and at a minimum operating height of 80 ft. The values provided in the vendor LoC will be included in the APL report. Refer to UCR 2008 [Section 6.1.6.14](#), Submission of Wireless Systems to UCCO for DSN Connection Request, concerning guidelines on submitting the cellular engineering analysis package.

6.1.6.8.4 *Availability*

[Required] The DCVX shall have an availability of 99.99 which includes schedule maintenance.

6.1.6.8.5 *Encryption*

[Required] The DCVX must provide appropriate radio and network transport bandwidth to support secure calls via SCIP, other NSA accredited encryption scheme(s), and/or other required accredited encryption schemes as defined in the appropriate Security Technical Implementation Guides (STIGs) for cellular to support Terminal Device Encryption Requirements in UCR 2008 [Section 6.1.6.9.4](#).

[Required] The DCVX shall support SCIP, other NSA accredited encryption scheme(s) and/or required accredited encryption schemes as defined in the appropriate STIGs for cellular. STIG required encryption shall be provided to secure the wireless call as a minimum if SCIP and/or other NSA accredited encryption schemes are not provided. DCVX that supports SCIP, a.k.a Terminal Device, will be required to go secure E2E with another SCIP phone and/or via a SCIP Gateway if AS-SIP is used while the DCVX supports the establishment and maintaining the secure call.

[Conditional] The DCVX may have the capability to provide secure SCIP gateway functions.

Section 6.1 – Unique Tactical Requirements

6.1.6.8.6 *Calling Features*

6.1.6.8.6.1 Call Waiting Feature Requirement

The Call Waiting (CW) feature interacts with MLPP. If precedence and preemption capability is available in the DCVX, the MLPP interactions must meet the requirements described in UCR 2008 [Section 6.1.6.8.10.1](#), Precedence Call Waiting. CW 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. A CW tone is only audible to the line with the Call Waiting feature activated.

CW [Required] The CW feature shall generate a call waiting tone only audible to the line with the CW feature activated.

Cancel CW [Required] The Cancel CW feature is required when CW is active. The user must be able to cancel the CW service. Cancel CW is a feature that allows the user with CW service to inhibit the operation of CW for one call. The user dials the Cancel CW code, obtains recall dial tone, and places a call normally. During this call, the CW service shall be inactive so that anyone calling the CW user shall receive the normal busy treatment, and no CW tones shall interrupt the user's call.

6.1.6.8.6.2 Three-Way Calling (TWC) Requirement

The TWC feature interacts with MLPP. If Precedence and Preemption capability is provided in the DCVX, the MLPP interactions must meet the requirements described in UCR 2008 [Section 6.1.6.8.10.2](#), Precedence TWC.

[Conditional] TWC 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 places the other party on hold, receives recall dial tone, dials the third party's telephone number, and then takes the 1st line off of hold to establish the TWC connection. This may occur any time after the completion of dialing the second number joining the TWC. After the TWC connection has been established, the customer with the service activated may disconnect the last party added. 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.

[Conditional] The Terminal Device may support signaling to allow TWC.

6.1.6.8.6.3 Conference Calling

The Conference Calling feature is conditional because it interacts with MLPP. If precedence and preemption and conference calling capability are provided in the DCVX, the MLPP interactions must meet the requirements described in UCR 2008 [Section 6.1.6.8.10.3](#), Precedence Conference Calling.

[Conditional] 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.

[Conditional] The Terminal Device may support signaling to allow conference calling.

6.1.6.8.7 Roaming

[Conditional] The DCVX system may only support roaming to one or more DCVXs within the tactical OAN. Network connections with commercial cellular systems in support of roaming are not allowed. *Roaming shall meet the Global Block Numbering Plan (GBNP) requirements as specified for the DVX-C* in UCR 2008 [Section 6.1.3.4](#), Tactical Routing and Numbering.

6.1.6.8.8 Precedence and Preemption

The DCVX may support preemption and precedence under the following conditions:

[Conditional] The DCVX may support the cellular version of MLPP called eMLPP and/or a proprietary methodology. When Precedence and Preemption are available the TDM interface to the DSN network and/or the supporting DVX-C shall support MLPP PRI and/or CCS7 as described in UCR 2008 [Section 6.1.6.11.5.1](#), MSO MLPP Trunks and Interfaces

[Conditional] The DCVX will support preemption and precedence capability under one or more of the following conditions.

1. The DCVX supports GSM in the DoD GSM Cellular Band as described in UCR 2008 [Section 6.1.6.6.2](#), DoD GSM Cellular Band.
2. The DCVX supports the use of leased cellular frequency in one of the bands and protocol(s) listed in [Table 6.1-1](#).
3. The DCVX supports one or more of the cellular bands and protocol(s) as described in [Table 6.1-1](#) in an OCONUS environment, where the local Forces-Status Agreement allow eMLPP/proprietary version operation.

Section 6.1 – Unique Tactical Requirements

4. The DCVX supports one or more of the cellular bands and protocol(s) as described in [Table 6.1-1](#) dependent upon the operational environment and usage of cellular frequencies allowed by local and/or national civilian authorities.

6.1.6.8.9 Precedence Capability Terminal Device Activation/deactivation

[Conditional] If precedence and preemption capability is provided in the DCVX, the DCVX may be capable of providing any supported Terminal Device the user's Precedence Class Table Assigned features for providing said features to the Terminal Device based on the user entering a specified PIN number on same said Terminal Device. The DCVX will assign to the Terminal Device all of the user's precedence capability as defined in the switches class features table(s). This will allow the user to make precedence calls from different Terminal Devices other than the one assigned or provided to the user. Additionally, the precedence features assigned to that active terminal device can be turned off by re-entering the same or different PIN number on the said terminal device. The precedence capability user's activation/de-activation PIN number may be stored in the DCVX or in another database accessible by the DCVX to validate the user's PIN number(s) associated with the user's precedence capability. The user's precedence activation or de-activation PIN number may be assigned and/or user settable after given an initial assigned PIN number.

6.1.6.8.10 Precedence and Preemption Calling Features

[Conditional] If precedence and preemption capability is provided in the DCVX, then under the following calling features, once a higher precedence call has been connected to the terminal device and the higher precedence call is in progress, the calling party of lower precedence will receive a notification that the lower precedence call was rejected.

6.1.6.8.10.1 Precedence CW

[Conditional] The following Precedence CW treatments shall apply to precedence levels of PRIORITY and above if Precedence and Preemption capability is provided in the DCVX.

6.1.6.8.10.1.1 Busy with Higher Precedence Call

[Required] If the precedence level of the incoming call is lower than the existing MLPP call, precedence call waiting shall be invoked. In an active call, if the incoming call is PRIORITY precedence or above, the precedence call waiting tone shall be applied to the called party.

6.1.6.8.10.1.2 *Busy with Equal Precedence Call*

[Required] The DCVX shall provide the precedence call waiting signal to the called station. The DCVX shall apply this signal 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.

6.1.6.8.10.1.3 *Busy with Lower Precedence Call*

[Required] The DCVX 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 three seconds. After the current call is terminated and the terminal device is idle, the station to which the precedence call is directed shall be provided precedence notification described in UCR 2008 Section 5.2 or comparable vibration cadence. The station shall be connected to the preempting call after going off-hook.

6.1.6.8.10.1.4 *No Answer*

[Required] If, after receiving the precedence CW 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.

6.1.6.8.10.2 **Precedence TWC**

[Conditional] If Precedence and Preemption and TWC are provided in the DCVX, the following TWC requirements apply:

[Required] In TWC, each call shall have its own precedence level. When a TWC 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 TWC.

[Required] The DCVX shall class mark the originator of the TWC 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 higher of the two segments shall preempt unless the call is marked non-preempt able.

[Required] When a higher precedence call is placed to any one of the TWC participants, that participant receives the preemption tone. The other two parties shall receive a conference disconnect tone. This tone indicates to the other parties that one of the other TWC participants is being preempted.

Section 6.1 – Unique Tactical Requirements

[Required] 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.

6.1.6.8.10.3 Precedence Conference Calling

[Conditional] If precedence and preemption and conference calling are provided in the DCVX, then the following precedence conference calling requirement as described below is required.

[Required] 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 “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 Blocked Precedence Announcement (BPA).

6.1.6.8.10.4 Voice Mail

The voice mail feature interacts with MLPP. If precedence and preemption capability and voice mail are provided in the DCVX or voice mail added externally, the MLPP interactions must meet the requirements described in UCR 2008 Section 5.2.2.3, Precedence Call Diversion.

[Conditional] The DCVX may provide ROUTINE calls only voice mail capability for users. Additional features such as message forwarding and others may be provided in addition to basic voice mail capability provided they do not interfere with precedence and preemption if capability is provided in the switch.

6.1.6.8.10.4.1 *Precedence and Preemption Interaction with Voice Mail*

[Conditional] If precedence and preemption is provided in the DCVX and voice mail capability is provided internally to the DCVX or connected externally to the DCVX as an adjunct, the following requirement applies:

[Required] The DCVX shall divert all precedence calls above ROUTINE that are destined for voice mail in accordance with UCR-2008 Section 5.2.2.3, Precedence Call Diversion.

6.1.6.8.11 *Management Capabilities for Terminal Devices*

[Required] The DCVX shall have the capability to manage its supported Terminal Devices as published in its HLR such that it can assign, transfer, terminate services, features, and calling capability to include phone numbers for its Terminal Devices.

6.1.6.9 *Terminal Device Specific Requirements*

Cellular handsets often referred to as Mobile Subscribers, Hand Sets, PDAs, Blackberries, and any other user cellular end item devices commercial or Government developed, are herein referred to as Terminal Devices. The Terminal Device is the interface between the user and the cell network. The Terminal Device can be a hand held unit, a mounted mobile device, or a fixed location device.

6.1.6.9.1 *Terminal Device Requirements*

[Required] The Terminal Device shall provide the following status information to the network:

- Powered on
- Moved to a new location
- Alerting
- Dialing.

[Required] The Terminal Device shall display the following status information to the end-user:

- Signal strength
- Battery capacity
- Roaming status
- Service not available
- Call progress status

[Conditional] The Terminal Device may have the ability to provide key locking ability to lock the Terminal Device's keypad and unlock the keypad after providing the appropriate key

Section 6.1 – Unique Tactical Requirements

sequence/PIN number entries as provided by the vendor in the Terminal Device. The lock and unlock key sequence / PIN number shall be settable by the user. There will also be an administrator method that can be vendor proprietary that can unlock the Terminal Device in case the user PIN number is not available or supplied.

[Conditional] The Terminal Device may have the capability to support WPS on commercial networks and/or DoD networks where provided when not connected to and functioning on a DoD precedence and preemption network.

[Required] Removable/Exchangeable SIM: The SIM card in commercially available Terminal Devices shall be removable and exchangeable into other like commercially available Terminal Devices compatible with the DCVX system (applicable to a GSM-based system). This excludes Secure Terminal Devices and other Terminal Devices not readily commercially available.

6.1.6.9.2 Terminal Device Signaling

[Required] The Terminal Device shall provide information to allow the DCVX to identify the Terminal Device when the Terminal Device is powered up, successfully registered, and if in active call status.

6.1.6.9.3 Terminal Device Frequency Band Support

A Terminal Device that supports more than one frequency band has a high connection and reliability capacity.

[Conditional] A Terminal Device may support up to five frequency bands as specified in [Table 6.1-1](#) for each protocol supported in UCR 2008 [Section 6.1.6.8.2](#), Protocol/Format.

[Conditional] The Terminal Device may also support roaming and interconnecting with commercial cellular networks when operating outside the transmission range of the home based DCVX and other supporting DCVXs interconnected in support of roaming within the Tactical OAN.

6.1.6.9.4 Terminal Device Encryption

[Required] If SCIP and/or other NSA accredited encryption are implemented in the Terminal Device, the SCIP and/or other NSA accredited encryption capable Terminal Device shall have the capability to go secure to provide E2E encryption to another secure cellular like capable Terminal Device and via the DCVX to a non-cellular NSA encryption capable like devices per the requirements specified in the UCR 2008 for the DoD Secure Communications Device (DSCD). The SCIP and/or other NSA accredited encryption device shall provide end-to-end

encryption within the DCVX, from DCVX to DCVX (roaming) and from DCVX to external networks such as DSN and/or PSTN.

[Conditional] The Terminal Device may support other Non NSA encryption schemas, such as AES encryption as used by the Government Emergency Telecommunications Service (GETS) system.

6.1.6.9.5 *Terminal Device Battery Requirements*

[Required] The readily commercially available non-secure Terminal Device must have a battery that shall provide as a minimum 6 days standby time in total and 3 hours non-secure talk time in total but not both requirements sequentially on the same battery charge. NSA Encryption secure Terminal Devices (e.g., PDA Secure Mobile Environment Portable Electronic Device (SME PED)) must provide their specified battery and secure/unsecure talk time. All other Terminal Devices must provide their specified battery and unsecure talk time and/or secure talk time if applicable.

[Required] The Terminal Device shall have battery auxiliary capabilities when the primary battery is removed / drained to insure primary network and user settings are not lost on the device before a primary battery is installed/recharged to ensure the Terminal Device is able to connect to the DCVX on power-up. Auxiliary battery shall provide a minimum of two hours of power to retain Terminal Device settings only.

6.1.6.9.6 *Terminal Device Secure Call Handling*

[Conditional] If the Terminal Device supports SCIP or other NSA accredited encryption scheme(s) the Terminal Device/DCVX system will provide classified secure call handling features as defined in UCR 2008 [Section 6.1.4.8](#), Secure Call Handling.

6.1.6.9.7 *Terminal Device display/alerting features*

The terminal device shall have the following display and alerting features:

[Required] Power-on status: When the Terminal Device is powered on, the display shall indicate:

- Signal strength
- Remaining battery capacity
- Active call status
- HLR registration results (either success or failure)

Section 6.1 – Unique Tactical Requirements

[Required] Routine call alerting: The idle, registered Terminal Device shall provide or be provided an auditory and/or visual display alert for incoming routine calls.

[Conditional] Precedence call alerting: DCVX may be required to meet the eMLPP functionalities specified in UCR 2008 [Section 6.1.6.6.3](#), Precedence and Preemption. The eMLPP references or utilize a proprietary methodology. If precedence and preemption capability is provided, upon receiving a precedence call, the idle, registered Terminal Device will provide or be provided precedence alert and/or tone notification. Whether using eMLPP or proprietary version, the Terminal Device shall issue the same alerting tone(s) for precedence calls In Accordance With (IAW) eMLPP requirements. Upon notification the user will have the capability to select or reject the call of higher precedence.

6.1.6.10 Base Station Subsystem (BSS) Specific Requirements

The BSS minimally consist of the Base Station Controller, Base Station Transceiver Station(s), and the Cell Tower(s) with Radio Transceiver(s).

6.1.6.10.1 Signaling

[Required] The base transceiver for radio cells will determine which channel to use for call setup IAW the appropriate supported protocols listed in UCR 2008 [Section 6.1.6.8.2](#), Protocol/Format.

6.1.6.10.2 Strength

[Required] The base transceiver for radio cells will monitor the Terminal Device for signal strength and transfer the Terminal Device to the stronger cell when necessary IAW the appropriate supported protocols listed in UCR 2008 [Section 6.1.6.8.2](#), Protocol/Format.

6.1.6.10.3 Protocol/Format

[Required] The BSS shall support one or more of the protocols listed in the DCVX General Requirements UCR 2008 [Section 6.1.6.8.2](#), Protocol/Format.

6.1.6.10.4 Coverage

[Required] For radio cellular, the base station controller will assign the strongest cell to the Terminal Device. The coverage area this system will provide shall be in accordance to the GSM/CDMA standards and specifications in accordance with [Table 6.1-1](#) and UCR 2008 [Section 6.1.6.8.2](#), Protocol/Format. Actual coverage will be dependent upon topology / manmade structures, and frequencies.

6.1.6.10.5 *Preemption*

[Conditional] If precedence and preemption capability is provided in the DCVX, then when preemption to reuse occurs, the BSS must disable the old call but maintain the channel assignment to the Terminal Device to allow the set up of the new call. In the event where there are no idle channels and a precedence call is received, the base station controller will find the lowest precedence channel and preempt that channel to allow for the higher level precedence call to be completed.

6.1.6.11 *Deployed Mobile Switching Center (DMSC) Specific Requirements*

The DMSC will minimally consist of the Mobile Switching Office, a VLR, AUC, and EIR . The HLR does not need to be a local component part of the DMSC but it will be necessary for the DMSC to access a home location register to determine the attributes of any Terminal Device. Whether the HLR is local with the DMSC or is remotely queried, the HLR is a component of the DCVX under test.

6.1.6.11.1 *Visitor Location Register*

[Required] The DMSC shall maintain a VLR to allow service to any active Terminal Device operating in the area being served by the DCVX that is registered with the HLR. The VLR knows which BSS the active Terminal Device is being served by.

6.1.6.11.2 *Home Location Register*

[Required] The DMSC shall connect to a HLR to determine the attributes of the Terminal Device currently being served by the DCVX. The information provided by the HLR will tell the DMSC where the Terminal Device is located. The HLR will indicate what the Terminal Device attributes and status. The information on the Terminal Device from the HLR is stored in the VLR. The HLR can be co-located with the DMSC or deployed remotely. The local HLR may be queried by vendor proprietary methodology. The remote HLR can be queried using DMSC network trunk interfaces of CCS7, MLPP PRI, or ISDN PRI. Additionally, the local and/or remote HLR may be also be queried using CCS7 over IP (SIGTRAN), or AS-SIP.

[Required] HLR Storage: The HLR must store and support information on each Terminal Device registered to the network the HLR serves.

[Required] *HLR Change and Propagation:* The HLR must support changes to the Terminal Device information. Once the HLR receives the supported change information the HLR, whether local or remote from the DMSC, has three minutes to propagate the change information

Section 6.1 – Unique Tactical Requirements

to the VLR. If the DCVX supports roaming, the HLR change must also propagate to the querying VLRs.

[Conditional] *Intra DCVX Queries:* If roaming capability is supported in the DCVX, the HLR must support queries from other DCVXs using specified protocol methods for obtaining Terminal Device information (e.g. CDMA and GSM based queries).

6.1.6.11.3 *Equipment Identity Register*

[Required] To validate Terminal Devices to prevent a compromised Terminal Device from connecting to the Cellular Switch and obtain services, an EIR capability must be provided and integrated to work in conjunction with the Terminal Device Authentication Center process (see [Section 6.1.6.11.4](#)) to prevent compromising the DCVX.

6.1.6.11.4 *Terminal Device Authentication Center*

[Required] To authenticate Terminal Devices as valid Terminal Devices associated with the DCVX, the Cellular Switch will utilize standard cellular techniques, industry best practices, and/or vendor proprietary processes integrated into the switch.

[Conditional] Terminal Devices not assigned to the supporting DMSC HLR (e.g., roaming Terminal Devices) may be supported for authentication via the industry standard(s) and/or industry best practices for roaming authentication.

6.1.6.11.5 *Mobile Switching Office Functions and Features*

6.1.6.11.5.1 **MSO MLPP Trunks and Interfaces**

[Required] The MSO shall support one or more of the following TDM and/or IP trunks and interfaces, but may not connect to the DSN network with both types (TDM, or IP) simultaneously.

6.1.6.11.5.1.1 *TDM Support*

[Conditional] If TDM trunks are supported, then the following requirements apply as directed:

[Required] The MSO will minimally support ISDN PRI (T1/E1) as defined in UCR 2008 Section 5.2, Circuit-Switched Capabilities and Features, Table 5.2-1, Trunk Types and Signaling Used in The DSN (including legacy interfaces) for trunks that connect to the DSN/PSTN without MLPP capability.

[Conditional] If precedence and preemption capability is provided in the DCVX, the MSO will support one or more of the following:

1. MLPP PRI (ANSI T1.619a, and ITU Q.955.3 & Q.735.3) EO Access trunk as a minimum requirement. The MLPP PRI protocol will conform to the requirements for DSN trunks as defined in UCR 2008 Section 5.2, Table 5.2-1, for trunks that connect to the DSN with MLPP capability.
2. CCS7 for signaling and associated T1/E1 bearer trunks. 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 CCS7 requirements as listed in UCR 2008 Section 5.2.4.6. Only those CCS7 requirements that differ from their corresponding ANSI common channel signaling standard section are included in UCR 2008 Section 5.2.4.6. CCS7 shall only connect on DoD networks, not to the PSTN and/or other Non-Government networks.

[Conditional] The MSO may support TDM/ CAS trunk IAW UCR 2008 Section 5.2, Table 5.2-1 for EO Access Trunks.

[Conditional] The MSO may support CCS7 for signaling and associated T1/E1 bearer trunks. 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 SS7 networks. Exceptions to these standards are explicitly noted in CCS7 requirements as listed in UCR 2008 Section 5.2.4.6. Only those CCS7 requirements that differ from their corresponding ANSI common channel signaling standard section are included in UCR 2008 Section 5.2.4.6. CCS7 shall only connect on DoD networks, not to the PSTN and/or other non-Government networks.

6.1.6.11.5.1.2 *IP Trunking AS-SIP Support*

[Conditional] If AS-SIP IP trunks are supported, then the DCVX shall comply with the stated requirements of a LSC and if required act as a SIP B2BA for the Terminal Devices to meet the EI requirements in the UCR 2008.

6.1.6.11.5.1.3 *SIGTRAN*

[Conditional] The MSO may support CCS7 over IP using SIGTRAN in accordance with IETF RFC 2719, architectural framework for signaling transport and other associated supporting RFCs. SIGTRAN shall be used only in connecting DCVXs together on DoD IP Networks within

Section 6.1 – Unique Tactical Requirements

the Tactical OAN in support of roaming capability and/or querying the local/remote HLR. SIGTAN shall not connect to the PSTN and/or other non-Government networks.

6.1.6.11.5.2 Non-MLPP Networks Support

[Conditional] The MSO may support ISDN PRI (T1/E1) non-MLPP trunk for connecting to the PSTN and/or other Non-Government networks. The ISDN PRI protocol will conform to the requirements for commercial trunks as defined in UCR 2008 Section 5.2, Table 5.2-1, for trunks that connect to non-DSN networks.

6.1.6.11.5.3 Call Handling

[Required] The MSO shall handle both intra-switch calls and calls to and from the DSN, while recognizing a powered on Terminal Device that comes into its area. The MSO shall also receive information on the Terminal Device from the HLR and store that information in the VLR. For Secure call handling shall be as stated in UCR 2008 [Section 6.1.4.8](#).

6.1.6.12 Security

[Required] All components of the cellular system(s) shall meet security requirements, for each supported mode, as outlined in DODI 8510.01 28 November 2007, “Defense Information Assurance Certification and Accreditation Process (DIACAP)” and the applicable Security Technical Implementation Guides (STIG).

6.1.6.13 DCVX Network Traffic Management Operating System (NTMOS)

[Required] The DCVX switching systems shall provide network management data to the administering network management console via one of the three following physical interfaces:

- Ethernet/Transmission Control Protocol (TCP)/IP (Institute of Electrical and
- Electronics Engineers (IEEE) 802.3)
- Serial (RS-232)/Asynchronous
- Serial/Synchronous (X.25 and/or BX.25 Variant)

All network management data, and configurable features and functions that are collected shall, as a minimum, be accessible through one of these interfaces. The DCVX 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 shall be transmitted to the nm console in such a fashion as to allow for storage, recovery, and transfer of the information to or from digital media storage, and to allow for printing and/or

screen display using methods, such as American Standard Code for Information Interchange (ASCII), binary, or hexadecimal data.

The data channels shall be used for and 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 datafill administration and network controls)

6.1.6.14 *Submission of Wireless Systems to UCCO for DSN Connection Request*

[Required] DCVX systems shall be engineered properly so that the BSS and cellular Terminal Devices achieve the required performance requirements in their specific deployed environment. The user shall submit a network design and engineering performance analysis with supporting calculations to meet minimum MOS performance with the request for DSN connection. For certification procedures the UCCO submittal shall include wireless security compliancy as identified in UCR 2008 [Section 6.1.6.12](#).

THIS PAGE INTENTIONALLY LEFT BLANK.

FOR OFFICIAL USE ONLY

Section 6.2 – Unique Classified Unified Capabilities Requirements

SECTION 6.2 UNIQUE CLASSIFIED UNIFIED CAPABILITIES REQUIREMENTS	3
6.2.1 Purpose and Scope	3
6.2.1.1 Policy and Requirements Documents for DRSN and CVVoIP	4
6.2.2 General Requirements Overview	6
6.2.2.1 Assured Services	7
6.2.2.2 Multilevel Secure Voice Services	8
6.2.2.3 Secure Voice Quality Requirements	8
6.2.2.4 Command and Control Requirements	8
6.2.2.5 Key CVVoIP voice services Features	10
6.2.2.6 General Security Features	10
6.2.2.7 Special Security Features	11
6.2.2.8 Network Security	13
6.2.2.9 Network Interfaces	14
6.2.2.10 CVVoIP and VoSIP Connection Approval	14
6.2.2.11 DRSN/VoSIP/CVVoIP Network Management	15
6.2.2.12 Directory (white pages) Services	15
6.2.2.13 Conferencing Requirements	16
6.2.2.14 CVVoIP Equipment Certification and Testing Policy	16
6.2.3 VoSIP Migration to the DISN CVVoIP	16
6.2.4 Classified Unified Capabilities Technical Design Framework	21
6.2.5 Technical Design for 2009	24
6.2.5.1 FY2009 Signaling Design	26
6.2.6 Modifications to the SBU Assured Services Requirements to Include CVVoIP - Unique Requirements	28
6.2.6.1 Voice End Instrument	29
6.2.6.2 Classified LSC Requirements	29
6.2.6.2.1 usb LSC Requirements not applicable to Classified lsc	29
6.2.6.2.2 Classified LSC Unique Requirements	29
6.2.6.3 Network- Level Softswitch	29
6.2.6.4 Media Gateway with Signaling Interworking	30
6.2.6.5 Signaling Gateway	31
6.2.6.6 Edge Boundary Controller	31
6.2.6.7 Addressing Schema for LSC	31
6.2.6.8 Network Management	31
6.2.6.9 White Pages Directory Services	32
6.2.6.10 Voice Quality	33
6.2.6.11 Call Set-up Time	34
6.2.6.12 Unique Network Infrastructure Requirements for CVVoIP	34

FOR OFFICIAL USE ONLY

Unified Capabilities Requirements

Section 6.2 – Unique Classified Unified Capabilities Requirements

6.2.6.13	Unique IA Requirements for CVVoIP.....	34
6.2.7	Classified AS-SIP unique Requirements	38
6.2.7.1	Classified Signaling Environment	38
6.2.7.1.1	IP Signaling Path Reference Cases	40
6.2.7.2	Differences Between SBU and Classified AS-SIP Requirements	40
6.2.7.2.1	Nomenclature	41
6.2.7.2.2	Proxy-Require Header	42
6.2.7.2.3	CAL General Requirements.....	46
6.2.7.2.4	Option Tag ‘CAL’	51
6.2.7.2.5	418 Incompatible CAL Message	52
6.2.7.2.6	Route Header	53
6.2.7.2.7	SIP Preconditions.....	57
6.2.7.2.8	SIP URI Mapping of Telephone Number	58
6.2.7.2.9	64kbps Transparent Calls (Clear Channel).....	58
6.2.7.2.10	Transport of Route Code Information over AS-SIP	59
6.2.7.2.11	Precedence and Preemption	59
6.2.7.2.12	Policing of Call Count Thresholds.....	61
6.2.8	Physical Construction Unique Requirements	70

SECTION 6.2 UNIQUE CLASSIFIED UNIFIED CAPABILITIES REQUIREMENTS

6.2.1 Purpose and Scope

The purpose of UCR 2008, Section 6.2 is to describe technical requirements that are unique to providing Classified Unified Capabilities. Classified requirements consist of the SBU requirements defined in UCR 2008 with modifications as described here in UCR 2008, Section 6.2. This issue of the UCR 2008, Section 6.2 specifies technical requirements for assured interoperability and information assurance of the following set of unified capabilities that will be expanded in the future:

- Voice and Video Services Point to Point
- Voice Conferencing
- Videoconferencing.

More specifically, meeting the requirements specified in UCR 2008, Section 6.2 will allow the current best effort, H.323 based single-vendor VoSIP network to migrate to an AS-SIP-based multi-vendor assured services network, and enable Classified UC products to be tested and placed on the UC APL.

The Classified Voice and Video over IP (CVVoIP) system for FY 2009 is a single security level network operating over the secret aggregation routers of the DISN that includes secure voice capabilities that interfaces to the DRSN at selected locations. The CVVoIP system described for FY 2009 is not intended to replace the DRSN and its many unique features.

The contents of UCR 2008 Section 6.2 are arranged as follows:

1. [Section 6.2.1](#), Purpose and Scope, provides the purpose of UCR 2008 Section 6.2 and provides a listing of major policies that are unique to the multilevel secure voice services provided by the DRSN and to the single security level DISN VVoIP services.
2. [Section 6.2.2](#), General Requirements Overview, provides a summary of the CVVoIP requirements that drive the CVVoIP design.
3. [Section 6.2.3](#), VoSIP Migration to the DISN CVVoIP, addresses the VoSIP migration to a multivendor IP-based, assured, secure CVVoIP system.
4. [Section 6.2.4](#), Classified Unified Capabilities Technical Design Framework, addresses the migration from the VoSIP to CVVoIP and the migration of the current DRSN APL to a UC

Section 6.2 – Unique Classified Unified Capabilities Requirements

APL. The approved products for CVVoIP and the APL process are addressed in UCR 2008, Section 4.5.

5. [Section 6.2.5](#), Technical Design for 2009, addresses the CVVoIP IP technical design for the FY2009 time frame.
6. [Section 6.2.6](#), Modifications to the SBU Assured Services Features to Include CVVoIP-unique Requirements. This section describes the modifications to the SBU Assured Services requirements as necessary to include CVVoIP unique requirements. Topics discussed include, voice EI, LSC requirements, network-level SS, MG, SG, EBC, addressing schema, NM, white pages directory service, voice quality, WAN requirements, and the IA requirements.
7. [Section 6.2.7](#), Classified Assured Services Session Initiation Protocol (AS-SIP) Unique Requirements, defines the modifications to the SBU AS-SIP requirements as necessary for classified assured services.
8. [Section 6.2.8](#), discusses special construction requirements that include Protected Distribution System cabling, encryption of facilities leaving a secure enclave and TEMPEST.

6.2.1.1 Policy and Requirements Documents for DRSN and CVVoIP

All the policies identified in UCR 2008, Section 3 apply to CVVoIP. [Table 6.2.1-1](#) lists the major policy and requirements documents that are unique to Multilevel Secure Voice services provided by the DRSN and to single security level DISN CVVoIP services.

Table 6.2.1-1. Major Policy and Requirements Drivers for DISN CVVoIP Services

Joint Requirements Oversight Council (JROC), JROC Memorandum (JROCM) 202-02, “Global Information Grid (GIG) Mission Area Initial Capabilities Document (MA ICD),” 22 November 2002. JROCM and date listed refer to the latest JROC approval of the “Global Information Grid (GIG) Capabilities Requirement Document (CRD).” This MA ICD is a cut and paste conversion of the GIG CRD in MA ICD directed by JROCM 095-04 of 14 June 2004.

DoDD 5200.28, “Security Requirements for Automated Information Systems (AISs),” 21 March 1988.

Homeland Security Presidential Directive/HSPD-7, Subject: Critical Infrastructure Identification, Prioritization, and Protection, 17 December 2003.

Homeland Security Presidential Directive 8 (HSPD-8), “National Preparedness,” 17 December 2003.

H.R. 45646, Section 804, “Software Acquisition Process Improvement Programs.”

DoD 5200.1-R, “Information Security Program Regulation,” 14 January 1997.

Chairman of the Joint Chiefs of Staff Manual (CJCSM) 3170.01C, “Operation of the Joint Capabilities Integration and Development System,” 1 May 2007.

Global Command and Control Systems-Joint (GCCS-J) Single Acquisition Management Plan (SAMP) for Block V, Version 1.0.

“Joint Command and Control (JC2) Capability Technology Development Strategy (TDS),” Draft, Version 3.3.9.

Committee on National Security Systems (CNSS) Instruction No. 4009, “National Information Assurance (IA) Glossary,” Revised June 2006.

Defense Intelligence Agency (DIA) Memorandum DIA/DTI-4B, 8 October 1992.

“Operational Requirements Document (ORD) for Secure Voice Requirements,” J-6A 01665-92, 17 November 1992.

National Security Telecommunications and Information Systems Security (NSTISS)

Section 6.2 – Unique Classified Unified Capabilities Requirements

Instruction (NSTISSI) No. 4010, “Keying Material Management (U),” FOUO, 17 June 1993.

National Security Telecommunications and Information Systems Security (NSTISS) Authority Manual (NSTISSAM) No. TEMPEST/2-95, “RED/BLACK Installation Guidelines,” FOUO, 12 December 1995.

National Security Telecommunications and Information Systems Security, NSTISSI No. 7003, “Protected Distribution Systems (PDS) (U),” 13 December 1996.

Defense Nuclear Agency/Defense Communications Agency (DNA/DCA), “Classification Guide for Electromagnetic Pulse Testing (EMPT),” Confidential/Restricted Distribution (C/RD), 16 May 1987.

National Security Telecommunications and Information Systems Security, NSTISSI No. 4002, “Classification Guide for COMSEC Information (U),” SNF, 5 June 1986.

Title 5, U.S. Code, Section 552a (Privacy Act), 23 January 2000.

Director of Central Intelligence Directive (DCID) 1/21, “Physical Security Standards for Sensitive Compartmented Information Facilities,” 30 January 1994.

DIA Manual (DIAM) 50-4, “Security of Compartmented Computer Operations,” 24 June 1980.

DCID 6/3, “Protecting Sensitive Compartmented Information Within Information Systems.”

6.2.2 General Requirements Overview

A high level summary of the requirements for CVVoIP are provided by a combination of the documents referenced in [Table 6.2.1-1](#) and a list of key system attributes that have been established in coordination with the Joint Staff over the past decade as the set of required features for an operational C2 communications service offering. These performance attributes have been proven in real world operations stretching from Desert Shield/ Desert Storm through Operation Iraqi Freedom.

The most demanding set of requirements in all these documents that drive the DISN Classified IP Convergence Migration Strategy involves those associated with:

- Multilevel secure service
- Rapid, high-quality, secure communications and conferencing capabilities for senior leaders and warfighters
- Assured services
- IA
- E2E interoperability
- NetOps

These are the most demanding requirements because COTS IP-based technologies are not sufficiently mature that they require GIG E2E system engineering by the Government, development by industry, and test and evaluation by the Government in order to meet these policies and requirements. In addition, the challenges discussed in the next section prevent the ability to install a common technology base for all services as a “flash cut.” Thus, networks based on hybrid technologies will be required for many years.

One of the key C2 functions of the DRSN is to provide rapid, flexible, and secure conferencing. Accordingly, there have been a number of unique non-COTS MLS operator console features developed in response to the Combatant Commanders’ command center requirements. These features which are part of the way those command centers conduct their business will not be required for the FY 2009 CVVoIP.

6.2.2.1 Assured Services

The CVVoIP system shall provide the Assured Services Features from UCR 2008, Section 4.2.

The most important consideration for implementing new technology is the impact on mission requirements. Implementing a new technology, such as VoIP, must first and foremost not degrade the C2 services currently being provided to secure voice users.

6.2.2.2 *Multilevel Secure Voice Services*

The DRSN provides DoD multilevel secure C2 voice services and is a key component of the DoD global secure voice services. The DRSN supports the secure voice and secure conferencing, requirements of the NCA, components, DoD, and select federal agencies in peacetime, in crisis situations, and in wartime. It is a separate, secure switched network that is considered part of the DISN. The DRSN, the STU-III/STE family of equipment that provides E2E encryption over the DSN, and Condor, the NSA's program to secure wireless communications, are the three subservices that together provide the foundation for the DoD secure voice services. In addition, DRSN provides an interface to the secure service at the SECRET-only level which shall be provided by the VVoIP system.

6.2.2.3 *Secure Voice Quality Requirements*

The EI-to-EI voice quality of a telephone connection is subjective and is determined from the complex interaction of multiple switching, speech encoding, voice compression techniques, and transmission parameters. The objective of the DRSN is to provide toll quality secure-voice service on a DRSN-user-to-DRSN-user basis, and to ensure the highest practical voice quality when DRSN users are interfaced to external systems and equipment. This is defined as receiving a score of at least 90 on the DRT and a score of at least 60 on the DAM. The DRT measures intelligibility, and the DAM measures quality. These objective intelligibility and quality scores are achieved by adhering to the DoD, national, vocoding, and international transmission design and operational standards. DRSN voice quality is addressed in the development of new vocoders for DRSN interfaces and voice compression algorithms for the network.

6.2.2.4 *C2 Requirements*

The DRSN provides all C2 features needed for critical applications while providing the rich feature suite of modern administrative telephony systems. Once IP technology matures to the necessary level, the requirements for CVVoIP will encompass the full DRSN requirements. For the near-term, the requirements listed below will be met by a mix of IP and the current suite of DRSN switches.

- Multi-Level Secure (MLS) Voice
 - Variable Security Access Level (Applicable to DRSN only, CVVoIP is fixed at SECRET)
 - Authentication
 - Low Probability of Misconnect

- High Crosstalk Isolation
- TEMPEST/EMI compliance
- Integrated Red-Black Instruments (DRSN only)
 - Instruments located in a Secure Compartmented Facility (SCIF) must be Telecommunications Security Group (TSG)-Approved (DRSN and CVVoIP).
- Secure Conferencing
 - Ad-Hoc Conference (3-way CVVoIP and DRSN)
 - Preset Conference (CVVoIP and DRSN)
 - Unlimited (DRSN only)
 - Dissimilar Devices (DRSN only)
 - Distributed Across Network (DRSN only)
 - Variable Security Levels during Conference Execution (DRSN only)
- Assured Connectivity
 - Non Blocking Components
 - Transport Bandwidth
 - Resilient Routing
 - MLPP with Override of Flash Override
- High Availability
 - Redundant Components
 - Redundant Transport
 - High-Altitude Electromagnetic Pulse (HEMP) Survivability for selected sites
- Real-Time operational control
 - C2 consoles giving execution control to operational personnel
 - “Override” capability by operational personnel
 - “Visibility” to operational personnel
- Management
 - Administrative (Provisioning)
 - Utilization (NM)
 - Fault Management
 - Real-time Health Monitoring

Section 6.2 – Unique Classified Unified Capabilities Requirements

- Interoperability
 - Legacy Devices (secure voice radios, instruments, and other terminal types [DRSN only])
 - Dissimilar Devices (e.g., between MILSTAR and STE terminals [DRSN only])
 - Media Conversion
 - Protocol Conversion
 - Speakers, Recorders
 - Other networks such as MILSTAR.SECN, DSCS/EPC, Homeland Security, FBI and Department of State. (DRSN only)

6.2.2.5 Key CVVoIP voice services Features.

The key CVVoIP voice services features and attributes are shown in [Table 6.2.2 -1](#).

Table 6.2.2–1 Key CVVoIP Voice Service Features

Feature Name	Feature Functional Purpose
Automatic Number Identification (ANI)	Identifies the caller before the call is answered.
Display of Call Security Level	Identifies the classification level of an incoming call
Directory (White Pages) Service Access	Presents location information and telephone numbers of personnel by using the IP EI display.
Instrument Lock-out	Requires user login to activate instrument. Any IP EI must be <u>DISABLED</u> at all times when not under the physical control of the authorized user
COTS Features	Call forward, call waiting, call hold, etc

6.2.2.6 General Security Features

1. DRSN RED Switches, classified LSCs and Tier0 SSs must operate with physical security and TEMPEST compliance to allow users within a RED enclave to conduct unencrypted, classified telephone conversations at the level commensurate with the facility, system, and user clearances. As a minimum, DRSN switching nodes must operate at the TS security

level. However, VoSIP and CVVoIP users and LSCs are only to be configured at the SECRET level until multilevel security operation for IP-based technology is mature.

2. Telephone instruments installed outside the RED enclave, but within a limited exclusion area in the same facility, may be connected to the switching subsystem through an approved PDS or link encryption between the RED enclave and the "exclusion" area.
3. All other connectivity into and out of a DRSN or CVVoIP RED enclave must be secured with NSA approved encryption equipment. In addition, connections to CVVoIP system (and VoSIP) must be approved or implemented as defined by the SIPRNet Connection Approval Process. DRSN RED switches, VoSIP Call Manager, and Classified LSCs must interconnect with other RED switches and/or peripheral devices (to include, but not limited to, tactical secure-voice switches/enclaves, radio interfaces, audio systems, voice announcers, and multimedia and/or secure-voice over data capabilities) through encrypted Interswitch Trunks (ISTs) or by means of a PDS. Other secure systems must interconnect to the DRSN using DISA-established interface criteria and encryption devices or PDS.

6.2.2.7 Special Security Features.

The following special security features are currently inherent to the DRSN. The following text is included to aid the reader in understanding the full aspects of the special security features. For CVVoIP, the initial feature set is limited to a fixed call security level of SECRET. The Confidential Access Level (CAL) parameter within the AS-SIP requirements is used to convey the call security level.

1. Automatic Number Identification (ANI). During intraswitch and interswitch call processing, DRSN switches exchange classmark information that include the calling and called-station identity and call security access level (SAL) assignments. The ANI information (of the calling party) is displayed on the called party's DRSN user telephone display prior to the call being answered by the called party. When the called party answers, the ANI information of the called party is displayed on the calling party's DRSN user instrument as well as the security level (SECRET, TS, or TS/SCI) of the established connection being displayed on both the calling and called parties' DRSN user instrument. User ANI identity information is defined in the database of the DRSN switch to which a user is directly connected. All equipment connected to the DRSN must be capable of providing ANI to the DRSN switch to which it is or will be connected. CVVoIP instruments will be fixed at the SECRET level and display the calling telephone number via AS-SIP signaling.

FOR OFFICIAL USE ONLY

Unified Capabilities Requirements

Section 6.2 – Unique Classified Unified Capabilities Requirements

2. SAL. The SAL is a user classmark assigned to each instrument, line key, and trunk and provides security authentication of the calling and called party. SALs are assigned to each instrument, line key, and trunk based upon the classification and access level authorized for the user. The DISA DRSN service manager will develop and publish a standardized set of SALs, which must be implemented at all DRSN nodes. In addition to a standardized set of SALs, the DISA DRSN service manager may implement special SALs on a case-by-case basis to meet specific mission requirements. Alteration of SALs and/or implementation of SALs without specific direction and/or approval of the DISA DRSN service manager are not permitted and constitute a reportable security infraction.

3. Automatic Security Authentication (ASA). ASA ensures DRSN calls are set up in accordance with security and access authorization criteria defined for each user and/or DRSN switch interface. ASA uses a combination of fixed and variable SAL assignments to reconcile and establish, or deny establishment of, connections between users and between users and DRSN switch interfaces based upon a highest common denominator scheme. For example, a connection between a user class-marked with a VSAL ([paragraph b](#)) of SECRET calling a user classmarked with a VSAL of TS will be permitted at the SECRET level. As another example, a connection between a user classmarked with a VSAL of SECRET calling a user classmarked with a FSAL ([paragraph 1](#)) of TS/SCI will NOT be permitted because there is no highest common denominator. This highest common denominator ASA scheme is equivalent to that implemented in the STU-III/STE family of equipment.
 - a. Fixed Security Access Level (FSAL). FSAL emphasizes call security over call completion. A user selects an FSAL-class-marked line when he or she must ensure the call is established at the desired security level. Under FSAL, a call's SAL is "fixed" at the user-selected level and cannot be downgraded as the call progresses through the network. If the called and calling parties and interconnecting trunks are class-marked with the same SAL (e.g., TS), the RED switches will establish the call and display the common security level. If a trunk group with a SAL equal to that of the originating station is not available for call routing, the originating RED switch will not complete the call, but instead will route the call to a security code violation-recorded announcement. If the called party has a different SAL assignment than the calling party (e.g., the called line is assigned SECRET and the calling line is assigned TS/SCI), the call will not be completed, and the originator will be routed to a security code violation-recorded announcement. CVVoIP instruments will be fixed at the SECRET level

 - b. Variable SAL. VSAL emphasizes call completion over call security level. With VSAL, a call is established if network resources are available. However, the call may be established at a security level less than that selected by the calling party. The

VSAL feature allows calls to be set up when the SAL codes among calling and called stations and trunk groups are not equal. Calls are automatically established at the highest common security level of the users and trunk facilities. The highest common security level, as determined by the switching system, is displayed on the called and calling instruments. Users must read the displayed security level and ensure the security level of conversations does not exceed the displayed security level. CVVoIP instruments will be fixed at the SECRET level.

4. Push-to-Talk Handset. The push-to-talk handset is an integral part of the physical protection afforded classified DRSN voice traffic. Removal of the push-to-talk feature may be justified only by legitimate operational requirements and will be approved on a case-by-case basis of the Designated Approval Authority (DAA), through the DISA DRSN information systems security manager. Prior to removal, the user must justify the action, develop procedures for maintaining the secure integrity of the instrument, and have written approval in accordance with DRSN security guidelines.

6.2.2.8 Network Security

1. DRSN RED Switches, VoSIP Call Managers, classified LSCs, and Tier0 SSs must be located in RED enclaves. DRSN RED Switches at the NMCC, the NMCC Site R, and combatant command headquarters, as well as those locations that have subscriber terminals authorized to process TS/SCI, must be located in SCIFs. DRSN RED switches, VoSIP Call Manager and classified LSCs will provide:
 - a. In-the-clear calling within each RED enclave by means of PDSs and protected ASLANs.
 - b. Cryptographically protected calling between RED enclaves supported by DRSN RED switches and VoSIP Call Manager and classified LSCs.
 - c. DRSN RED switches, VoSIP Call Managers and classified LSCs interface to external cryptographic equipment for all other calling.
2. NSA-approved encryption equipment provides COMSEC to the DRSN and the CVVoIP System. The encryption equipment or PDSs secure all DRSN ISTs and protect links to remote enclaves to include remote locations and quarters. The TSEC/KG-84 family of equipment (including KIV-7) provides Transmission Security (TRANSEC) to ISTs to locations (including quarters) receiving DRSN service via DPA, DTAs, and KG-84 telephone interfaces. The TSEC/KG-81 family of trunk equipment (including KIV-19s, TSEC/KG-81s, TSEC/KG-94s, and TSEC/KG-194s) bulk encrypts the digital streams between geographically separated RED enclaves.

Section 6.2 – Unique Classified Unified Capabilities Requirements

3. DRSN/VoSIP/CVVoIP instruments and service capability may be installed in senior officer quarters on a case-by-case basis. Such installations constitute the establishment of a RED enclave/limited exclusion area within the quarters and must comply with physical and technical security criteria applicable to the use and storage of COMSEC equipment. Use of DRSN equipment in quarters must comply with DRSN operating and security procedures applicable to a RED enclave office environment.
 - a. Any DRSN phone instrument installed in a quarters must be DISABLED at all times when not under the physical control of the authorized user.
 - b. Where the RED signal path (digital or analog) between COMSEC and the DRSN RED equipment (i.e., DRSN instrument and other DRSN terminal equipment) is greater than 3 meters from the COMSEC device, the RED signal path will be routed in an approved PDS.
 - c. Prior to the installation of DRSN service in quarters, the DISA DRSN service manager should be contacted for approval and confirmation of current applicable operating and security criteria.

6.2.2.9 Network Interfaces

A key feature of the DRSN is its ability to interface and interoperate with a variety of DOD and commercial networks. The CVVoIP and VoSIP systems interface to the DRSN through a gateway. (See UCR 2008, [Section 6.2.6.4.](#)) The current VoSIP to DRSN interface uses a vendor-unique implementation of a PRI trunk-signaling interface.

As part of the migration towards a multi-vendor based CVVoIP environment, gateway signaling between CVVoIP system, the DRSN and VoSIP will be standardized to accommodate AS-SIP signaling. A SG will allow H.323-based VoSIP to work with the AS-SIP based CVVoIP system during a transition period.

6.2.2.10 CVVoIP and VoSIP Connection Approval

All interfaces to the DRSN must be approved in writing on a case-by-case basis by the DISA DRSN service manager. Connection to the CVVoIP system and VoSIP must follow the SIPRNet Connection Approval Process. JITC certification letters documenting a technical interoperability with the DRSN do not constitute connection approval. Such certification letters only serve as a technical basis for requesting approval for connection to the DRSN in support of a Joint Staff-validated mission requirement. DISA DRSN service manager's approval for an interface may be in the form of a permanent, conditional, or temporary interface. Use of interfaces not conforming to DRSN interface criteria or as stipulated in the DISA DRSN service

manager's approval letter can have adverse technical and security impacts on all DRSN users and constitute an unauthorized use of the DRSN. Any such interfaces can result in the switch supporting such interfaces being denied network-level access to the DRSN infrastructure. All connectivity from a DRSN switch to users outside the RED enclave (i.e., to another building, facility, location, or system) must be provided through an approved interface.

6.2.2.11 DRSN/VoSIP/CVVoIP Network Management

DISA establishes DRSN management systems and procedures to ensure responsive, secure, interoperable, survivable, and cost-effective service. DRSN is under the management control of the Director, DISA SSM, on behalf of USSTRATCOM, and is responsive to the Chairman of the Joint Chiefs of Staff, the combatant commands, the Military Departments, and Defense agencies and activities.

1. DISA must possess read-access and limited/controlled write-access capabilities to all DRSN switch and network-level classified SSs (Tier0 SSs) network-related database tables, RED bandwidth managers, and other network-level infrastructure data.
2. DISA must maintain a CM database of all switch configurations (CONUS and OCONUS) and provide access to agencies, activities, and Military Departments as authorized by OSD, the Director, DISA, and the Joint Staff.
3. DISA must have the ability to implement network-level database changes and/or network control commands to all DRSN nodal switch and classified network-level SSs (Tier0 LSCs) network-related database tables, RED bandwidth managers, and other network-level infrastructure data. To the maximum extent practical, the DISA DRSN service manager must attempt to notify O&M activities before implementing DRSN nodal switch network-level database changes and/or network controls.
4. During emergencies, DISA has the authority to use direct write capabilities to implement switch database revisions required for operation and management of the DRSN.
5. DISA will take necessary action to establish capabilities and procedures necessary to sustain the DRSN and VoSIP/CVVoIP in the event of a failure of the RNOSCs and to reconstitute a major DRSN nodal element in the event of a catastrophic failure.

6.2.2.12 Directory (white pages) Services

The CVVoIP (VoSIP) extension of the DRSN will have a directory look-up services (White Pages) capability that allows a subscriber to look up directory numbers assigned to other CVVoIP subscribers. It is anticipated that by FY 2012 a multi-vendor standards compliant

Section 6.2 – Unique Classified Unified Capabilities Requirements

directory schema will be implemented. Requirements to be defined for directory services are detailed in [Section 6.2.6.9](#).

6.2.2.13 Conferencing Requirements

The CVVoIP services will not provide the full conferencing features inherent with the DRSN. The CVVoIP conferencing features are currently limited to 3-way calling and preset conferencing. Enhancements based on implementing “Meeting Place” servers at selected DISN core nodes are under consideration.

6.2.2.14 CVVoIP Equipment Certification and Testing Policy

Interoperability and Information Assurance testing of CVVoIP equipment will follow the standard process outlined in UCR 2008 Section 4.5. Unified Capabilities Approved Product List Process.

6.2.3. VoSIP Migration to the DISN CVVoIP

[Figure 6.2.3-1](#) provides an overview of the integrated migration strategy for the VoSIP migration to CVVoIP. The left side of the figure illustrates today’s environment. Currently, the DRSN is providing critical classified voice and conferencing services using time division multiplexing (TDM)/circuit switched technologies. The VoSIP employs the Secret Internet Protocol Routing Network (SIPRNet) and single-vendor (Cisco®) voice equipment.

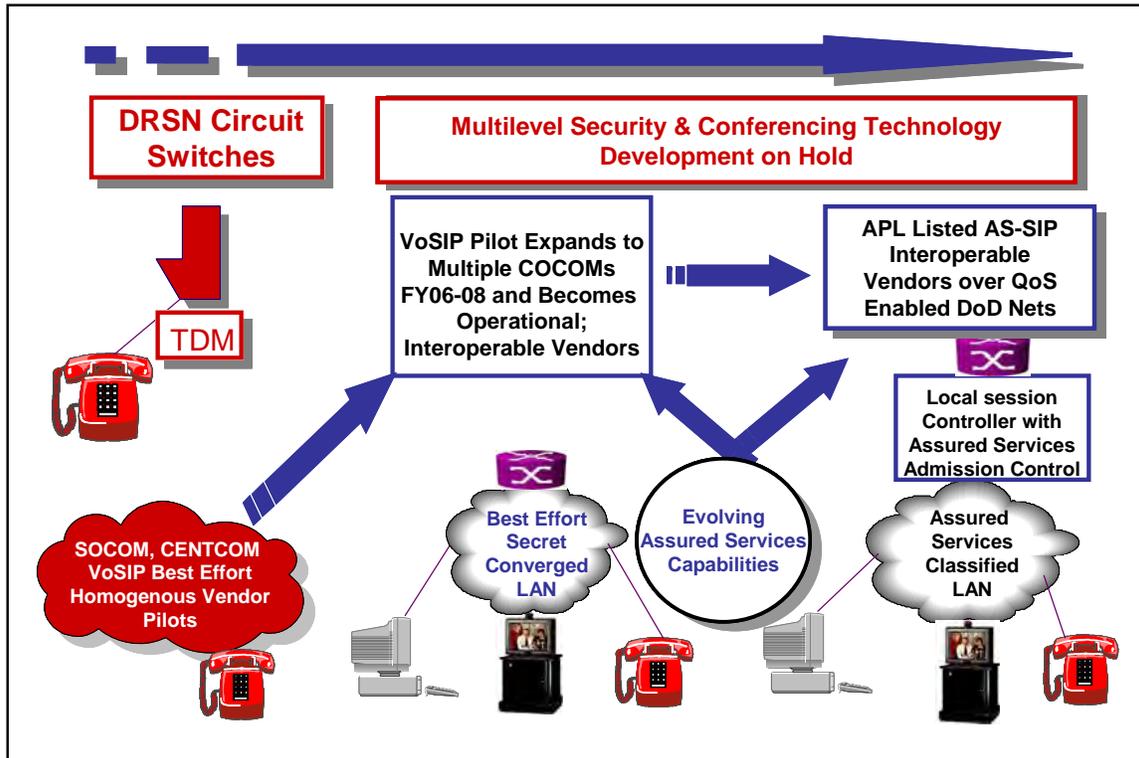


Figure 6.2.3-1. VoSIP Migration to DISN CVVoIP

On the right side of the figure, the target Net-Centric CVVoIP solution is shown. The future target is an all IP solution using the DISN WAN that will provide Quality of Service (QoS) and Edge solutions, which will provide ASLANs. These ASLANs will have functionality to provide bandwidth allocation for voice and video based on precedence among voice, video, collaboration, time critical messaging, and other service offerings (e.g., e-mail, Net-Centric Enterprise Services (NCES Web portals). The ASAC will provide the required PBAS to replace multilevel precedence and preemption (MLPP) on the WAN. AS-SIP signaling will be used to set up and take down the CVVoIP sessions and will allow multiple vendors to provide systems based on the UC APL. The ASLAN will support fully converged services meeting the performance and security requirement of each service.

The connection between today's systems and the future target is the major migration challenge. The DRSN's unique features of MLS and conferencing require both IP technology development and the expansion of the vendor base for these features to try to create a competitive market. A multivendor MLS market may not be practical, while a multivendor conferencing market must be practical. Investment is essential for this collaborative Government and industry effort. Until this investment is made and the effort succeeds, all Nuclear command and control (C2) users will continue to get their service via the legacy DRSN. As a result, the CVVoIP requirements will be focused initially on a single security level (SECRET). Currently, the VoSIP Pilot is being expanded to include multiple COCOMs and is open to all vendors when they meet the VoSIP

Section 6.2 – Unique Classified Unified Capabilities Requirements

Pilot technical requirements and can provide AS-SIP. A dual-signaling directory/gatekeeper (Tier0 SS) will be deployed to allow users to migrate from the signaling protocol of the pilot to a fully AS-SIP signaling environment. The work (i.e., system design, engineering, assessment and pilot testing, GSR) on both sensitive but unclassified (SBU) and CVVoIP will be leveraged to evolve the assured services capabilities to allow CVVoIP products to be placed on the UC APL.

An end-to-end view of the DRSN/VoSIP IP migration strategy needed to meet the CVVoIP migrations is illustrated in [Figure 6.2.3-2](#), DISN CVVoIP Convergence Migration Strategy Overview.

The top of [Figure 6.2.3-2](#) shows the current VoSIP capability, which is a Single Security Level Best Effort service over the SIPRNet, using the H.323 signaling protocol. The DISN Video Services II (DVS II) video teleconferencing (VTC) IP services and data services, ranging from e-mail to Web services to C2 applications, are also sharing the same local area networks (LANs) and the SIPRNet backbone as IP converged services. However, the VoSIP Pilot is focused on only voice services. The DRSN circuit-switched services interface the VoSIP services via signaling and media gateways. The DRSN provides the critical MLS and conferencing services that IP technologies cannot provide currently. In addition, the DRSN circuit switches serve as the interface to critical interoperable services to national security networks, allies, and federal and civil agencies.

The bottom of the diagram shows the future CVVoIP services where AS-SIP signaling is used to allow for heterogeneous vendor edge APL solutions and for assured services to be provided end-to-end as a first step. A gateway to the DRSN provides access to the DRSN for selected users. A future step may be a limited phase-out of the DRSN and the phase-in of the multilevel security (MLS) and conferencing features of the DRSN pending a funded successful research, development, testing, and evaluation (RDT&E) program to develop the features in IP-based technologies.

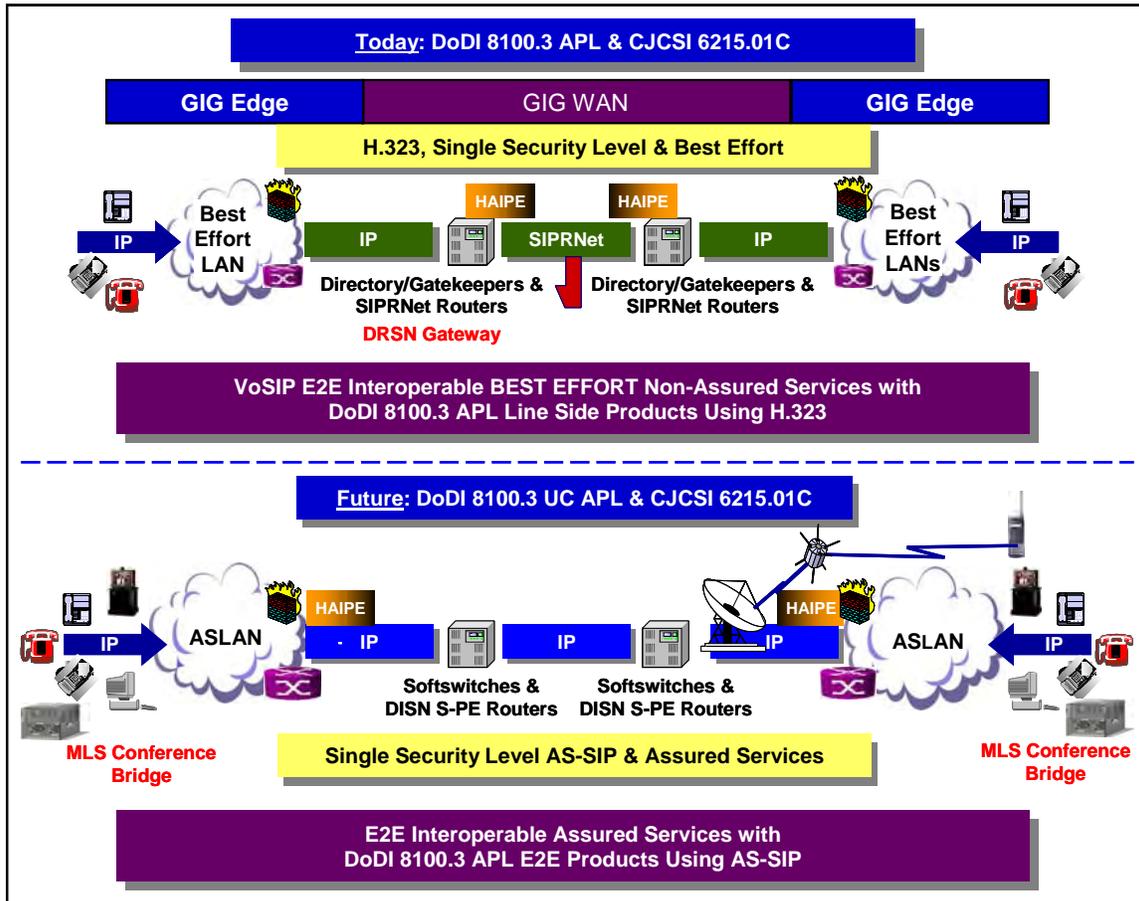


Figure 6.2.3-2. DISN CVVoIP Convergence Migration Strategy Overview

The current “Best Effort” VoSIP network must be upgraded to migrate from H.323 to AS-SIP, which will provide for assured information delivery end-to-end under conditions where bandwidth is restricted due to network damage, surge traffic, or tactical deployments. This migration provides a single level of security over the secret level DISN aggregation routers and is still dependent on the DRSN for MLS and conferencing services.

The progress being made by the National Security Agency (NSA) with respect to the modifications needed to High Assurance Internet Protocol Encryptor (HAIZE) and cross-domain solutions to allow RSVP to achieve its full potential will be monitored closely.

An upgrade to the VoSIP Directory/Gatekeeper to support both H.323 and AS-SIP signaling will be conducted and the Gatekeeper will be placed on the UC APL. Interoperable Classified VVoIP vendors will be tested and placed on the UC APL for CVVoIP products using AS-SIP. Thus in FY2010, the operational VoSIP services can begin migration to Assured Services vice “Best Effort” enabled by AS-SIP based on available funding by the MILDEPs to upgrade their existing systems as part of their normal scheduled upgrades.

Section 6.2 – Unique Classified Unified Capabilities Requirements

The migration of the DRSN MLS and Conferencing features to IP technologies cannot be described at this time since extensive RDT&E has not yet begun.

The DRSN circuit-switched network could phase out eventually if:

1. UC Migration Classified MLS system design, system engineering, UCRs and test programs are completed. The FY08 System 70% Design and UCR 2008 must be validated in the DISN VVoIP Spiral deployment of capabilities. This will provide the VVoIP foundation upon which the migration to classified unified capabilities can be implemented using future versions of the UCR consistent with major policies and requirements for Net Centricity and NetOps that are continuing to be refined and matured. In addition, the RDT&E program to develop MLS IP technologies must be successfully completed and result in a UCR that both DIA and NSA approve.
2. DISN WAN and MILDEP Intranets Service Level Agreements for Quality of Service Capabilities are available. Assured services requirements capabilities projected to be available by FY2010 include: assured service SLAs (e.g., non-blocking Grade of Service (GoS), voice and video quality, packet loss, jitter, latency, availability, DSCPs from the GIG QoS Working Group, PHB determined by supporting network based on VVoIP SLAs).
3. UC APL Assured Services Solutions are available. All IP solutions necessary to replace the circuit switched services are on the APL.
4. Deployment is completed for dual signaling H.323/AS-SIP SSs which allow for secure interoperability among multiple vendors and mixed technologies.
5. UC Master Plan is approved.
 - a. DoD plans and programs to fund, purchase, and install hybrid MFSSs and, ultimately, migrate to pure SSs for SBU voice and video.
 - b. The DoD components plan and program to fund, purchase, and install VVoIP Edge systems from the APL.
 - c. The DoD tactical community plans and programs to fund, purchase, and install VVoIP APL Edge systems or obtain a Joint Staff-approved Information Support Plan.

6. UC Master Plan is executed. Detailed joint transition and cutover planning unique to each theater and country will be required.

6.2.4 Classified Unified Capabilities Technical Design Framework

The Classified UC technical design will initially be focused on VVoIP. The CVVoIP technical design will transform in each of the three target time frames: 2009, 2012, and 2016. Due to funding and technology maturity, in all three timeframes, CVVoIP will be provided by three types of designs: 1) FY2008/2009 Hybrid with DRSN and VoSIP Pilot design, 2) FY2009 Hybrid with DRSN and CVVoIP converged at the Edge, and 3) Post-FY16 goal design of IP E2E. [Figure 6.2.4-1](#), CVVoIP FY2008/2009 Hybrid Design, illustrates the FY2008/2009 Hybrid with DRSN and VoSIP Pilot designs. The top of the figure illustrates that the current VoSIP Pilot design, which uses H.323 signaling, is a single security level with “Best Effort” over the SIPRNet. This design cannot provide precedence and preemption to support bandwidth on demand based on mission priorities consistent with situational awareness.

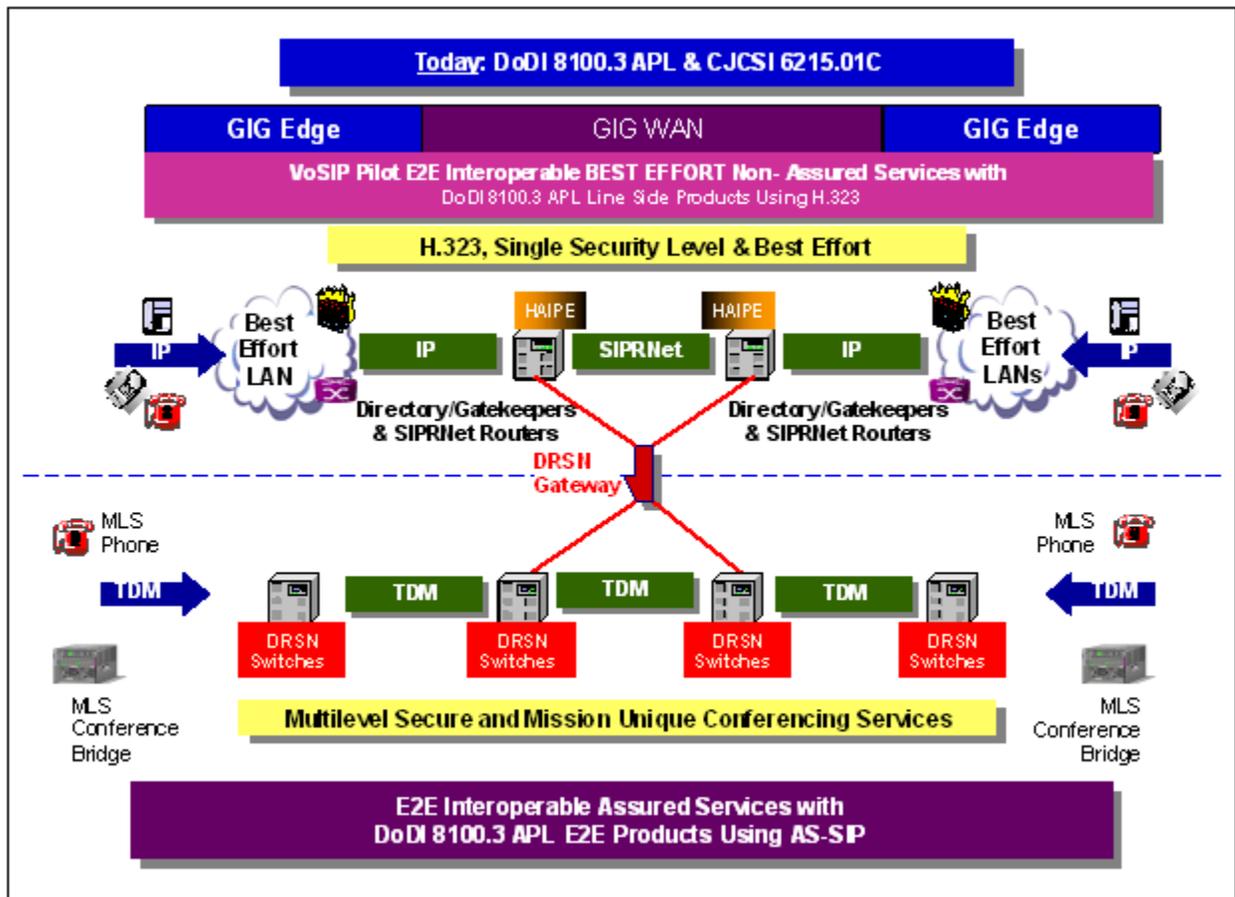


Figure 6.2.4-1. CVVoIP FY2008/2009 Hybrid Design

Section 6.2 – Unique Classified Unified Capabilities Requirements

[Figure 6.2.4-2](#), DISN CVVoIP FY2009 Design Overview, illustrates the FY2009 design, which is the first major step in the VoSIP migration to allow for IP converged operations at the Edge and for precedence and preemption to support bandwidth on demand based on mission priorities consistent with situational awareness. This is achieved by using the SBU VVoIP APL solutions with augmented AS-SIP signaling. In addition, this design extends assured services to the tactical community through the DISA Teleport program and because of collaboration with the tactical programs in the development of their ISP and tailored ISPs. The implementation of these designs is dependent on the continued updating of policy to address the potential phase-out of the DRSN with an all IP-based system (e.g., CVVoIP).

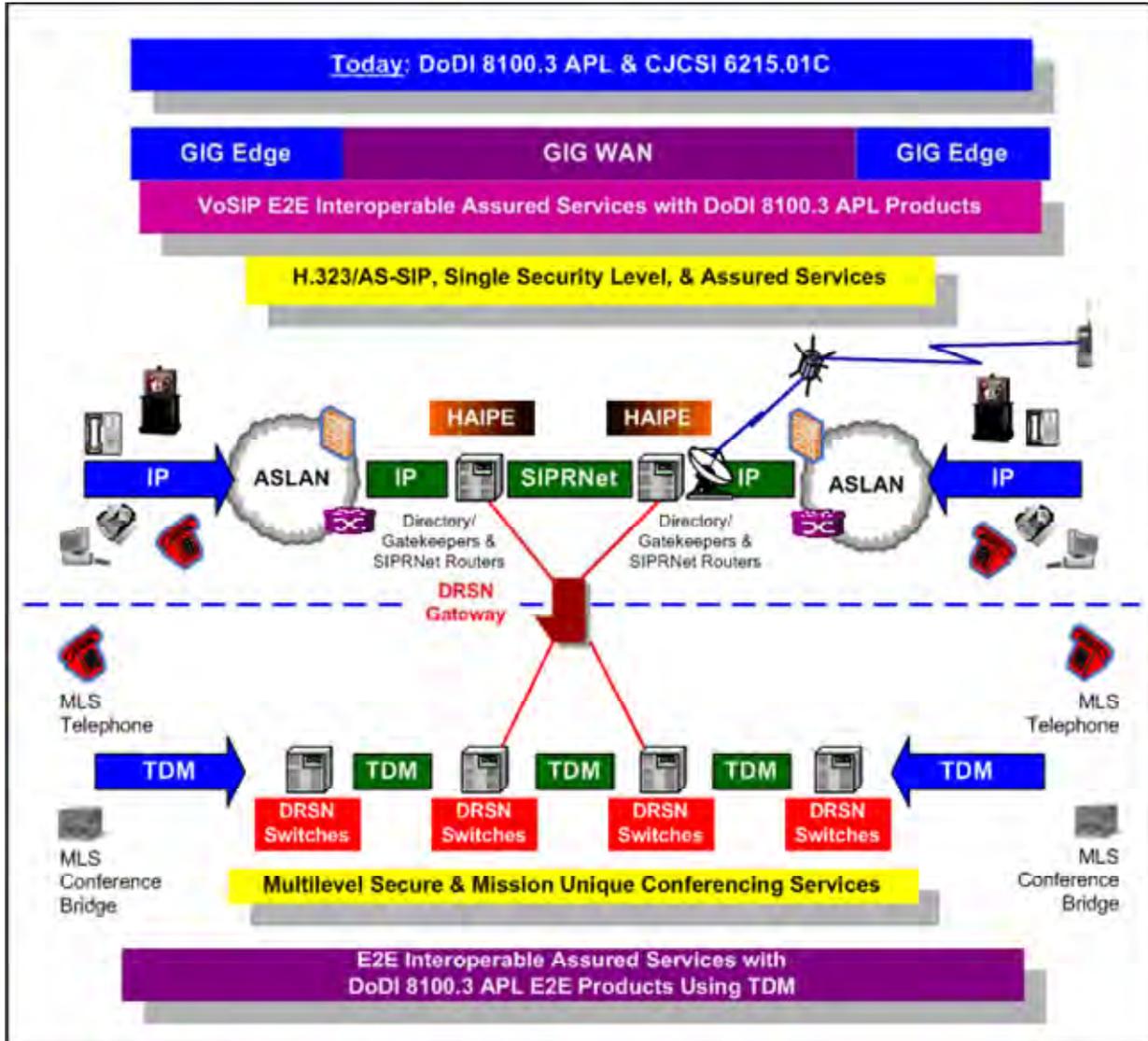


Figure 6.2.4-2. DISN CVVoIP FY2009 Design Overview

Figure 6.2.4-3, Three Tier Design of the VoSIP Associated with the CVVoIP FY2009 Design, illustrates the three-tier design of the VoSIP associated with the CVVoIP FY2009 design, as it migrates from a Best Effort voice service based on H.323 signaling to an assured services CVVoIP based on AS-SIP signaling.

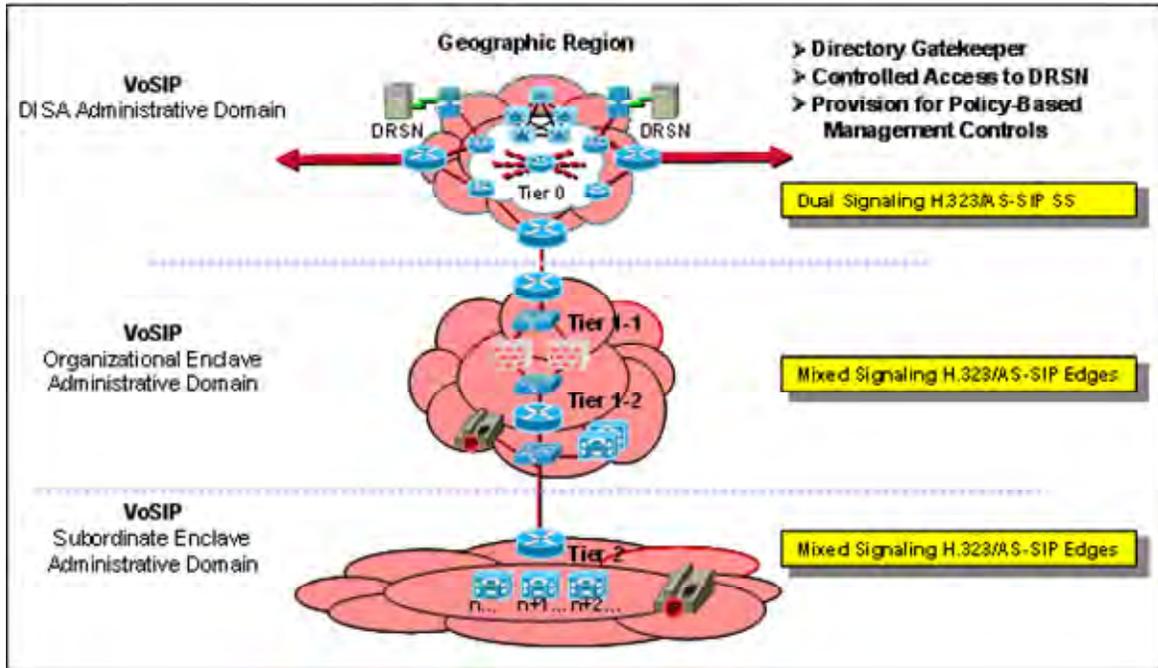


Figure 6.2.4-3. Three Tier Design of the VoSIP Associated with the CVVoIP FY2009 Design

6.2.5 Technical Design for 2009

Figure 6.2.5-1, Overview of CVVoIP Assured Services Design for FY2009, illustrates the CVVoIP technical design for assured classified services at a single security level in the 2009 time frame. The red text illustrates the significant changes introduced to achieve end-to-end CVVoIP with assured service. The design is similar to the one that will be used by the SBU VVoIP with the following significant differences:

The Secret Provider Edge (S-PE)/Secret Customer Edge (S-CE)/Secret Aggregation (S-A) routers versus the Unclassified Provider Edge (U-PE)/Unclassified Customer Edge (U-CE)/Unclassified Aggregation (U-A) routers will be used.

HAIPE will be used with the S-PE router.

There may possibly be variations in the version of AS-SIP that will be used.

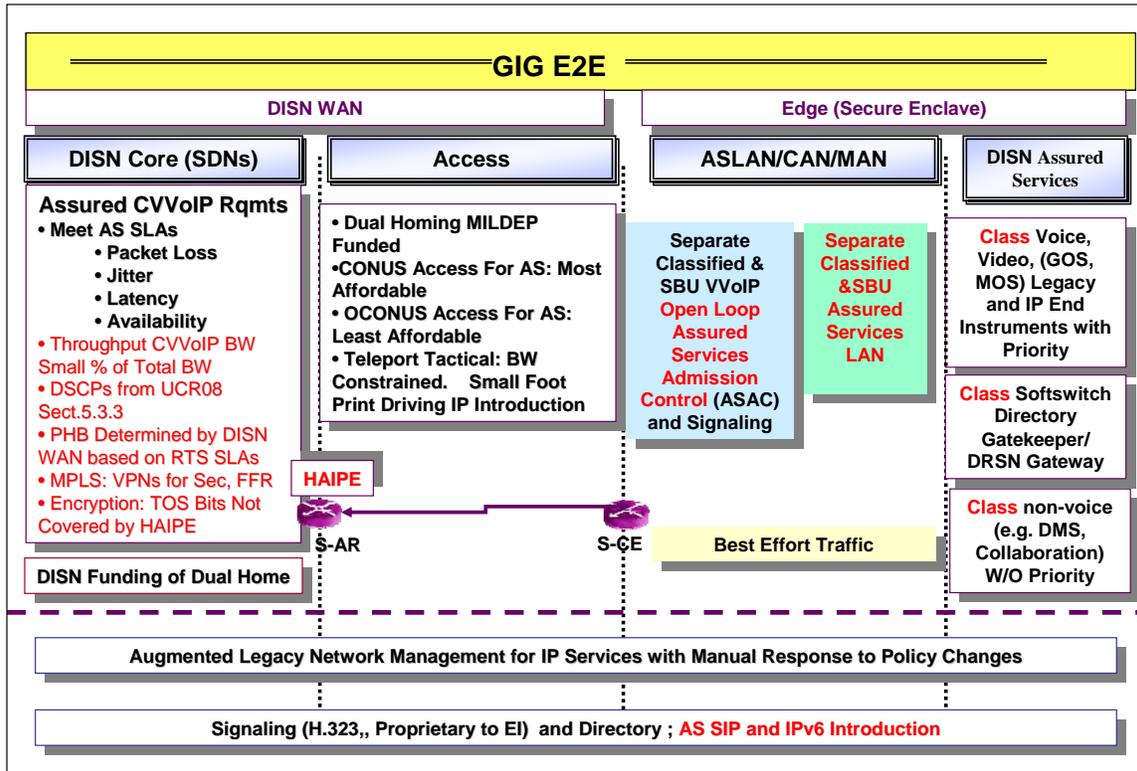


Figure 6.2.5-1. Overview of CVVoIP Assured Services Design for FY2009

The classified SS, called a Directory/Gatekeeper, is pure IP without a TDM signaling capability, and provides a unique interface to the DRSN.

Both networks depend on the robustness of the DISN WAN and its ability to meet SLAs for CVVoIP as illustrated by the list in the DISN Core portion of the chart.

In this time frame, TDM-based classified video service for services will be H.320 (KIV-7 encrypted) over the legacy DSN switches for users who have not yet migrated to IP. Single security level IP-based secure video over SIPRNet is available from secure enclaves. Multilevel secure video will be provided by integrated services digital network (ISDN) and KIVs that allow unencrypted signaling, and then transition to an encrypted bearer mode. This is because no MLS IP encryptors are available to support IP video services. The DVS II hubs will interoperate with the legacy ISDN H.320 services as well as with IP video H.323 users. Users will be encouraged to convert to IP video services when AS-SIP with the full H.323 feature set is available some time in 2009. Nevertheless, until NSA develops an IP replacement for the KIV, multilevel secure services will have to be over the DSN ISDN circuit-switched services.

6.2.5.1 *FY2009 Signaling Design*

The signaling design for this time frame has to provide both backward and forward technology capabilities. Thus, channel associated signaling (CAS) and primary rate interface (PRI) in the DRSN has to interoperate with H.323 signaling in the VoSIP Pilot to be followed by H.323 and AS-SIP interoperating in CVVoIP until all IP services are via AS-SIP. Once that is achieved, the DRSN interoperability must be maintained until its features can be replicated with IP technologies.

The hybrid CVVoIP signaling design for FY08 is depicted in [Figure 6.2.5-2](#). The signaling design is constructed as a two-tier hierarchy consisting of a ‘local’ level and a ‘backbone’ level. At the local level, LSCs are located in secure enclaves and represent the level of the signaling hierarchy closest to the EIs. The local level is based on a multi-vendor assortment of LSCs. The backbone, or Tier0 signaling level is of a robust, homogeneous design based on a current vendor-unique geographic cluster arrangements of Tier0 SS used in VoSIP. The CVVoIP Assured Services signaling backbone will be based on the Tier0 SS cluster concept, with AS-SIP as the CVVoIP signaling method, but during the transition period from VoSIP to CVVoIP there will also be segments using H.323 signaling.

The backbone Tier0 SSs represent the upper level of the signaling hierarchy and provide inter-enclave as well as inter-geographical area signaling forwarding. Some of the LSCs as well as a few, select Tier0 SSs provide ‘Managed Services’ to a limited set of EI and therefore a Tier0 SS may also have an LSC function associated with it.

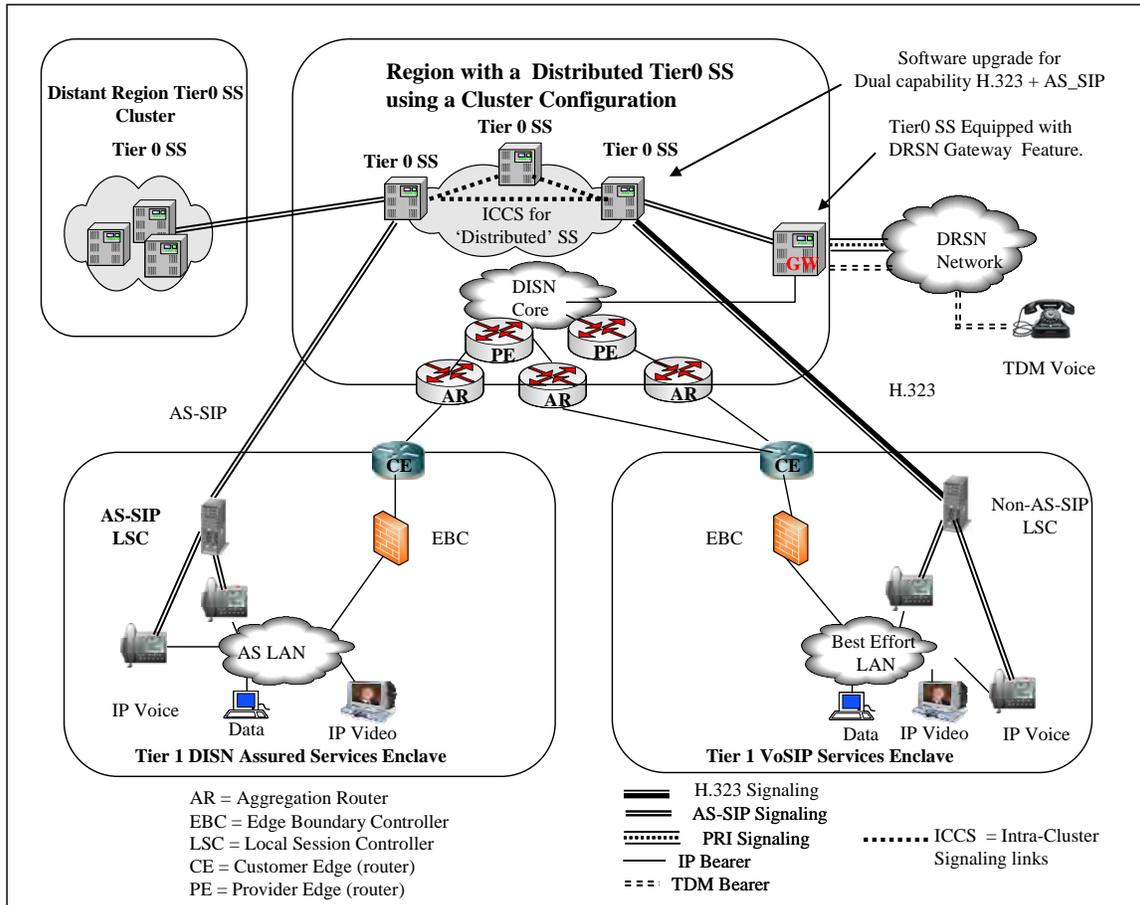


Figure 6.2.5-2. DISN CVVoIP FY2009 Signaling Design

Every LSC is assigned to a primary Tier0 SS and to at least one secondary Tier0 SS for automatic failover.

A Tier0 geographic cluster typically consists of at least three Tier0 SSs. The clustered SSs are connected over proprietary Intra-Cluster Communication Signaling (ICCS) links and automatically update each other’s databases as required in response to configuration changes within the geographic region controlled by the cluster, and as such, can be viewed as a distributed SS. This feature provides an extremely robust Tier0 signaling design enabling automatic non-service interrupting failover in the case a Tier0 SS goes down. The distance between the clustered SSs must be planned so that the maximum round-trip time (RTT) between the clustered SSs does not exceed 40 ms. Based on a propagation delay of 6 microseconds per kilometer without any other network delays being considered, this translates to a maximum theoretical transmission distance of approximately 1860 miles.

Section 6.2 – Unique Classified Unified Capabilities Requirements

To simplify the signaling path description below, the term Tier0 SS from here on refers to a geographic clustered Tier0 SS. Note that during a transition period, H.323 and AS-SIP will coexist at certain locations. All session signaling messages received by a LSC from local EI and intended for a destination outside the secure service enclave is sent by the LSC in the form of an AS-SIP message to its assigned Tier0 SS. The Tier0 SS then forwards the AS-SIP message to the distant-end by either forwarding the message directly to the distant-end LSC or to a Tier0 SS located in a different geographic area; this Tier0 SS then, in turn, forwards the message to the distant-end LSC. Similarly, all session signaling messages sent from a remote location and intended for IP EIs associated with a given LSC will be routed to the Tier0 SS assigned to the destination LSC and the Tier0 SS will forward the AS SIP signaling messages to the destination LSC.

The basic AS SIP message flow between an originating LSC assigned to one backbone geographic cluster Tier0 SS and a destination LSC assigned to another backbone geographic cluster Tier0 SS is:

Originating LSC --- Tier0 SS 1 ----- Tier0 SS 2 --- Destination LSC

The basic AS SIP message flow between an originating LSC and a destination LSC assigned to the same Tier0 SS is:

Originating LSC --- Tier0 SS --- Destination LSC

The access link between the CE router and the AR is resource constrained and the LSC has primary responsibility for ensuring that the telephony 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 Tier0 SS is responsible for implementing a policing function to protect the access links (and to protect the classified network itself) whereby the Tier0 SS intervenes by blocking session requests or preempting session requests and active sessions when the Tier0 SS determines that the LSC has exceeded its provisioned threshold for voice traffic or video traffic.

6.2.6 Modifications to the SBU Assured Services Requirements to Include CVVoIP - Unique Requirements

UCR 2008, Section 5.3.2 addresses the functions, methods, protocols, and associated technical parameters for the EI, LSC, MFSS, EBC, and NM components of the DISN VVoIP System. UCR 2008, Section 5.3.4 provides requirements for the SBU version of AS-SIP.

This Section (6.2.6) addresses the AS requirements that are unique to the CVVoIP Services.

In general, the majority of the SBU requirements are applicable and common to both the SBU and Classified VVoIP services. The following modifications and additions to the SBU requirements are caused by unique CVVoIP requirements:

6.2.6.1 Voice End Instrument

1. Voice EI requirement UCR 2008, Section 5.3.2.6.1 defines a CAC-enabled instrument as a CONDITIONAL requirement. For Classified instruments, this is **REQUIRED**.
2. New exclusive requirement for Classified Instrument: Display CAL (Security Level) of the call.
3. New exclusive requirement for Classified: Phone browser or menu capability to access System-wide White Pages directory. (Objective FY 2012 requirement)

6.2.6.2 Classified LSC Requirements

6.2.6.2.1 USB LSC Requirements not applicable to Classified LSC

The following LSC Requirements defined in UCR 2008, Section 5.3.2.7 do not apply to the classified LSC:

1. MG, SG for SS7 (the Classified LSC's do not interface to external networks)
2. Public safety features (e.g., PSAB, E911 access)

6.2.6.2.2 Classified LSC Unique Requirements

The following requirements are unique to Classified LSCs:

- Located in Secure enclave
- PDS cabling per DRSN requirements
- DHCP not allowed, strict control of EI Assignments
- Use the Classified version of AS-SIP Signaling

6.2.6.3 Network- Level SS

While UCR 2008, Section 5.3.2.8 discusses the MFSS, the CVVoIP system employs a simpler backbone SS referred to as a Tier0 SS.

Section 6.2 – Unique Classified Unified Capabilities Requirements

1. **[Required: Tier0 SS]** Needs to handle both H.323 Directory/Gatekeeper functionality and AS-SIP. As well as inter-working between the two signaling methods. (This is a transitional requirement until VoSIP becomes all AS SIP-based e.g., CVVoIP).
2. **[Required: Tier0 SS]** Managed Services. Managed Services is the term used to describe the situation where a limited, few subscribers are served on a remote basis from either an LSC or the LSC function of a Tier0 SS. The subscribers are located in a remote secure enclave and provided secure (encrypted) access to the LSC.
3. **[Required: Tier0 SS]** Numbering Plan/Addressing compatibility with VoSIP, DRSN, Tactical Global Block Numbering Plan, SIPRNet IP Addressing Schema.
4. **[Conditional: Tier0 SS]** No MFSS TDM capabilities except as noted for the MG function at selected locations.
5. **[Not Required: Tier0 SS]** Public Safety Features (e.g., PSAB, E911 access).

6.2.6.4 *Media Gateway with Signaling Interworking*

The only MG used in the FY 2008 CVVoIP system is a unique interface between the Classified Tier0 SS and a DRSN Switching System. This MG performs two functions:

1. Media conversion
2. Signaling conversion

The DRSN ‘trunk side’ employs a modified version of a vendor-unique PRI trunk. The MG performs media conversion between the IP-bearer stream and T1- based media stream. (T1 format is ESF, B8ZS.) In addition, this MG also acts as a ‘SG’ in that it converts the current H.323-based signaling to the DRSN interface trunk signaling (a vendor-variant of PRI with two data elements modified to carry SAL-level of the call and precedence level).

For FY 2008, all interfaces to external non-CVVoIP and non-DRSN networks are through DRSN interfaces (e.g., STU-IIIR protected access, or encrypted access using KG-xx, KIV-7, etc).

1. **[Required: MG]** Tier0 SS: AS-SIP signaling to DRSN-unique signaling conversion
2. Objective FY 2012 Requirement: AS-SIP signaling and MG via encrypted access to non-secure (unclassified) networks (such as the DSN, PSTN).

6.2.6.5 *Signaling Gateway*

UCR 2008, Section 5.3.2.13 defines the SG as a signaling gateway exclusively for translating between AS-SIP and SS7 Signaling. Since the CVVoIP system does not interface with any SS7-based network, this requirement does not apply to the CVVoIP system.

6.2.6.6 *Edge Boundary Controller*

All requirements for the EBC specified in UCR 2008, Section 5.3.2 apply to the CVVoIP system.

Additional EBC requirement for the CVVoIP System:

1. The EBC must be dedicated to CVVoIP services and not shared with SBU services.

6.2.6.7 *Addressing Schema for LSC*

The following are all additional requirements unique to the Classified LSCs:

1. **[Required: LSC]** DRSN and VoSIP numbering Plan Capability
2. **[Required: LSC]** Interoperability with Tactical Global Block Numbering Plan (GBNP)
3. **[Required: LSC]** SIPRNet IP addressing Schema

6.2.6.8 *Network Management*

All requirements specified in UCR 2008, Section 5.3.2.17 for NM apply to the Classified LSC, EBC and Tier0SS.

The following unique features are required for classified:

1. **[Required: LSC]** The LSC shall generate an alarm message indicating that a secure phone has been unplugged.
2. **[Required: LSC]** The NM system shall have the capability to mark certain EIs as ‘high-interest items’. This feature is used by network control personnel to analyze failure of specific phone calls (e.g., 4-star users).

6.2.6.9 White Pages Directory Services

The CVVoIP extension of the DRSN will have a directory look-up services (White Pages) capability that allows a subscriber to look up directory numbers assigned to other CVVoIP subscribers. This is a FY 2012 OBJECTIVE requirement and is included here for consideration by product development teams. The directory system will be of the same design and hardware as for SBU VVoIP, but for security reasons, this will be an implementation separate from the SBU system. It is anticipated that by FY 2012 a multi-vendor standards-based directory schema will be implemented. [Figure 6.2.6-1](#) illustrates a centralized white pages directory arrangement.

Decisions need to be made concerning requirements for the following items:

- Use of External ‘Corporate’ Directory:
 - Location
 - Maintenance Responsibility
 - Synchronization with the local (LSC) Directories

- Definition of Multi-Vendor Standards for Directory Data Items:
 - Length of each field (# of Characters)
 - Common Set of Fields to be used (LSC and ‘Corporate’)
 - “Ownership” and control of each data Field
 - Coordination of LSC and external directory formats

- Definition of Instrument Display Fields:
 - -Character Fields
 - -Length of Fields
 - -How many/which Fields
 - -Soft/hard key functions such as a ‘directory access button’

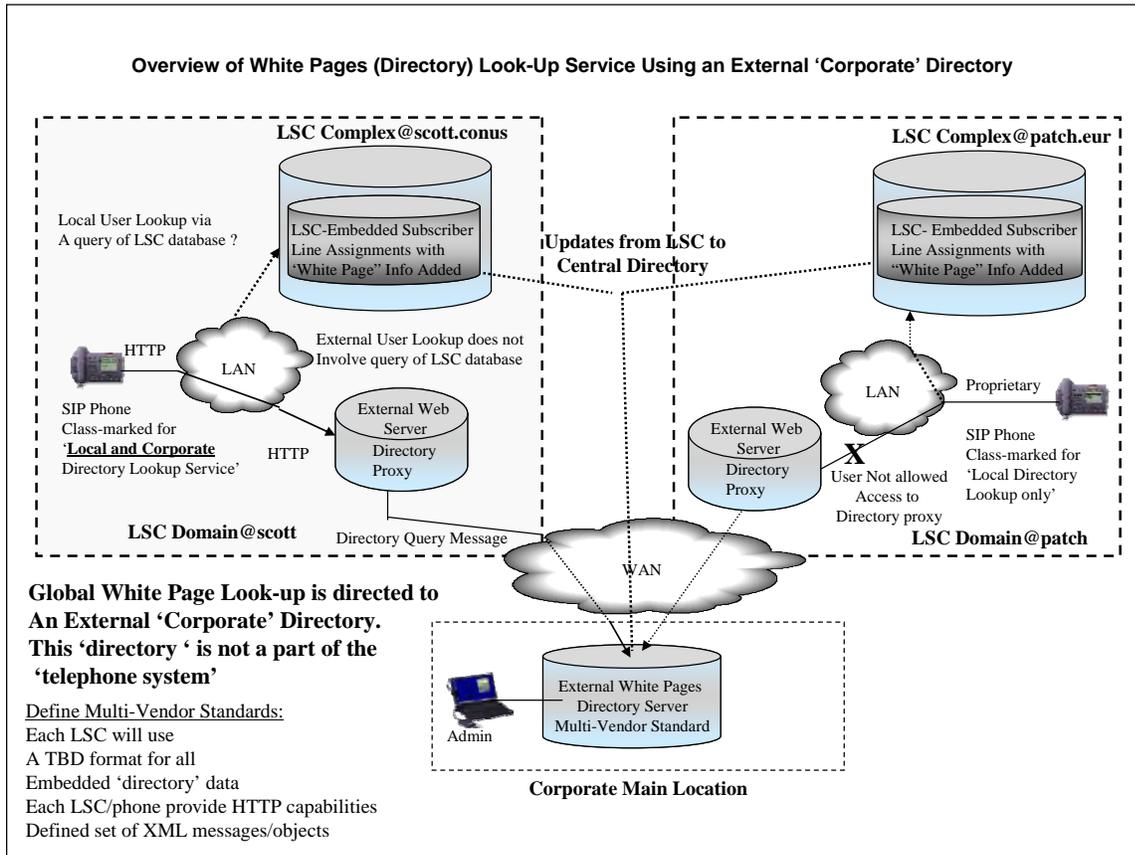


Figure 6.2.6-1. Centralized White Pages (Directory) Service

6.2.6.10 Voice Quality

The classified system has the following classified voice quality requirement:

The EI-to-EI voice quality of a telephone connection is subjective and is determined from the complex interaction of multiple switching, speech encoding, voice compression techniques, and transmission parameters. The objective of the system is to provide toll quality secure-voice service on a user-to-user basis, and to ensure the highest practical voice quality when users are interfaced to external systems and equipment. The voice quality requirement is defined as receiving a score of at least 90 on the Diagnostic Rhyme Test (DRT) defined by ANSI S3.2-1989 standard, and a score of at least 60 on the DAM. The DRT measures intelligibility, and the DAM measures quality. These objective intelligibility and quality scores are achieved by adhering to the DoD, national, vocoding, and international transmission design and operational standards. For the DRSN voice quality is addressed in the development of new vocoders for DRSN interfaces and voice compression algorithms for the network. Routine day-to-day assessment of voice quality occurs at the user level with problem reporting to the site voice operations and maintenance support activity for resolution.

6.2.6.11 Call Set-up Time

The following call set-up times apply to the classified VVoIP network:

1. For LSC Intra-enclave calls the average delay should be no more than one second. For the 95% of calls, the delay should not exceed 1.5 seconds during normal traffic conditions.
2. For inter-enclave and worldwide calls within the classified environment average delay should not exceed 6 seconds, with 95% of calls not to exceed 8 seconds during normal traffic conditions.

6.2.6.12 Unique Network Infrastructure Requirements for CVVoIP

The following requirements are found under the SBU network infrastructure requirements but are restated here to make the point that they are applicable to the HAIPE environment too. By keeping the Maximum Transmission Unit (MTU) as specified, the addition of encryption will not result in packet fragmentation.

1. **[Conditional]** If the classified Edge System appliance supporting VVoIP uses an Ethernet interface for connecting to the LAN, then its NIC MTU size shall be set to 1280 bytes.
NOTE: This will allow for overhead associated with encryptors or VPNs.
2. **[Required]** The DISN Core Network shall be traffic engineered to ensure that VVoIP media E2E completion of sessions above ROUTINE are ensured under the worst-case failure conditions. NOTE: This requirement is to ensure that the DISN Core continues to try to find a path for sessions above ROUTINE if a path exists even though the path may be suboptimal (i.e., a satellite connection that does not meet the SLA). NOTE: This requirement assumes the DSCP discriminators exist between ROUTINE and above ROUTINE VVoIP sessions across the encryption boundaries (i.e., HAIPE).

[Figure 6.2.6-2](#) illustrates where encryption elements fit within the FY08 architecture.

6.2.6.13 Unique IA Requirements for CVVoIP

All IA requirements are specified in UCR 2008, Section 5.4, *IA GSR*. In addition, the following requirements are unique to the CVVoIP services:

[Required: EI] The system shall be capable of being enabled/disabled using enable/disable codes.

NOTE: An enable code (password or PIN system) is required to restrict access to EIs. Classified EIs must be disconnected or disabled when they are not manned by appropriately cleared persons or when use of the EI is no longer required. The LSC should not be used to disable the EI based on date/time conditions.

[Required: EI] If the system supports an enable/disable code, the enable code shall be unique for that facility.

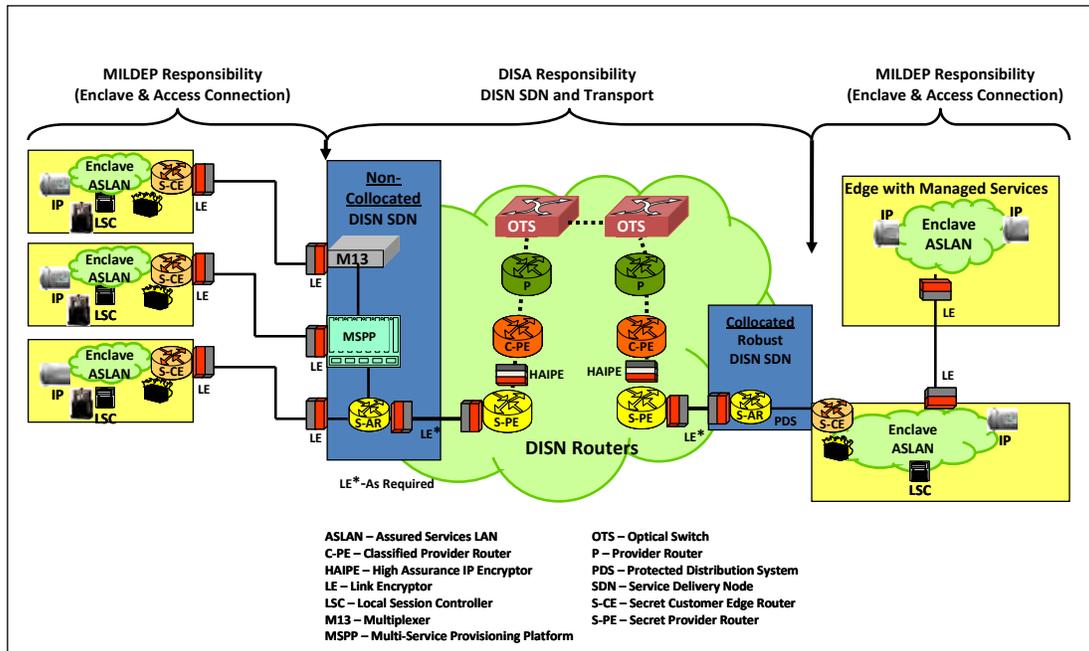


Figure 6.2.6-2. Addition of Encryption within the FY08 Network Infrastructure.

[Required: EI] If the system supports an enable/disable code, the code shall be able to be modified by an authorized authority.

[Required: EI] If the system supports an enable/disable code, the system shall have a configurable code aging parameter and the default shall be 90 days.

[Conditional: LSC, EI] The system shall use three-factor authentication to include PKI certificates and biometric mechanisms 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.

[Required: EI] The system shall be capable of meeting the DoD Public Key Enabled (PKE) requirements for PKI based authentication.

Section 6.2 – Unique Classified Unified Capabilities Requirements

Note: PKI is required for EIs, whereas in the SBU it is conditional. In summary, the EI is required to support PKI and all the PKI requirements apply.

[Required: Tier0 SS, LSC, MG, BC] The system shall be capable of detecting physical tampering to equipment cabinets and/or devices. NOTE: This requirement may be met by using anti-tamper tape and/or tamper proof screws or locks.

[Required: Tier0 SS, LCC, MG, BC] If the system supports classified users, the system shall be capable of ensuring that all unused network access device connections or physical ports are appropriately secured from unauthorized use by one of the following methods listed in preferential order:

- Ports are disabled (i.e., shutdown)
- Ports are assigned to an unused VLAN is applicable
- MAC based port security is employed on active ports
- Port authentication is employed using 802.1X
- VLAN Management Policy Server (VMPS)

[Required: Tier0 SS, LSC, MG, BC, 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:

- Invalid user authentication attempt
- Unauthorized attempts to access system resources
- Changes made in a user's security profile and attributes
- Changes made in security profiles and attributes associated with an interface/port
- Changes made in access rights associated with resources (i.e., privileges required of a user and a interface/port to access)
- Changes made in system security configuration
- Creation and modification of the system resources performed via standard operations and maintenance procedures
- Disabling a user profile

- Events associated with privileged users

[Conditional] If the system contains resources that are deemed mission critical (for example a risk analysis classifies it critical), then the system should log any events associated with access to those mission critical resources.

- Successful login attempts.
- Failed login attempts to include the following:
 - Failed login attempt due to an excessive number of logon attempts.
 - Failed logon attempt due to blocking or blacklisting of a user ID.
 - Failed logon attempt due to blocking or blacklisting of a terminal.
 - Failed logon attempt due to blocking or blacklisting an access port.
- Logouts.
- Remote system access.

NOTE: Only the last two bullets are additions to the CVVoIP (logouts and remote system access).

[Required: Tier0 SS, LSC, MG, BC, R, LS] The security log event record shall be capable of including at least the following information:

- Date and time of the event (both start and stop)
- User ID including associated terminal, port, network address, or communication device
- Event type
- Names of resources accessed
- Success or failure of the event
- Origin of the request (e.g., terminal ID)

NOTE: Only the last bullet is an addition for the CVVoIP(Origin of the request).

Section 6.2 – Unique Classified Unified Capabilities Requirements

[Required: Tier0 SS, LSC, MG, BC, R, LS] The system shall be capable of supporting an out-of-band (OOB) or direct connection method for system device management.

[Conditional: Tier0 SS, LSC, MG, BC, R, LS] If the system uses an OOB management method, it shall be capable of using a separate dedicated (closed network).

NOTE: This OOB network must use dedicated infrastructure, however, some portions of its connectivity may be via segregated logical circuits.

[Conditional: R] If the system uses an OOB management method, the system shall be capable of limiting management connections to authorized source IP addresses.

[Conditional: R] If the system uses an OOB management method, the system shall be capable of maintaining a separation between the management and production networks.

NOTE: This requires physically separate networks.

[Conditional: Tier0 SS, LSC, MG, BC, R, LS] If the system uses an OOB management method, it shall be capable of ensuring system management access using the following four security restrictions:

- Role based authenticated access control
- Strong two-factor authentication (e.g., Secure ID)
- Encryption of management and login sessions
- Auditing of security related events

[Conditional: Tier0 SS, LSC, MG, BC, R, LS] If the system uses in-band management, it shall be capable of restricting the sessions to a limited number of authorized IP addresses.

6.2.7 Classified AS-SIP unique Requirements

UCR 2008, Section 5.3.4 addresses the general AS-SIP Requirements. While the AS-SIP requirements for the Classified VoIP are almost identical to that of the SBU VoIP, this section addresses the AS-SIP requirements that are unique to the Classified VoIP.

6.2.7.1 Classified Signaling Environment

The classified signaling environment is unique in that it will employ a mix of an existing vendor-based H.323 and AS-SIP signaling during the transition period to all DISN CVVoIP. In addition, a unique MG capability exists as part of Tier0 SS.

The signaling design during the transition period has to provide both backward and forward technology capabilities. Thus, CAS and PRI in the DRSN has to interoperate with H.323

signaling in the VoSIP Pilot to be followed by H.323 and AS-SIP interoperating in the CVVoIP system until all IP services are via AS-SIP. Once that is achieved, the DRSN interoperability must be maintained until its features can be replicated with IP technologies.

The signaling design is described in UCR 2008, [Section 6.2.5.1](#), FY2008 Signaling Design. The design is also depicted in [Figure 6.2.7-1](#).

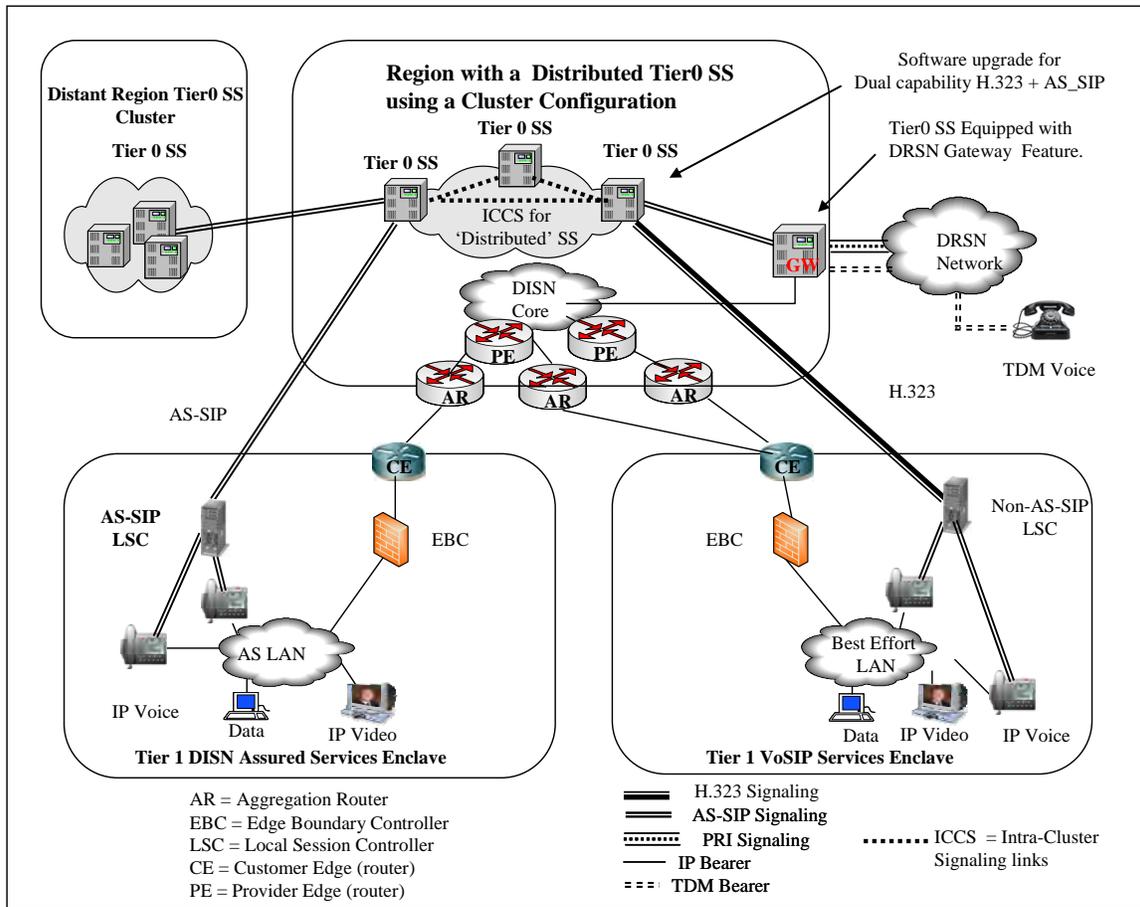


Figure 6.2.7-1. DISN CVVoIP FY2009 Signaling Design

To simplify the signaling path description below, the term Tier0 SS from here on refers to a geographic clustered Tier0 SS. (Please note that during a transition period, H.323 and AS-SIP will coexist at certain locations.) All session (call) signaling messages received by a LSC from local EIs and intended for a destination outside the secure service enclave is sent by the LSC in the form of an AS-SIP message to its assigned Tier0 SS. The Tier0 SS then forwards the AS-SIP message to the distant-end by either forwarding the message directly to the distant-end LSC or to a Tier0 SS located in a different geographic area; this Tier0 SS then, in turn, forwards the message to the distant-end LSC. Similarly, all session (call) signaling messages sent from a remote location and intended for IP EIs associated with a given LSC will be routed to the Tier0

SS assigned to the destination LSC and the Tier0 SS will forward the AS SIP signaling messages to the destination LSC.

6.2.7.1.1 IP Signaling Path Reference Cases

Based on the top-level signaling design depicted in Section 6.2.7.1, the signaling paths that must be supported in order to provide the Classified VVoIP services are identified in Figure 6.2.7-2 and Table 6.2.7-1.

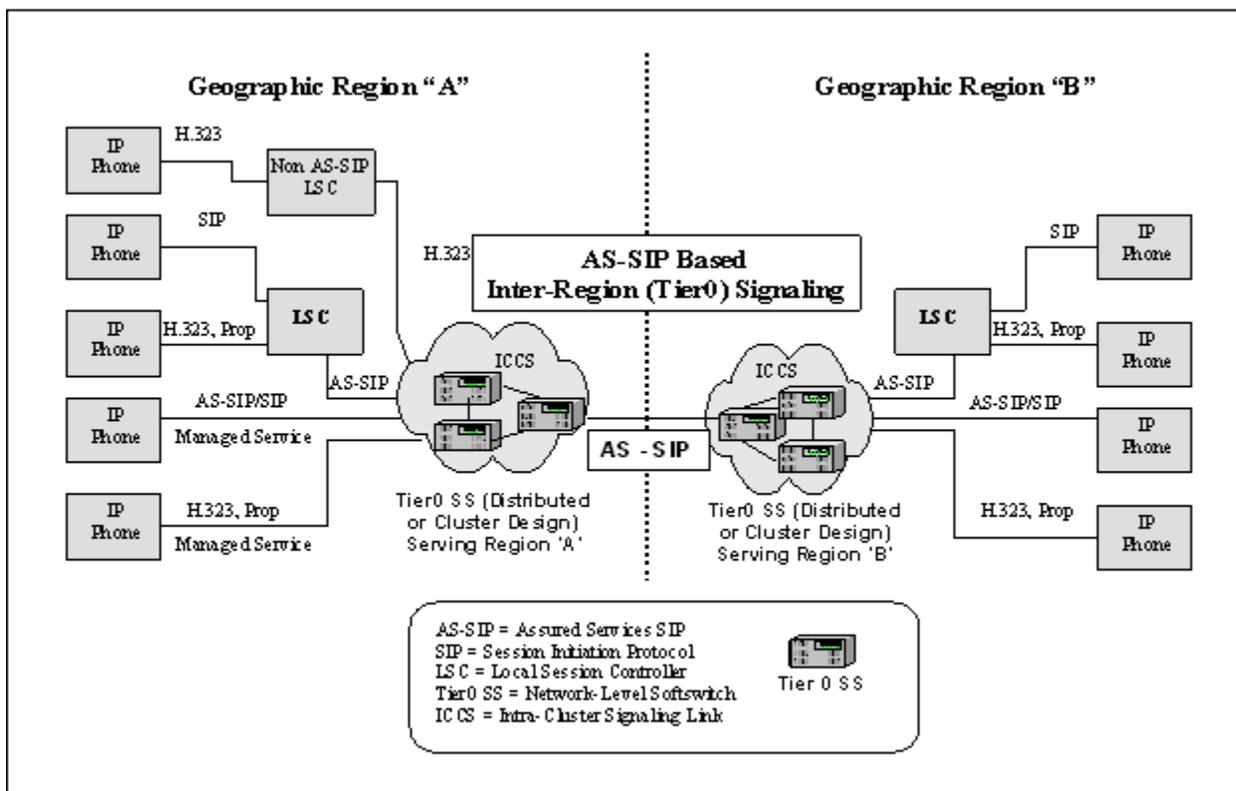


Figure 6.2.7-2. IP Signaling Path Reference Illustration

6.2.7.2 Differences Between SBU and Classified AS-SIP Requirements

UCR 2008 Section 5.3.4 AS-SIP Requirements defines both SBU and Classified requirements. The Classified-specific requirements are defined in Sections 5.3.4.7.3.1.5.1,-3, 5.3.4.7.3.1.10, -.15, 5.3.4.7.3.2.3, 5.3.4.7.3.3.5.1-3, 5.3.4.7.3.4.8-11, 5.3.4.7.4.1.11, 5.3.4.7.5b.1-8, 5.3.4.7.9.1-19.2, and 5.3.4.10.2.1.2.5,-8. In addition, sections that specify ‘domain name’, ‘namespace’, and/or ‘domain subfields define “DSN” as Required for the SBU environment, and “DRSN” as Required for the Classified environment.

The following sections describe detailed differences between the SBU and Classified AS-SIP requirements.

6.2.7.2.1 Nomenclature

- The Classified environment uses the term Tier0 SS (Tier0 SS) while UCR 2008 Section 5.3.4 AS-SIP Requirements uses the term SS to denote the SBU environment.
- The Classified environment uses “DRSN” as the network domain name while the SBU environment uses “DSN” as the network domain name.

FOR OFFICIAL USE ONLY

Unified Capabilities Requirements

Section 6.2 – Unique Classified Unified Capabilities Requirements

Table 6.2.7-1. 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
			LSC	AS-SIP	Tier0 SS	AS-SIP	Tier0 SS	AS-SIP	LSC		
1A	IP phone	SIP	LSC	AS-SIP	Tier0 SS	AS-SIP	Tier0 SS	AS-SIP	LSC	SIP	IP phone
1B	IP phone	SIP	LSC	AS-SIP	Tier0 SS	AS-SIP	Tier0 SS	AS-SIP	LSC	H323, Prop.	IP phone
1C	IP phone	SIP	LSC	AS-SIP	Tier0 SS	AS-SIP	Tier0 SS			SIP	IP phone
1D	IP phone	SIP	LSC	AS-SIP	Tier0 SS	AS-SIP	Tier0 SS			H323, Prop.	IP phone
1E	IP phone	H323, Prop.	LSC	AS-SIP	Tier0 SS	AS-SIP	Tier0 SS	AS-SIP	LSC	SIP	IP phone
1F	IP phone	H323, Prop.	LSC	AS-SIP	Tier0 SS	AS-SIP	Tier0 SS	AS-SIP	LSC	H323, Prop.	IP phone
1G	IP phone	H323, Prop.	LSC	AS-SIP	Tier0 SS	AS-SIP	Tier0 SS			SIP	IP phone
1H	IP phone	H323, Prop.	LSC	AS-SIP	Tier0 SS	AS-SIP	Tier0 SS			H323, Prop.	IP phone
1I	IP phone	SIP			Tier0 SS	AS-SIP	Tier0 SS	AS-SIP	LSC	SIP	IP phone
1J	IP phone	SIP			Tier0 SS	AS-SIP	Tier0 SS	AS-SIP	LSC	H323, Prop.	IP phone
1K	IP phone	SIP			Tier0 SS	AS-SIP	Tier0 SS			SIP	IP phone
1L	IP phone	SIP			Tier0 SS	AS-SIP	Tier0 SS			H323, Prop.	IP phone
1M	IP phone	H323, Prop.			Tier0 SS	AS-SIP	Tier0 SS	AS-SIP	LSC	SIP	IP phone
1N	IP phone	H323, Prop.			Tier0 SS	AS-SIP	Tier0 SS	AS-SIP	LSC	H323, Prop.	IP phone
1O	IP phone	H323, Prop.			Tier0 SS	AS-SIP	Tier0 SS			SIP	IP phone
1P	IP phone	H323, Prop.			Tier0 SS	AS-SIP	Tier0 SS			H323, Prop.	IP phone
2A	IP phone	SIP	LSC	AS-SIP	Tier0 SS	AS-SIP			LSC	SIP	IP phone
2B	IP phone	SIP	LSC	AS-SIP	Tier0 SS	AS-SIP			LSC	H323, Prop.	IP phone
2C	IP phone	SIP	LSC	AS-SIP	Tier0 SS					SIP	IP phone
2D	IP phone	SIP	LSC	AS-SIP	Tier0 SS					H323, Prop.	IP phone
2E	IP phone	H323, Prop.	LSC	AS-SIP	Tier0 SS	AS-SIP			LSC	SIP	IP phone
2F	IP phone	H323, Prop.	LSC	AS-SIP	Tier0 SS	AS-SIP			LSC	H323, Prop.	IP phone
2G	IP phone	H323, Prop.	LSC	AS-SIP	Tier0 SS					SIP	IP phone
2H	IP phone	H323, Prop.	LSC	AS-SIP	Tier0 SS					H323, Prop.	IP phone
2I	IP phone	SIP			Tier0 SS	AS-SIP			LSC	SIP	IP phone
2J	IP phone	SIP			Tier0 SS	AS-SIP			LSC	H323, Prop.	IP phone
2K	IP phone	SIP			Tier0 SS					SIP	IP phone
2L	IP phone	SIP			Tier0 SS					H323, Prop.	IP phone
2M	IP phone	H323, Prop.			Tier0 SS	AS-SIP			LSC	SIP	IP phone
2N	IP phone	H323, Prop.			Tier0 SS	AS-SIP			LSC	H323, Prop.	IP phone
2O	IP phone	H323, Prop.			Tier0 SS					SIP	IP phone
2P	IP phone	H323, Prop.			Tier0 SS					H323, Prop.	IP phone

NOTE: Reference cases 2A through 2P (see [Table 6.2.7-1](#)) represent the call paths when the same Tier0 SS serves both the calling party calling party’s LSC (or the calling party’s EI directly) and the called party’s LSC (or the called party’s EI directly).

6.2.7.2.2 Proxy-Require Header

The ‘Proxy-require’ header is REQUIRED in the classified environment because of the CAL parameter, but not required in the SBU environment. Therefore, this unique requirement has been added to sections 5.3.4.7.3.1, 5.3.4.7.3.2, and 5.3.4.7.3.3 in UCR 2008, Section 5.3.4 AS-SIP Requirements to form the complete set of Classified requirements as outlined below.

6.2.7.2.2.1 Modification to UCR 2008 Section 5.3.4.7.3.1 consists of adding the SIP header field ‘Proxy-Require’ as shown below:

6.2.7.2.2.1.1 The AS-SIP signaling appliances serving SIP EIs, and H.323 and proprietary IP EIs 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 (used for CAL)
Rack
Reason
Record-Route
Refer-To
Replaces
Require
Resource-Priority
Retry-After
RSeq
Session-Expires
Subscription-State

Section 6.2 – Unique Classified Unified Capabilities Requirements

Supported
To
Unsupported
Via
Warning

6.2.7.2.2.2 Modification to Section 5.3.4.7.3.2 consists of adding the SIP header field ‘Proxy-Require’ as shown:

6.2.7.2.2.2.1 The AS-SIP signaling appliances serving SIP EIs, but not serving H.323 or proprietary IP EIs, 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)
Proxy-Require (used for CAL)
Rack
Reason
Replaces
Record-Route
Resource-Priority
RSeq
Session-Expires
Supported
Via

6.2.7.2.2.1.3 Modification to Section 5.3.4.7.3.3 consists of adding SIP header field ‘Proxy-Require’:

6.2.7.2.2.1.3.1 The AS-SIP signaling appliances serving H.323 and/or proprietary IP EIs, but not SIP EIs, 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 (used for CAL)
Rack
Reason
Record-Route
Refer-To
Replaces
Require
Resource-Priority
Retry-After
RSeq
Session-Expires
Subscription-State
Supported
To
Unsupported
Via
Warning

Section 6.2 – Unique Classified Unified Capabilities Requirements

6.2.7.2.3 CAL General Requirements

The CAL requirements apply to Classified only. For completeness, the following Classified requirements also appear in UCR 2008, Section 5.3.4 AS-SIP Requirements. The following paragraph numbers refer to UCR 2008, Section 5.3.4 AS-SIP Requirements.

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 EI. 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 EI 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 INVITE 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.

The following requirements apply to 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 EI, 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 EI/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 EI/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 EI/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 EI 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 EI 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 EI 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 EI/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 EI/user then the AS-SIP signaling appliance returns a 418 response.

5.3.4.7.9.11 SIP EIs **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 EI is NOT an authorized value for the EI/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 EI/user.
- If the mode is fixed, the AS-SIP signaling appliance returns a 418 response.

FOR OFFICIAL USE ONLY

Unified Capabilities Requirements

Section 6.2 – Unique Classified Unified Capabilities Requirements

5.3.4.7.9.11.2 If the initial INVITE received from the served SIP EI 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 EI 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 EI is NOT an authorized value for the EI/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 CAL 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 EIs 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 EI.

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 EIs, the initial INVITE sent by the SIP EI 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 EIs 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 EIs the SIP EI 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.

The following Apply to 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 EI that is the intended recipient of the message MUST process the CAL header in accordance with the procedures set forth in [5.3.4.7.9.17.1.1 - 5.3.4.7.9.17.1.6](#) below.

NOTE: When the INVITE with CAL header is intended for a SIP EI then the SIP EI will process the CAL instead of the AS-SIP signaling appliance to which the SIP EI is assigned. See the following procedure:

5.3.4.7.9.17.1 The AS-SIP signaling appliance receiving the request on behalf of the non-SIP IP EI [or the SIP EI] 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 EI then the AS-SIP signaling appliance [or SIP EI] 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 EI 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

Section 6.2 – Unique Classified Unified Capabilities Requirements

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 EI] 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 EI] 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 EI) 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 EI) 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 EI) deems the 2 resolved values to be incompatible, THEN the AS-SIP signaling appliance (or SIP EI) 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.

6.2.7.2.4 Option Tag ‘CAL’

[Required] The Option Tag “confidential-access-level” (CAL) used in ‘proxy-require header’ and ‘require header’ is REQUIRED in the classified environment because the classified uses the CAL option tag, while it is not used in the SBU environment.

Section 6.2 – Unique Classified Unified Capabilities Requirements

For completeness of the AS-SIP requirements, the set of classified requirements listed below also appear within UCR 2008, Section 5.3.4.7.3 ‘Header Fields’.

5.3.4.7.3.1.5.1 The AS SIP signaling appliances serving SIP EIs **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 EI or intended for a served SIP EI.

5.3.4.7.3.1.5.2 The AS SIP signaling appliances serving non-SIP IP EIs that generate either an INVITE or an UPDATE on behalf of a served non-SIP IP EI **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 The AS SIP signaling appliances serving non-SIP IP EIs **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 EI.

5.3.4.7.3.2.3 The AS SIP signaling appliances serving SIP EIs **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 EI or intended for a served SIP EI.

5.3.4.7.3.3.5.1 The AS SIP signaling appliances serving non-SIP IP EIs that generate either an INVITE or an UPDATE on behalf of a served non-SIP IP EI **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 The AS SIP signaling appliances serving non-SIP IP EIs **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 EI.

5.3.4.7.3.3.5.3 Tier0 SSs not serving IP EIs **MUST** support use of the option tag “confidential-access-level” for the Proxy-Require header of an INVITE or UPDATE message.

6.2.7.2.5 *418 Incompatible CAL Message*

The 418 Incompatible CAL message requirement described in UCR 2008, Section 5.3.4.7.4.1.11 is only applicable to the classified AS-SIP. The classified requirement is as follows:

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.

6.2.7.2.6 *Route Header*

The Route Header requirements described here in [Section 6.2.7.2.6](#) apply to the Classified environment only; for completeness of the AS-SIP requirements, the Classified requirements also appear in UCR2008, Section 5.3.4, AS-SIP Requirements. The Route Header requirements for AS SIP signaling appliances serving SIP EIs, H.323 EIs, and proprietary IP EIs are specified in requirements 5.3.4.7.3.1.6 and 5.3.4.7.3.1.7. The Route Header requirements for SS not directly serving IP EIs are specified in requirements 5.3.4.7.3.4.1 and 5.3.4.7.3.4.2. These requirements 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 E2E AS-SIP call. 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 EIs (SIP EI and/or H.323 EIs and/or proprietary IP EIs) 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 EIs 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-FY 2010]** 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.

Section 6.2 – Unique Classified Unified Capabilities Requirements

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:ebcenc1@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 FY 2010+]** 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 FY 2010+]** 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.

The following apply to Tier0 SSs Not Directly Serving IP End Instruments –

5.3.4.7.3.4.8 **[Required FY2008]** 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.

Section 6.2 – Unique Classified Unified Capabilities Requirements

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 **[Required FY2008]** 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 **[Required FY2008]** 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 **[Required FY2008]** 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.

6.2.7.2.7 *SIP Preconditions*

The Classified SIP preconditions requirements are specified in UCR 2008, Section 5.3.4.7.5b. The SBU SIP preconditions (defined in UCR 2008 Section 5.3.4.7.5) are conditional for the SBU environment.

The following requirements paragraphs which also appear in UCR 2008 section 5.3.4 AS-SIP requirement are **REQUIRED** for the Classified environment.

5.3.4.7.5b.1 Implementation of preconditions is mandatory for AS-SIP signaling appliances serving IP EIs 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 E2E status-type **MUST** be supported.

5.3.4.7.5b.4 The AS-SIP signaling appliances **MUST** employ the 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 EIs 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]

Section 6.2 – Unique Classified Unified Capabilities Requirements

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 AS precedence and preemption rules. 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: UCR 2008 Section, 5.3.4.10, Precedence and Preemption, includes details on the precedence and preemption requirements.

6.2.7.2.8 *SIP URI Mapping of Telephone Number*

UCR 2008, Section 5.3.4.7.6, describes the SIP URI and telephone number mapping requirements. The following modifications apply to the Classified version of AS-SIP:

- Instead of dsn.mil, use drsn.mil in the host name for classified SIP URIs
- Instead of dsn.mil, use drsn.mil with the phone-context parameter
- SBU Requirements 5.3.4.7.6.4, and 5.3.4.7.6.5 apply to inter-working of phone numbers on the PSTN is conditional in the classified spec.
- The 3-digit 911 and 411 numbers are conditional in the classified spec. There is no current requirement to support access to 911 services in the classified network.

6.2.7.2.9 *64kbps Transparent Calls (Clear Channel)*

There are no requirements for clear channel service within the Classified environment therefore the SBU AS-SIP requirement defined in UCR 2008, Section 5.3.4.7.7 do not apply.

6.2.7.2.10 *Transport of Route Code Information over AS-SIP*

There are no requirements for transport of route codes (used for hotline service) within the Classified environment, therefore the SBU AS-SIP requirement defined in UCR 2008, Section 5.3.4.7.8 do not apply.

6.2.7.2.11 *Precedence and Preemption*

UCR 2008, Section 5.3.4.10 specifies AS-SIP Precedence and Preemption requirements. The following differences in requirements exist between the SBU and Classified environments:

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 6.2.7-2](#)).

Table 6.2.7-2. 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 6.2.7-2](#).

5.3.4.10.2.1.2.7 **[FY 2008-2012]** AS-SIP signaling appliances **MUST** support the priority values ‘0’, ‘2’, ‘4’, ‘6’, ‘8’, ‘9’ for the network domain “DRSN.”

5.3.4.10.2.1.2.8 **[FY 2012+]** The single character text string representations of ‘1’, ‘3’, ‘5’, ‘7’ will be valid r-priority values for the network domain “DRSN.”

6.2.7.2.11.1 **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).

FOR OFFICIAL USE ONLY

Unified Capabilities Requirements

Section 6.2 – Unique Classified Unified Capabilities Requirements

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.

5.3.4.10.2.1.1.3.1 (Classified only) [FY 2008-FY 2012] AS SIP signaling appliances in the classified network are only required to recognize the “DRSN” network domain.

- The default namespace for the classified network is ‘DRSN’ not ‘DSN’
- The classified network has a sixth precedence level: ‘flash-override-override’ which is assigned the text value ‘9’ for use in the r-priority field

6.2.7.2.11.2 Classified VoIP Information Signals

Table 5.3.4.10-3 from UCR 2008, Section 5.3.4 AS-SIP requirements has been expanded for the classified environment to include secure dial tone, line busy tone, and reorder tone requirements as outlined in DRSN documentation. The expanded table, [Table 6.2.7-3](#).

Table 6.2.7-3. CVVoIP Information Signals

SIGNAL	FREQUENCIES (HZ)	SINGLE TONE LEVEL	COMPOSITE LEVEL	INTERRUPT RATE	STONE ON	STONE OFF
Secure Dial Tone	350 + 440 (Mixed)	-13 dBm0	-10 dBm0	Continuous		
Line Busy Tone	480 + 620 (Mixed)	-24 dBm0	-21 dBm0	60 IPM	0.5 sec	0.5 sec
Reorder Tone (No circuit)	480 + 620 (Mixed)	-24 dBm0	-21 dBm0	120 IPM	0.2 sec	0.3 sec
Audible Ringback (Routine Call)	440 + 480 (Mixed)	-16 dBm0	-13 dBm0	10 IPM	2.0 sec	4.0 sec
Audible Ringback Precedence Call	440 + 480 (Mixed)	-16 dBm0	-13 dBm0	30 IPM	1640 ms	360 ms
Alerting (Ring) Signal Routine	-	-	-	10 IPM	2.0 sec	4.0 sec
Alerting (Ring) Signal Precedence				30 IPM	1640 ms	360 ms
Preemption	440 + 620	-19	-16 dBm0	Continuous	Steady	

FOR OFFICIAL USE ONLY

Section 6.2 – Unique Classified Unified Capabilities Requirements

SIGNAL	FREQUENCIES (HZ)	SINGLE TONE LEVEL	COMPOSITE LEVEL	INTERRUPT RATE	TONE ON	TONE OFF
Tone	(Mixed)	dBm0			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	

6.2.7.2.12 Policing of Call Count Thresholds

UCR 2008, Section 5.3.4.11, Policing of Call Count Thresholds, defines the requirements for policing of call count thresholds. The following augmentations to the AS-SIP requirements apply for classified:

- Flash-override-override is added to requirements that describe policing for precedence levels beginning with ‘Flash’.
- The updated requirements are reflected in the following UCR 2008, AS-SIP requirements paragraphs: 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, 5.3.4.11.2.15.7
- The UCR 2008 the following paragraphs are updated to reflect the classified requirements.

Outbound INVITE & re-INVITE

5.3.4.11.1.9 When the Tier0 SS receives an outbound flash (r-priority = ‘6’) or flash-override (r-priority = ‘8’) or flash-override-override (r-priority = ‘9’) AS-SIP INVITE for a telephony call

Section 6.2 – Unique Classified Unified Capabilities Requirements

(that is either an initial INVITE¹ or a re-INVITE where the existing call is a video session²) from a served LSC that exceeds the telephony budget [new call request means $IPC > IPB$ if no directionalization or $IPCo > IPBo$ 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 higher precedence call request. (See 5.3.4.10.3.3.1.1.2 for details on the selection process for preempting lower precedence call requests and calls). The Tier0 SS MUST notify the NM system whenever Tier0 SS performs a network preemption in the context of its policing function to compel adherence to a telephony call count threshold. (See 5.3.4.11.1.16, 5.3.4.11.1.17)³

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 higher precedence call request. (See 5.3.4.10.3.3.1.1.2 for details on the selection process for preempting lower precedence call requests and calls). The Tier0 SS MUST notify the NM system whenever the Tier0 SS performs a network preemption in the context of its policing function to compel adherence to a telephony call count threshold. (See 5.3.4.11.1.16, 5.3.4.11.1.17)⁴

‘Policing of Inbound Telephony Call Requests’

‘Inbound INVITE with sdp’

5.3.4.11.1.13.2 If the INVITE (in 5.3.4.11.1.13) had a priority level of flash (r-priority = ‘6’) or flash-override (r-priority = ‘8’) or flash-override-override (r-priority = ‘9’) AND the Tier0 SS receives a 1xx > 100 or 2xx response from its served LSC then the Tier0 SS 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 flash or flash-override or flash-override-override call request. (See 5.3.4.10.3.3.1.1.2 for details on the selection process for preempting lower precedence call requests and calls). The Tier0 SS MUST notify the NM

1 An empty INVITE is also classified as a telephony call

2 The Tier0 SS 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

3 If the Tier0 SS is unable to preempt a call request or call on behalf of a flash or flash-override call request then the Tier0 SS MUST notify the NM system (see 5.3.4.11.1.16, 5.3.4.11.1.17)

4 If the Tier0 SS is unable to preempt a call request or call on behalf of a flash or flash-override call request then Tier0 SS MUST notify the NM system (see 5.3.4.11.1.16, 12.1.17)

system whenever the Tier0 SS performs a network preemption in the context of its policing function to compel adherence to a telephony call count threshold. (See 5.3.4.11.1.18)⁵

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 flash or flash-override or flash-override-override call request. (See 5.3.4.10.3.3.1.1.2 for details on the selection process for preempting lower precedence call requests and calls). The Tier0 SS MUST notify the NM system whenever the Tier0 SS performs a network preemption in the context of its policing function to compel adherence to a telephony call count threshold. (See 5.3.4.11.1.18)⁶

‘Inbound Empty INVITE’ (The text in the following paragraphs is similar to that in the SBU AS-SIP spec, but some have added requirements for the classified environment.)

5.3.4.11.1.14.3 If the empty INVITE (in 5.3.4.11.1.14) had a priority level of flash (r-priority = ‘6’) or flash-override (r-priority = ‘8’) or flash-override-override (r-priority = ‘9’) AND the Tier0 SS receives either a 1xx > 100 response having no sdp offer, a 1xx > 100 response with an sdp offering audio capabilities only, or a 200 response with an sdp offering audio capabilities only then the Tier0 SS 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 flash or flash-override or flash-override-override call request. (See 5.3.4.10.3.3.1.1.2 for details on the selection process for preempting lower precedence call requests and calls). The Tier0 SS MUST notify the NM system whenever the Tier0 SS performs a network preemption in the context of its policing function to compel adherence to a telephony call count threshold. (See 5.3.4.11.1.18)⁷

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 flash or flash-override or flash-override-override call request. (See 5.3.4.10.3.3.1.1.2 for details on the selection process for preempting lower precedence call requests and calls). The Tier0 SS MUST notify the NM system whenever the Tier0 SS performs a network preemption in the context of its policing function to compel adherence to a telephony call count threshold. (See 5.3.4.11.1.18)⁸

5 If the Tier0 SS is unable to preempt a call request or call on behalf of a flash or flash-override call request then the Tier0 SS MUST notify the NM system (see 5.3.4.11.1.16, 12.1.17)

6 If the Tier0 SS is unable to preempt a call request or call on behalf of a flash or flash-override call request then the Tier0 SS MUST notify the NM system (see 5.3.4.11.1.16, 12.1.17)

7 If the Tier0 SS is unable to preempt a call request or call on behalf of a flash or flash-override call request then the Tier0 SS MUST notify the NM system (see 5.3.4.11.1.16, 12.1.17)

8 If the Tier0 SS is unable to preempt a call request or call on behalf of a flash or flash-override call request then the Tier0 SS MUST notify the NM system (see 5.3.4.11.1.16, 12.1.17)

Section 6.2 – Unique Classified Unified Capabilities Requirements

5.3.4.11.1.14.4 If the empty INVITE (in 5.3.4.11.1.14) had a priority level of flash (r-priority = ‘6’) or flash-override (r-priority = ‘8’) or flash-override-override (r-priority = ‘9’) AND the Tier0 SS receives either a 1xx > 100 response with an sdp offering audio & video capabilities or a 200 response with an sdp offering both audio & video capabilities AND the VSUs required for the new video session exceeds the video budget [the new session request means $VDC > VDB$ if no directionalization or $VDC_i > VDB_i$ if directionalization] then the Tier0 SS 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 flash or flash-override or flash-override-override session request. (See 5.3.4.10.3.3.1.1.2 for details on the selection process for preempting lower precedence call requests and calls). The Tier0 SS MUST notify the NM system whenever the Tier0 SS performs a network preemption in the context of its policing function to compel adherence to a video session count threshold. (See 5.3.4.11.2.18)9

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 flash or flash-override or flash-override-override session request. (See 5.3.4.10.3.3.1.1.2 for details on the selection process for preempting lower precedence call requests and calls). The Tier0 SS MUST notify the NM system whenever the Tier0 SS performs a network preemption in the context of its policing function to compel adherence to a video session count threshold. (See 5.3.4.11.2.18)10

‘Inbound re-INVITE’ (The text in the following paragraphs is similar to that in the SBU AS-SIP spec, but some have added requirements for the classified environment.)

5.3.4.11.1.15.2 If the re-INVITE (in 5.3.4.11.1.15) had a priority level of flash (r-priority = ‘6’) or flash-override (r-priority = ‘8’) or flash-override-override (r-priority = ‘9’) AND the Tier0 SS receives the 18x or 200 response in 5.3.4.11.1.15 from its served LSC then the Tier0 SS 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 flash or flash-override or flash-override-override call request. (See 5.3.4.10.3.3.1.1.2 for details on the selection process for preempting lower precedence call requests and calls). The Tier0 SS MUST notify the NM

9 If the Tier0 SS is unable to preempt a call request or call on behalf of a flash or flash-override call request then the Tier0 SS MUST notify the NM system (see 5.3.4.11.2.16, 12.2.17)

10 If the Tier0 SS is unable to preempt a call request or call on behalf of a flash or flash-override call request then the Tier0 SS MUST notify the NM system (see 5.3.4.11.2.16, 12.2.17)

system whenever the Tier0 SS performs a network preemption in the context of its policing function to compel adherence to a telephony call count threshold. (See 5.3.4.11.1.18)¹¹

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 flash or flash-override or flash-override-override call request. (See 5.3.4.10.3.3.1.1.2 for details on the selection process for preempting lower precedence call requests and calls). The Tier0 SS MUST notify the NM system whenever the Tier0 SS performs a network preemption in the context of its policing function to compel adherence to a telephony call count threshold. (See 5.3.4.11.1.18)¹²

5.3.4.11.2 Policing of Video Sessions and Session Requests

‘Policing of Outbound Video Session Requests’ (The following text is similar to that in the SBU AS-SIP spec, but requirements have been added for the classified environment.)

5.3.4.11.2.10 When the Tier0 SS receives an outbound flash (r-priority = ‘6’) or flash-override (r-priority = ‘8’) or flash-override-override (r-priority=‘9’) INVITE from a served LSC offering audio & 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 budget¹³ the Tier0 SS MUST:

1. 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 flash or flash-override or flash-override-override session request. (See 5.3.4.10.3.3.1.1.2 for details on the selection process for preempting lower precedence session requests and sessions). The Tier0 SS MUST notify the NM system whenever the Tier0 SS performs a network preemption in the context of its policing function to compel adherence to a video count threshold. (See 5.3.4.11.2.18)¹⁴.

¹¹ If the Tier0 SS is unable to preempt a call request or call on behalf of a flash or flash-override call request then the Tier0 SS MUST notify the NM system (see 5.3.4.11.1.16, 12.1.17)

¹² If the Tier0 SS is unable to preempt a call request or call on behalf of a flash or flash-override call request then the Tier0 SS MUST notify the NM system (see 5.3.4.11.1.16, 5.3.4.11.1.17)

¹³ 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

¹⁴ If the Tier0 SS is unable to preempt a call request or call on behalf of a flash or flash-override call request then the Tier0 SS MUST notify the NM system (see 5.3.4.11.2.16, 5.3.4.11.2.17)

Section 6.2 – Unique Classified Unified Capabilities Requirements

2. 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 flash or flash-override or flash-override-override session request. (See 5.3.4.10.3.3.1.1.2 for details on the selection process for preempting lower precedence session requests and sessions). The Tier0 SS MUST notify the NM system whenever the Tier0 SS performs a network preemption in the context of its policing function to compel adherence to a video count threshold. (See 5.3.4.11.2.18) 15
3. 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 flash or flash-override or flash-override-override session request. (See 5.3.4.10.3.3.1.1.2 for details on the selection process for preempting lower precedence session requests and sessions). The Tier0 SS MUST notify the network management system whenever the Tier0 SS performs a network preemption in the context of its policing function to compel adherence to a video count threshold. (See 5.3.4.11.2.18) 16
4. 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 flash or flash-override or flash-override-override session request. (See 5.3.4.10.3.3.1.1.2 for details on the selection process for preempting lower precedence session requests and sessions). The Tier0 SS MUST notify the NM system whenever the Tier0 SS performs a network preemption in the context of its policing function to compel adherence to a video count threshold. (See 5.3.4.11.2.18) 17

Policing of Inbound Video Session Requests

Inbound INVITE

5.3.4.11.2.14.2 In the event the INVITE (in 5.3.4.11.2.14) had a priority level of flash (r-priority = ‘6’) or flash-override (r-priority = ‘8’) or flash-override-override (r-priority = ‘9’) AND the

15 If the Tier0 SS is unable to preempt a call request or call on behalf of a flash or flash-override call request then the Tier0 SS MUST notify the NM system (see 5.3.4.11.2.16, 12.2.17)

16 If the Tier0 SS is unable to preempt a call request or call on behalf of a flash or flash-override call request then the Tier0 SS MUST notify the NM system (see 5.3.4.11.2.16, 12.2.17)

17 If the Tier0 SS is unable to preempt a call request or call on behalf of a flash or flash-override call request then the Tier0 SS MUST notify the NM system (see 5.3.4.11.2.16, 12.2.17)

Tier0 SS receives a 1xx > 100 response or 2xx response with an sdp answer that accepts audio & video capabilities from its served LSC or a 1xx>100 response with no sdp answer then the Tier0 SS MUST:

1. 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 flash or flash-override or flash-override-override session request. (See 5.3.4.10.3.3.1.1.2 for details on the selection process for preempting lower precedence session requests and sessions). The Tier0 SS MUST notify the NM system whenever the Tier0 SS performs a network preemption in the context of its policing function to compel adherence to a video count threshold. (See 5.3.4.11.2.18)¹⁸
2. 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 flash or flash-override or flash-override-override session request. (See 5.3.4.10.3.3.1.1.2 for details on the selection process for preempting lower precedence session requests and sessions). The Tier0 SS MUST notify the NM system whenever the Tier0 SS performs a network preemption in the context of its policing function to compel adherence to a video count threshold. (See 5.3.4.11.2.18)

5.3.4.11.2.14.7 If the INVITE (in 5.3.4.11.2.14) had a priority level of flash (r-priority = ‘6’) or flash-override (r-priority = ‘8’) or flash-override-override (r-priority = ‘9’) AND the Tier0 SS receives a 1xx >100 response or 2xx response with an sdp answer that accepts audio capabilities only from its served LSC then the Tier0 SS MUST verify whether the call request would cause IPC to exceed IPB [or in the case of directionalization if IPC_i would exceed IPB_i]. If the call request would cause the call count to exceed the telephony call count threshold then the Tier0 SS MUST:

1. 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 flash or flash-override or flash-override-override call request. (See 5.3.4.10.3.3.1.1.2 for details on the selection process for preempting lower precedence call requests and calls). The Tier0 SS MUST notify the NM system whenever the Tier0 SS performs a network preemption in the

¹⁸ If the Tier0 SS is unable to preempt a call request or call on behalf of a flash or flash-override call request then Tier0 SS MUST notify the NM system (see 5.3.4.11.2.16, 12.2.17)

Section 6.2 – Unique Classified Unified Capabilities Requirements

context of its policing function to compel adherence to a telephony call count threshold.
(See 5.3.4.11.1.18)19

2. 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 flash or flash-override or flash-override-override call request. (See 5.3.4.10.3.3.1.1.2 for details on the selection process for preempting lower precedence call requests and calls). The Tier0 SS MUST notify the NM system whenever the Tier0 SS performs a network preemption in the context of its policing function to compel adherence to a telephony call count threshold.
(See 5.3.4.11.1.18)20

NOTE: The policing of inbound empty INVITEs is covered in requirement 5.3.4.11.1.14.

Inbound re-INVITE

5.3.4.11.2.15.2 In the event the re-INVITE (in 5.3.4.11.2.15) had a priority level of flash (r-priority = ‘6’) or flash-override (r-priority = ‘8’) or flash-override-override (r-priority = ‘9’) AND the Tier0 SS receives a 1xx or 200 response with a sdp answer accepting the video offer or a 1xx>100 response with no sdp answer from its served LSC then the Tier0 SS 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 flash or flash-override or flash-override-override session request. (See 5.3.4.10.3.3.1.1.2 for details on the selection process for preempting lower precedence session requests and sessions). The Tier0 SS MUST notify the NM system whenever the Tier0 SS performs a network preemption in the context of its policing function to compel adherence to a video count threshold. (See 5.3.4.11.2.18)21

1. 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 flash or flash-override or flash-override-override session request. (See 5.3.4.10.3.3.1.1.2 for details on the selection process for preempting lower precedence session requests and sessions). The Tier0 SS MUST notify the NM system

19 If the Tier0 SS is unable to preempt a call request or call on behalf of a flash or flash-override call request then the Tier0 SS MUST notify the NM system (see 5.3.4.11.1.16, 12.1.17)

20 If the Tier0 SS is unable to preempt a call request or call on behalf of a flash or flash-override call request then the Tier0 SS MUST notify the NM system (see 5.3.4.11.1.16, 12.1.17)

21 If the Tier0 SS is unable to preempt a call request or call on behalf of a flash or flash-override call request then Tier0 SS MUST notify the NM system (see 5.3.4.11.2.16, 12.2.17)

whenever the Tier0 SS performs a network preemption in the context of its policing function to compel adherence to a video count threshold. (See 5.3.4.11.2.18) 22

2. 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 flash or flash-override or flash-override-override session request. (See 5.3.4.10.3.3.1.1.2 for details on the selection process for preempting lower precedence session requests and sessions). The Tier0 SS **MUST** notify the NM system whenever the Tier0 SS performs a network preemption in the context of its policing function to compel adherence to a video count threshold. (See 5.3.4.11.2.18) 23
3. 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 flash or flash-override or flash-override-override session request. (See 5.3.4.10.3.3.1.1.2 for details on the selection process for preempting lower precedence session requests and sessions). The Tier0 SS **MUST NOTIFY** the NM system whenever the Tier0 SS performs a network preemption in the context of its policing function to compel adherence to a video count threshold. (See 5.3.4.11.2.18) 24

5.3.4.11.2.15.7 In the event the re-INVITE (in 5.3.4.11.2.15) had a priority level of flash (r-priority = ‘6’) or flash-override (r-priority = ‘8’) or flash-override-override (r-priority = ‘9’) AND the Tier0 SS receives a 1xx >100 response or 2xx response with an sdp answer that accepts audio capabilities only from its served LSC then the Tier0 SS **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 Tier0 SS **MUST**:

1. 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 flash or flash-override or flash-override-override call request. (See 5.3.4.10.3.3.1.1.2 for details on the selection process for preempting lower precedence call requests and calls). The Tier0 SS **MUST** notify the NM system whenever the Tier0 SS performs a network preemption in the

22 If the Tier0 SS is unable to preempt a call request or call on behalf of a flash or flash-override call request then Tier0 SS **MUST** notify the NM system (see 5.3.4.11.2.16, 12.2.17)

23 If the Tier0 SS is unable to preempt a call request or call on behalf of a flash or flash-override call request then Tier0 SS **MUST** notify the NM system (see 5.3.4.11.2.16, 12.2.17)

24 If the Tier0 SS is unable to preempt a call request or call on behalf of a flash or flash-override call request then Tier0 SS **MUST** notify the NM system (see 5.3.4.11.2.16, 12.2.17)

Section 6.2 – Unique Classified Unified Capabilities Requirements

context of its policing function to compel adherence to a telephony call count threshold. (See 5.3.4.11.1.18)²⁵

2. 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 flash or flash-override or flash-override-override call request. (See 5.3.4.10.3.3.1.1.2 for details on the selection process for preempting lower precedence call requests and calls). The Tier0 SS MUST NOTIFY the NM system whenever the Tier0 SS performs a network preemption in the context of its policing function to compel adherence to a telephony call count threshold. (See 5.3.4.11.1.18)²⁶

6.2.8 Physical Construction Unique Requirements

Physical construction requirements for classified elements within a secure enclave must adhere to current requirements for:

1. Cabling: All cabling must follow Protected Distribution System (PDS) guidelines.
2. Cabling or interfaces leaving a secure enclave must be encrypted.
3. Equipment must comply with TEMPEST requirements.

²⁵ If the Tier0 SS is unable to preempt a call request or call on behalf of a flash or flash-override call request then the Tier0 SS MUST notify the NM system (see 5.3.4.11.1.16, 12.1.17)

²⁶ If the Tier0 SS is unable to preempt a call request or call on behalf of a flash or flash-override call request then the Tier0 SS MUST notify the NM system (see 5.3.4.11.1.16, 12.1.17)

TABLE OF CONTENTS

<u>SECTION</u>	<u>PAGE</u>
SECTION 7 REQUIREMENTS SUMMARY	1511
7.1 Requirements synopsis.....	1511
7.1.1 Overview of Approved Products	1511
7.1.2 SBU UC Products for E2E Systems That Support SBU Voice and Video Services.....	1512
7.1.3 Circuit-Switched Products with IP on the Line Side Only that Support SBU Voice and Video Services.....	1513
7.1.4 Classified UC Products for E2E Systems that Support SBU Voice and Video Services	1514
7.1.5 DISN Network Infrastructure Products	1514
7.1.6 Tactical UC Products.....	1515
7.1.7 Encryption Products.....	1516

SECTION 7 REQUIREMENTS SUMMARY

7.1 REQUIREMENTS SYNOPSIS

Section 7, Requirements Summary, provides a summary of where requirements for the various UC products are described in UCR 2008.

7.1.1 Overview of Approved Products

The UCR covers six categories of approved products as follows:

1. The SBU UC products for IP E2E systems that support SBU voice and video services.
2. Circuit-switched products with IP on the Line Side only that support SBU voice and video services.
3. Classified UC products for IP E2E systems that support Classified voice and video services.
4. Network infrastructure products (e.g., DISN SDN/MILDEP Intranet and terrestrial transport components products). The ASLAN products, which are Access, Distribution, and Core devices, are a subset of the network infrastructure products.
5. Tactical products.
6. Encryption products.

Instant Messaging (IM) and Chat Collaboration UCs are not considered to be stand-alone UC products; these are applications that create the possibility of real-time text-based communication between two or more participants over the network infrastructure. General requirements for IM and Chat Collaboration applications are described in UCR 2008, Section 5.7, Presence/Awareness, Instant Messaging, and Chat Requirements. These UC features are included in the SBU UC Products for IP E2E systems that support SBU voice and video services; Classified UC Products for IP E2E systems that support SBU voice and video services; and in Tactical Products.

[Figure 7-1](#), Overview of UC Product Categories within the DoD UC APL, provides an overview of the structure of the DoD UC APL in terms of services and network infrastructure. The various UC products for each of the six UC product categories are found under their appropriate section

of the UC APL. Many UC products, however, show up under multiple UC product categories since they can be used under multiple categories. Examples include the LSCs, CE routers, EBCs, and ASLANs, which can be used for both SBU and Classified voice and video services.

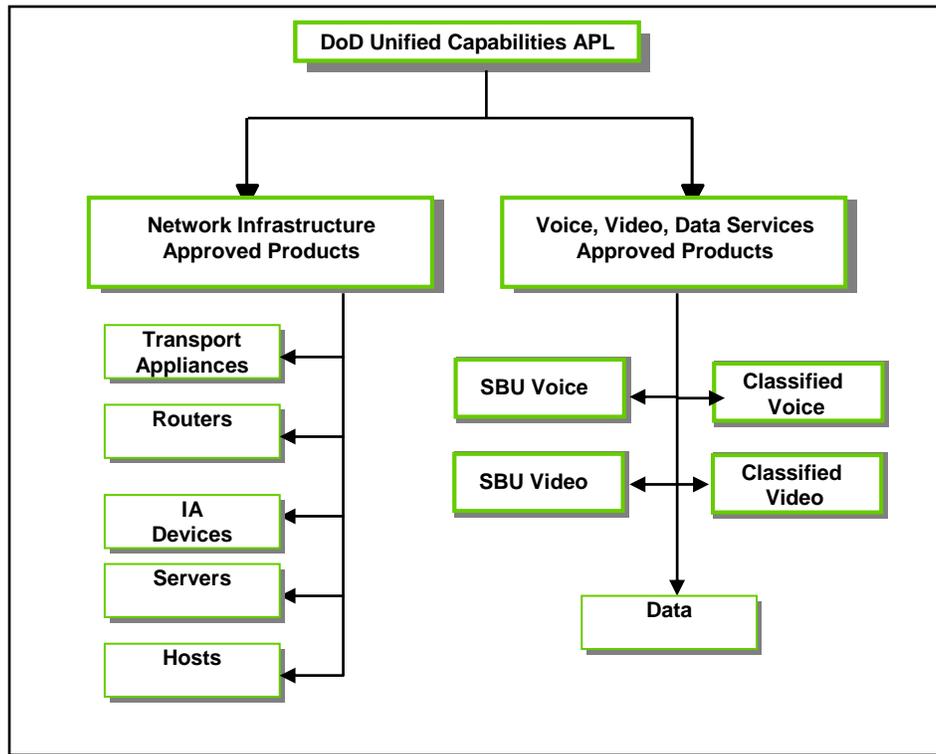


Figure 7-1. Overview of UC Product Categories within the DoD UC APL

7.1.2 SBU UC Products for E2E Systems That Support SBU Voice and Video Services

[Table 7-1](#), IP-Based UC products that Support SBU Voice and Video Services, delineates the UCR 2008 sections where requirements for these products are found.

Table 7-1. IP-Based UC Products that Support SBU Voice and Video Services

PRODUCT AND APPLIANCE FUNCTION		GENERAL REQUIREMENTS	IA REQUIREMENTS	IPV6	SIGNALING TYPE	
PRODUCT	APPLIANCE				AS-SIP	TDM
MFSS	TDM Side	5.2	5.4	5.3.5		5.2
	SS Side	5.3.2	5.4	5.3.5	5.3.4	5.3.4
LSC	CCA	5.3.2.9	5.4	5.3.5	5.3.4	
	Media Gateway	5.3.2.12	5.4	5.3.5	5.3.4	5.2
	Signaling Gateway	5.3.2.13			5.3.4	5.2
LAN Access Switch	NA	5.3.1	5.4	5.3.5	5.3.4	NA
LAN Distribution Switch	NA	5.3.1	5.4	5.3.5	5.3.4	NA
LAN Core Switch	NA	5.3.1	5.4	5.3.5	5.3.4	NA
EBC	NA	5.3.2.15	5.4	5.3.5	5.3.4	NA
CE Router	NA	5.3.2.14	5.4	5.3.5	5.3.4	NA

7.1.3 Circuit-Switched Products with IP on the Line Side Only that Support SBU Voice and Video Services

[Table 7-2](#), Circuit-Switched Products with IP on the Line Side Only that Support SBU Voice and Video Services, delineates the UCR 2008 sections where requirements for these products are found. The requirements for each of the circuit-switched products are distributed throughout Section 5.2, Circuit-Switched Capabilities and Features.

Table 7-2. Circuit-Switched Products with IP on the Line Side only that Support SBU Voice and Video Services

PRODUCT	REQUIREMENTS SECTION	ROLE AND FUNCTIONS
Multifunction Switch (MFS)	5.2	System providing local telephone service and tandem switching with full set of Assured Service features, including network traffic management controls
End Office	5.2	System providing local telephone service and full set of Assured Service features, including network traffic management controls
Small End Office	5.2	Smaller version of the EO System providing local telephone service and full set of Assured Service features
Private Branch Exchange (PBX) Type 1	5.2	System providing local telephone service and MLPP capabilities

PRODUCT	REQUIREMENTS SECTION	ROLE AND FUNCTIONS
Private Branch Exchange (PBX) Type 2	5.2	System providing local telephone service without MLPP capabilities
Remote Switching Unit (RSU)	5.2	Small System providing local telephone service as an extension to an EO/SMEO or PBX

7.1.4 Classified UC Products for E2E Systems that Support SBU Voice and Video Services

[Table 7-3](#), Classified UC Products for IP E2E that Support Classified Voice and Video Services, delineates the UCR 2008 sections where requirements for these products are found. Classified product requirements consist of general requirements found throughout Section 5.3.2, Assured Services Requirements, plus unique Classified requirements found throughout Section 6.2, Unique Classified Unified Capabilities Requirements. The combination of requirements found across Sections 5.3.2 and 6.2 provides the total requirements that apply to the classified products.

Table 7-3. Classified UC Products for IP E2E that Support Classified Voice and Video Services

PRODUCT	UNIQUE REQUIREMENTS	GENERAL REQUIREMENTS	IA REQUIREMENTS	IPV6	AS-SIP
Tier0 SS	6.2	5.3.2	5.4	5.3.5	5.3.4 and 6.2
LSC	6.2	5.3.2	5.4	5.3.5	5.3.4 and 6.2
LAN Access Switch	NA	5.3.1	5.4	5.3.5	5.3.4
LAN Distribution Switch	NA	5.3.1	5.4	5.3.5	5.3.4
LAN Core Switch	NA	5.3.1	5.4	5.3.5	5.3.4
EBC	NA	5.3.2	5.4	5.3.5	5.3.4
CE Router	NA	5.3.2	5.4	5.3.5	5.3.4

7.1.5 DISN Network Infrastructure Products

[Table 7-4](#), DISN Network Infrastructure UC Product Categories, delineates the network infrastructure UC products, which can be used by all MILDEPs for their Intranets. These UC products do not currently include data firewalls but will in future updates.

Table 7-4. DISN Network Infrastructure UC Product Categories

ITEM	REQUIREMENTS SECTION	ROLE AND FUNCTIONS
M13	5.5	System providing access to the DISN WAN from the Edge by multiplexing lower bandwidth connections to higher speed circuits
MSPP	5.5	System providing access to the DISN WAN from the Edge by multiplexing lower bandwidth connections to higher speed circuits
Aggregation Router	5.5	System serving as a port expander for a PE Router
Provider Edge Router	5.5	System providing robust, high-capacity IP routing at the entry points to the DISN WAN
Provider Router	5.5	System providing robust, high-capacity IP routing in the DISN WAN
Optical Switch	5.5	Switching system providing high-speed optical transport in the DISN WAN
LEGEND DISN Defense Information Systems Network IP Internet Protocol MSPP Multi-Service Provisioning Platforms		PE Provider Edge WAN Wide Area Network

7.1.6 Tactical UC Products

[Table 7-5](#), Tactical UC Product Categories and Paragraph Reference, delineates the tactical UC products. Tactical switching system requirements consist of general requirements found throughout Section 5.2, Circuit-Switched Capabilities and Features, plus unique tactical requirements found throughout Section 6.1.3, Deployable Voice Exchanges. The combination of requirements found throughout Section 5. 2 and Section 6.1, Unique Capabilities and Requirements, provides the total requirements that apply to the tactical products.

Table 7-5. Tactical UC Product Categories and Paragraph Reference

PRODUCT	GENERAL REQUIREMENTS SECTION	UNIQUE REQUIREMENTS SECTION	ROLE AND FUNCTIONS
DVX-C	5.2	6.1.3	Tactical voice switch with ASF capabilities to support assured service requirements. This switch is used for rapid deployment situations and contingencies in the tactical environment.
DVX Legacy (DVX-L)	5.2	6.1.3	Tactical voice switch with ASF capabilities to support assured service requirements. This switch is part of the TRI-TAC systems and thus termed Legacy.

FOR OFFICIAL USE ONLY

Unified Capabilities Requirements 2008

Section 7 –Requirements Summary

PRODUCT	GENERAL REQUIREMENTS SECTION	UNIQUE REQUIREMENTS SECTION	ROLE AND FUNCTIONS
Deployable DSN PBX1	5.2	6.1.3	A DSN PBX1 used in the tactical arena. When used in the tactical arena, the PBX1 is connected to a DSN EO through a STEP/Teleport.
Tactical Network Elements	NA	6.1.4	Network elements deployed in a tactical arena.
Tactical LANs	5.3.1	6.1.5	LAN deployed in a tactical arena.
DCVX	NA	6.1.6	Tactical cellular system with ASF capabilities to support assured service requirements. This system is used for rapid deployment situations and contingencies in the tactical environment.
LEGEND ASF Assured Services Features COTS Commercial Off-the-Shelf DCVX Deployed Cellular Voice Exchange DSNY Defense Switched Network DVX Deployable Voice Exchange DVX-C Deployable Voice Exchange–COTS		DVX-L Deployable Voice Exchange–Legacy EO End Office LAN Local Area Network PBX1 Private Branch Exchange 1 STEP Standardized Tactical Entry Point TRI-TAC Tri-Service Tactical Communications	

7.1.7 Encryption Products

[Table 7-6](#), Encryption Products and Paragraph Reference, summarizes the encryption products used in the IP environment. The requirements for encryption products are found in UCR 2008 Section 5.6, Generic Encryption Device Requirements.

Table 7-6. Encryption Products and Paragraph Reference

ITEM	REQUIREMENTS SECTION	ROLE AND FUNCTIONS
HAIPE	5.6	HAIPE is a programmable IP INFOSEC device with traffic protection, networking, and management features that provide IA services for IPv4 and IPv6 networks.
Link Encryptors	5.6	Link encryptors provide data security in a multitude of network elements by encrypting point-to-point, netted, broadcast, or high-speed trunks.
LEGEND HAIPE High Assurance Internet Protocol Encryptor IA Information Assurance INFOSEC Information Security		IPv4 Internet Protocol Version 4 IPv6 Internet Protocol Version 6

SECTION A1 INTRODUCTION

A1.1 SCOPE

Appendix A1 contains definitions for the various UC systems, subsystems, and components, along with acronyms and abbreviations used within the entire Unified Capabilities Requirements 2008 (UCR 2008).

A1.2 APPENDIX A1 OVERVIEW

This appendix consists of four sections as follows:

- Section A1 describes the scope of this appendix.
- Section A2 contains a glossary describing the terminology used within the UCR 2008.
- Section A3 lists the abbreviations and acronyms used within the UCR 2008.
- Section A4 contains the references used within the UCR 2008.

THIS PAGE INTENTIONALLY LEFT BLANK



SECTION A2 GLOSSARY AND TERMINOLOGY DESCRIPTION

A2.1 OVERVIEW

This glossary defines terms as they apply to the UCR 2008. It is understood that other documents or organizations may define the terms differently. These terminology definitions are not requirements and are defined to provide context for a requirement in the UCR 2008.

[A](#) [B](#) [C](#) [D](#) [E](#) [F](#) [G](#) [H](#) [I](#) [J](#) [K](#) [L](#) [M](#) [N](#) [O](#) [P](#) [Q](#) [R](#) [S](#) [T](#) [U](#) [V](#) [W](#)

A

Add-On Transfer and Conference Calling A feature set that provides the user with the capabilities to handle more than one call at a time on a given line.

Admission Control The process by which flows are allowed to enter a network based on their level of quality of service.

Aggregate Service Class An aggregation of service classes based on a selected set of quality of service criteria.

Appliance A hardware platform with its supporting software that performs a single function or multiple functions.

Application Layer Control Protocol See Call Control.

Approved Products List (APL) A list of products that have received Joint Interoperability Certification (JIC) and Information Assurance Accreditation (IAA) from the Defense Information System Network (DISN) Designated Approval Authorities (DAAs) in accordance with the Department of Defense Instruction (DoDI) 8100.3. The list is published on the Joint Interoperability Test Command (JITC) home page (<http://jitc.fhu.disa.mil/tssi/apl.html>).

Approved Product List System Under Test (SUT) The set of appliances required to meet a Defense Switched Network (DSN) switch certification (i.e., multifunction switch (MFS), end office, etc.). Examples of a SUT include Time Division Multiplexing (TDM) or circuit switch components, Voice over Internet Protocol (VoIP) system components (e.g., Local Session Controller (LSC) and gateway), local area network (LAN) components (e.g., routers and Ethernet switches), and end instruments.

FOR OFFICIAL USE ONLY

Appendix A1 – Definitions, Abbreviations and Acronyms, and References

Section A2 – Glossary and Terminology Description

Assured Forwarding (AF) Provides delivery of IP packets in four independently forwarded AF classes. Within each AF class, an IP packet can be assigned one of three different levels of drop precedence. In case of congestion, the drop precedence of a packet determines the relative importance of the packet within the AF class. A congested Differentiated Services (DS) node tries to protect packets with a lower drop precedence value from being lost by preferably discarding packets with a higher drop precedence value. A DS node must allocate forwarding resources (i.e., buffer space and bandwidth) to AF classes so that, under reasonable operating conditions and traffic loads, packets of an AF class x do not have a higher probability of timely forwarding than packets of an AF class y if $x < y$. [RFC 2597]

Assured Real Time Services (ARTS) Softswitch (SS) The ARTS SS within the DoD environment is defined in accordance with the International Softswitch Consortium definition and is a programmable network appliance that provides the following capabilities:

- Controls connection services for a media gateway and/or native IP endpoints.
- Selects processes and services that can be applied to a call.
- Provides routing for call control within the network based on signaling and customer database information.
- Transfers control of the call to another network element.
- Interfaces to and supports management functions such as provisioning, fault, and billing.
- Ability to control the access of sessions within and external to its domain.

In the fiscal year (FY) 2008 architecture, the ARTS SS is not a stand-alone appliance and its functionality is included within the functions of a multifunction softswitch (MFSS). The FY12 architecture may support a stand-alone ARTS SS. To support these capabilities, the ARTS SS includes a Local Session Controller (LSC), media gateway controller (MGC), and signaling gateway. In addition to the International Softswitch Consortium definition, the ARTS SS is also capable of policing subtended LSCs, ARTS SSs, and MFSSs, and performing preemption in the Defense Information Systems Network (DISN) wide area network (WAN) between itself and other MFSSs or softswitches using the WAN Level Assured Services Admission Control (W-ASAC).

Assured Service The ability of a system to optimize session completion rates for all command and control (C2) users despite degradation because of network disruptions, natural disasters, or surges during crisis or war.

Assured Services Admission Control (ASAC) A process by which the quality of service requirements of a higher precedence service will be met at the expense of a lower precedence service if the network conditions do not allow meeting quality of service requirements of all services.

Assured Services Local Area Network (ASLAN) The Internet Protocol (IP) network infrastructure components used to provide command and control (C2) voice services to end users. It applies to switch certifications for multifunction switches (MFSs), end office switches (EOSs), small end office (SMEO) switches, and private branch exchange 1 (PBX1), and to certifications for Local Session Controllers (LSCs), multifunction softswitches (MFSSs), and softswitches. A local area network (LAN) that supports C2 users is considered an ASLAN. The ASLAN has two configurations depending on whether it supports C2 users or special C2 users. An ASLAN that supports C2 users is classified a Medium Availability ASLAN and the primary requirements that differentiate it from a non-ASLAN are that it requires a two (2) hour power backup capability for all ASLAN components in addition to providing 0.99997 reliability. An ASLAN that supports special C2 users is classified a High Availability ASLAN and the primary requirements that differentiate it from a Medium Availability ASLAN are that it requires an eight (8) hour power backup capability for all ASLAN components in addition to providing 0.99999 reliability.

Assured Service Session Initiation Protocol (AS-SIP) A session signaling protocol consisting of a defined set of Session Initiation Protocol (SIP) signaling standards and incorporating DoD Assured Service functionality.

Assured Service Session Initiation Protocol (AS-SIP) Signaling Appliance Any DoD signaling appliance (exclusive of end instruments) that supports the receipt, processing, or forwarding of AS-SIP messages. These appliances MAY support the receipt and forwarding of encapsulated Integrated Services Digital Network User Part (ISUP) Multipurpose Internet Mail Extension (MIME) objects.

Audio Add-On A feature that allows a participant to join a videoconference via audio (telephone) only.

Automated Receiving Devices (ARD) A family of automated devices, which are customer premises equipment (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 ARDs that are complex can be full function Automatic Call Distributors (ACDs) that also include predetermined schemes 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 the caller had not terminated the call, ARD can terminate the call, or send the call to another

Section A2 – Glossary and Terminology Description

location. Usually the ARD invokes a network carrier based “take back and transfer” to the alternative location. Automated Receiving Devices do not originate calls to the network.

Availability The fraction of the time the system is available to a service user’s requests. The time during which the system is unavailable is called downtime; the time during which the system is available is called uptime. In IP terms, it is the percentage of time that the packet loss is less than the threshold. (NCID v3 QoS (T300])

B

Back-to-Back User Agent (B2BUA) “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]

Blocking The process by which a message is denied entry to a network due to lack of resources in the network.

C

Call A message that is subject to Call Admission Control (CAC) or Session Admission Control (SAC).

Call Admission Control (CAC) 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 requirements for the call.

Call Connection Agent (CCA) The CCA is part of the Session Control and Signaling functions and includes both the Interworking function (IWF) and the media gateway controller (MGC). As a result, the scope of the CCA includes the following areas:

- Control of Assured Services Session Initiation Protocol (AS-SIP) sessions within the network appliance
- Support for public switched telephone network (PSTN) and Voice over IP (VoIP) signaling protocols

- Protocol interworking of signaling protocols (for example, AS-SIP ↔ DoD Common Channel Signaling System No. 7 (CCS7) interworking), through the CCA IWF Control of media gateways (MGs) that link the network appliance with Time Division Multiplexing (TDM) network elements
- Support for interactions with other network appliance functions
- Support for assured real time services (ARTS) voice calls and ARTS video calls
- Support for ARTS user features and services (USFs)

Call Control Establishes, modifies, and terminates sessions (e.g., multimedia conferences). It can invite participants to existing sessions, such as multicast conferences. [Referred to as Application Layer Control Protocol in RFC 3261.]

Call Forwarding Variable This feature allows ROUTINE precedence calls attempting to terminate to a line to be redirected to another customer-specified line served by the same office or by another office for Defense Switched Network (DSN) and/or commercial.

Call Hold A feature that 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.

Call Stateful A proxy is call stateful if it retains state for a dialog from the initiating INVITE to the terminating BYE request. A call stateful proxy is always transaction stateful, but the converse is not necessarily true. [RFC 3261]

Call Waiting 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.

Communities of Interest (COI) 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:

1. For an outgoing call request, the dialed destination matches a code in the user's COI screening list.
2. For local calls only, an incoming call request is to a user who is assigned to the same COI group as the calling user.

FOR OFFICIAL USE ONLY

Appendix A1 – Definitions, Abbreviations and Acronyms, and References

Section A2 – Glossary and Terminology Description

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 deemed external but these do not undergo any COI screening; and hence, are not subject to the special COI restrictions and privileges.

Cancel Call Waiting A feature that allows the customer with Call Waiting service to inhibit the operation of call waiting for one call.

Certificate Path A sequence of certificates that connect the target certificate to one of the relying party's trust points. Construction of the path is known as path development and verification of that path provides a chain of trust and is known as path processing. A target certificate belongs to an end-entity that either sent a signed message to the relying party or to which the relying party desires to send an encrypted message. This is also called a certificate chain.

Certificate Trust List (CTL) A predefined list of items that have been signed by a trusted entity. All items in the list are authenticated and approved for use by the signing entity.

Chat The capability for two or more users operating on different computers to exchange text messages in real time. Chat is distinguished from instant messaging (IM) by being focused on group chat, or room-based chat. Room persistence is typically a key feature of multiuser chat; in contrast with typically ad hoc IM capabilities.

Circuit Emulation Service (CES) over Internet Protocol (IP) Circuit Emulation Service over IP is trunking of time division multiplexing (TDM) data between IP points. Circuit Emulation Service over IP provides a method to transport T1/E1 or T3/E3 streams over an IP network. The service is similar to CES over asynchronous transfer mode (ATM) that has been in the industry for some time but the transport layer is IP. The circuit may include compression, which may include silence suppression, and echo cancellation. The CES over IP also known as Circuit Emulation Service over Packet (CESoP).

Classifier An entity that selects packets based on the content of packet headers according to defined rules. [RFC 2475]

codec Acronym for Coder/Decoder. In video conferencing, an electronic device that converts analog signals, typically video and/or voice, into digital form and compresses them into a fraction of their original size to save frequency bandwidth on a transmission path. The device also multiplexes digital data, such as graphic images into the transmitted signal. It also performs the inverse operation; decompressing received signals, demultiplexing them, and converting previously digitized analog signals nearly back to their original state.

Command and Control (C2) User Users who have a requirement for “C2 communications but do not meet the criteria for class of Special C2 user.” C2 users include any person (regardless of the position in the chain-of-command) who issues or receives guidance or orders that direct, control, or coordinate any military forces regardless of the nature of the military mission (including combat support, administration, and logistics), whether said guidance or order is issued or effected during peacetime or wartime. Four types of C2 users are as follows:

“Users approved by the Joint Staff or DOD component for PRIORITY and ROUTINE precedence origination.”

DoD users having a military mission that might receive “C2 calls for orders and direction at precedence above ROUTINE, even though they do not have a C2 mission for issuing guidance or orders.” Therefore, these users must be served by switching facilities that provide the MUFs of the DSN.

“Any Joint Staff/CC/S/A user that is authorized to originate ONLY Routine calls does not need to meet the availability or redundancy requirements of the Special C2 users or C2 users capable of originating I/P precedence.”

Any non-DoD U.S. Government organization supporting Homeland Security that requires the Military Unique Services of the DSN and are validated by the Joint Staff.

“The exercise of authority and direction by a properly designated commander over assigned and attached forces in accomplishment of the mission. C2 functions are performed through an arrangement of personnel, equipment, communications, facilities, and procedures employed by a commander in planning, directing, coordinating, and controlling forces and operations in the accomplishment of the mission.” [CJCSI 6215.01C]

Common Channel Signaling System No. 7 (i.e., SS7 or C7) A global standard for telecommunications defined by the International Telecommunications Union (ITU) Telecommunication Standardization Sector (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 American National Standards Institute (ANSI) and Telcordia Technologies (Bell Communications Research) standards used in North America, and the European Telecommunications Standards Institute (ETSI) standard used in Europe.

FOR OFFICIAL USE ONLY

Appendix A1 – Definitions, Abbreviations and Acronyms, and References

Section A2 – Glossary and Terminology Description

Community of Interest (COI) Group A feature that 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.

Community of Interest (COI) Group Classmarks Specify the outgoing and incoming call restrictions and/or privileges for calls internal to the COI group. The COI group classmarks are defined as follows:

1. 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 that are specified within the COI screening list. The user is allowed to exercise the normal authorized precedence for these calls.
2. Outgoing Precedence Allowed. The COI user is allowed to exercise up to and including the COI precedence for calls internal to the COI.
3. Outgoing Precedence Mandatory. Only COI precedence calls are permitted for calls internal to the COI.
4. 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.

Community of Interest (COI) Incoming Classmarks A COI group user with no incoming classmarks limits the COI user to receiving locals 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 because these do not undergo COI screening.

1. Incoming Precedence Mandatory. This COI service only permits calls internal to the COI that are at the COI precedence level, which only applies for local calls that 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).
2. 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 restricted also.
3. COI Member Classmarks. In addition to the COI group classmarks that are part of the COI group, specific COI members can have COI classmarks at the subscriber level that specify the type of incoming and outgoing call restrictions and/or privileges for calls external to the COI.

Community of Interest (COI) Member A user that has a COI group assigned is defined as being a member of that COI group.

Community of Interest (COI) 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.

Community of Interest (COI) Precedence Level A COI feature that allows precedence level to be either required or allowed, depending upon the COI group classmarks, for calls to/from users of a COI group.

Community of Interest (COI) Screening List A COI feature that allows a list to be specified for 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 or deny the call request.

Conditional Requirement [Conditional] A requirement that addresses features and capabilities that are not considered critical for DoD mission support based on DoD policies. However, it is recognized that such features and capabilities do have utility for some users or for specific operations. To ensure interoperability and consistency of these features and capabilities across all platforms, these features and capabilities are specified with set parameters. If these features and capabilities are provided, the appliance shall perform and meet the specifications as identified in the appropriate section of UCR 2008.

Conference Calling A feature that allows the user to establish a call involving up to six conferees (including the user).

Congested Condition One hundred percent utilization of bandwidth on the link, or links, under test. Link traffic may be any combination of real time services (RTS) traffic and data, up to and including specified traffic engineering (i.e., 25 percent voice, 25 percent video, and data up to 100 percent).

Control Plane Quality of service mechanism to provide the ability to route data correctly and perform actions during session establishment and operation to allow a network to meet quality of service needs in the data plane. The purpose of this plane is to define the configuration, start-up conditions, and instability conditions of the control protocols, which may include routing protocols, multicast protocols, link management, and multiprotocol label switching (MPLS) protocols.

Section A2 – Glossary and Terminology Description

Converged Local Area Network (CLAN) A local area network (LAN) is an Internet Protocol (IP) network, composed of routers and LAN switches, that is used to connect nodes that are geographically close, usually within the same building. In a wider view of a LAN, multiple LANs are interconnected in a geographically compact area, usually by attaching the LANs to a higher-speed local backbone called a campus area network (CAN). A CAN is larger than a LAN but smaller than a metropolitan area network (MAN) or wide area network (WAN). A CLAN is a LAN that supports multiple types of IP services. In the DoD, the CLAN supports voice, video, and data services as a minimum. The CLAN is not intended to support C2 users and the requirements associated with a CLAN are those that are typical for commercial real time service (RTS) CLANs to include commercial grade power and availability requirements.

Converged Network An Internet Protocol (IP) network used to transmit a combination of voice, video, and/or data services.

Cryptographic Boundary An explicitly defined continuous perimeter that establishes the physical bounds of a cryptographic module and contains all the hardware, software, and/or firmware components of a cryptographic module.

Cryptographic Module The set of hardware, software, and/or firmware that implements approved security functions, including cryptographic algorithms and key generation, and are contained within the cryptographic boundary.

Customer Edge Router (CE Router) A router located at the boundary between the Edge segment and the Access segment of the WAN. The customer edge router (CER) provides traffic conditioning, bandwidth management on a granular service class (i.e., voice, video) basis, and quality of service (QoS) using per hop behaviors (PHBs). A base/post/camp/station (B/P/C/S) may have a single CER or multiple CERs based on the local architecture.

D

Data Plane Quality of service mechanism to provide the ability to manage and forward data packets, including one or more of the following: packet marking and re-marking, implementing scheduling and packet drop priorities, metering the traffic and performing congestion control, and policing and shaping the traffic. The purpose of this plane is to define the configuration, start-up conditions, and instability conditions of the data traffic including the traffic, collection of network elements, links between network elements, and interface profile.

Default Best Effort (BE) This is the common, best-effort forwarding behavior available in existing routers. When no other agreements are in place, it is assumed that the packets belong to this aggregate. Such packets may be sent into a network without adhering to any particular rules,

and the network will deliver as many of these packets as possible and as soon as possible, subject to other resource policy constraints. This forwarding behavior is not be used for VoIP.

Defense Switched Network (DSN) An interbase, nonsecure or secure DoD telecommunications system that provides dedicated telephone service, voice-band data, and dial-up Video Teleconference (VTC) for end-to-end command use and DoD authorized command and control (C2) and non-C2 users in accordance with national security directives. Non-secure dial-up voice (telephone) service is the system's principal service.

Denied Originating Service A system feature that provides the capability to deny call originations selectively to individual lines.

Deployable Voice Exchange (DVX) A tactical switch with MUF capabilities to support the assured service requirements of CJCSI 6215.01C used for rapid deployment situations and contingencies in the tactical environment. The DVXs can either be DVX Commercial Off The Shelf (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 (Tandem Switch (TS)/Multifunction Switch (MFS)/End Office (EO)/Small End Office (SMEO)), if it is to be used as a temporary solution for either of the following:

- An initial capability that will be replaced by a more permanent solution for sustainment of strategic operations.
- A solution for augmenting a strategic communications facility to meet rapid growth or restoration requirements.

Deployable Voice Exchange Commercial Off-the-Shelf (DVX-C) A Government-deployable commercial switch that may have been modified for use within tactical environments to provide military-unique features (MUFs).

Deployable Voice Exchange – Legacy (DVX-L) A Government-deployable legacy voice switching system, such as the Common Baseline Circuit Switch (CBCS) and Unit Level Circuit Switch (ULCS).

Deployable Private Branch Exchange (PBX) A PBX that is allowed to connect to the DSN via a STEP/Teleport. Deployed PBX1s do not tandem calls and 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.

Section A2 – Glossary and Terminology Description

Differential Treatment A mechanism that allows differential handling of packets in the Edge and Core nodes. It also includes providing differential treatment at the time of resource reservation and provisioning requests.

Differentiated Services (DS) A quality of service delivery model, in which the flows are classified, policed, marked, and shaped at the edges of a DS domain. The nodes in the core of the network handle packets according to the per hop behavior (PHB) that is selected on the basis of the contents of the DS field (Differentiated Services Code Point (DSCP)) in the packet header.

Differentiated Services Architecture Contains two main components. One is the fairly well understood behavior in the forwarding path and the other is the more complex and still emerging background policy and allocation component that configures parameters used in the forwarding path. The differentiated services architecture is based on a simple model where traffic entering a network is classified and possibly conditioned at the boundaries of the network, and assigned to different behavior aggregates. Each behavior aggregate is identified by a single Differentiated Services Code Point (DSCP). Within the core of the network, packets are forwarded according to the per hop behavior (PHB) associated with the DSCP. [RFC 2475].

Differentiated Services (DS) Field (DSField) The six most significant bits of the Internet Protocol version 4 (IPv4) Type of Service (TOS) octet or the Internet Protocol version 6 (IPv6) traffic class octet.

Differentiated Services Code Point (DSCP) A value that is encoded in the Differentiated Services (DS) field and that each DS node must use to select the per hop behavior (PHB) that is to be experienced by each packet it forwards.

Directed Inward Dial (DID) A feature that allows an incoming call to reach a specific PBX station line without attendant assistance. With DID, the switch seizes a DID trunk and output 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.

Disruptive A disruptive action is one that prevents a given quantity of end instruments from placing or receiving a session for more than 5 minutes.

Directed Call Pickup A feature that 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.

DoD Directives Broad DoD policy documents containing what is required by legislation, the President, or the Secretary of Defense to initiate, govern, or regulate actions or conduct by the DoD Components within their specific areas of responsibilities.

DoD Secure Communications Devices (DSCD) Hardware devices that, when placed in the secure mode, protects the transmission of classified voice, data, or facsimile over the Defense Switched Network (DSN) or other connected networks to another compatible DSCD. Examples of DSCDs include, but are not limited to, Secure Terminal Equipment (STE), Secure Telephone Unit – Third Generation (STU-III), plus the Omni and Sectera Wireline Terminals (WLTs), secure GSM, and other like devices, including wireless devices.

E

Edge Boundary Controller (EBC) An appliance that provides RTS firewall functions. The EBC is located at the boundary between the Edge Segment and the Access Segment. The EBC is a logical entity and its functionality may be implemented in one or more physical platforms. The EBC is used to exert control over the signaling and media streams and is involved in setting up, conducting, and tearing down sessions. EBCs are put into the signaling and/or media path between the calling and the external called party. The effect of this behavior is that not only the signaling traffic, but also the media traffic (i.e., voice, video) crosses the EBC. Ultimately, EBCs allow their owners to control the kinds of session that can be placed through the networks on which they reside, and overcome some of the problems that firewalls and Network Address Translation (NAT) cause for IP real time service (RTS) sessions. As a minimum, the EBC provides topology hiding, “pinholing,” and filtering.

Elastic Service A service that has high tolerance for packet loss, delay, and jitter (i.e., delay variation) at packet and overall message level. This service can tolerate a wide variation in the throughput.

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

Encapsulated Time Division Multiplexing (TDM) T1/E1 or Fractional T1/E1 encapsulated within an alternate transport mechanism that provides assured bandwidth for both signaling and bearer channels.

End Instrument (EI) An EI is a user appliance that initiates, accepts, and/or terminates a voice or video session. End instruments may be stand-alone applications or may be used in conjunction with other applications (e.g., softphone). They may provide a single service (e.g.,

Section A2 – Glossary and Terminology Description

voice or video) or multiple services (e.g., videophone). In addition, EIs may signal the Local Session Controller (LSC) with standardized protocols or proprietary protocols.

The EI is the primary user interface to customers for voice or video and is the originating or terminating endpoint for all voice or video sessions. It is the appliance at which the user assigns the precedence to the voice or video session, and the EI is responsible for collecting and disseminating the user authentication information to the LSC. Finally, the EI is the point at which the network level Class of Service (CoS) markings are set based on instructions from the LSC.

End Office (EO) A central office at which user lines and trunks are interconnected, providing long-distance service by interconnecting with Defense Switched Network (DSN) nodal switches. End Office switches provide users with switched call connections and all DSN service features, including Multilevel Precedence and Preemption (MLPP).

A switch which is integral to the DSN and serves as a primary switch for long distance services for either an installation or group of installations in a geographic area by interconnecting users to the DSN nodal switches.

Entity An appliance or human that uses the system.

Expedited Forwarding (EF) The forwarding treatment for a particular Differentiated Services (DS) aggregate where the departure rate of the aggregate's packets from any DS node must equal or exceed a configurable rate. The EF traffic should receive this rate independent of the intensity of any other traffic attempting to transit the node. If the EF PHB is implemented by a mechanism that allows unlimited preemption of other traffic (e.g., a priority queue), the implementation shall include some means to limit the damage EF traffic could inflict on other traffic (e.g., a token bucket rate limiter). Traffic that exceeds this limit shall be discarded. [RFC 3246]

F

Fixed Wireless End Instrument (WEI) Those wireless end instruments (WEIs) that access a single wireless LAN access system (WLAS) for the duration of the session and are not expected to traverse between WLASs so that handoffs are required.

Flow A group of packets with similar attributes as defined by a subset of the parameters in the Internet Protocol (IP) header of each packet (see Microflow).

Future Narrowband Digital Terminal/Secure Communications Interoperability Protocol

(FNBDT/SCIP) A protocol used to conduct a secure session with another FNBDT/SCIP capable device. SCIP and FNBDT are synonymous terms and refer to the protocols currently documented in the SCIP series of documents (e.g., SCIP-215, 216.). The current preference is to use SCIP because it more accurately reflects a protocol (layer 7) as opposed to the use of FNBDT, which implies a terminal type.

G

Granular Service Class Represents the atomic identification of a service class. A set of granular service classes, sharing similar traffic characteristics form an aggregate service class.

Guaranteed Service The use of signaling to reserve network resources end-to-end to meet preset performance objectives.

H

H.323 to H.320 Gateway A videoconferencing endpoint that converts between H.323 IP endpoint protocols and services and H.320 endpoint protocols and services for transport of videoconferencing data between IP and serial or integrated services digital network (ISDN) sessions.

I

In-band Term used when network management system connects to the network device using the same Ethernet port communication channel used for user traffic.

Incoming Access Allows a community of interest (COI) user to receive local calls from all other non-COI user and from those other COI users who allow outgoing access.

FOR OFFICIAL USE ONLY

Appendix A1 – Definitions, Abbreviations and Acronyms, and References

Section A2 – Glossary and Terminology Description

Incoming Access with Precedence Allows a community of interest (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.

Individual Line A line arranged to serve only one main station, although additional stations may be connected to the line as extensions of the main station.

Inelastic Service A real time service (RTS) that typically requires strict bounds on packet loss, delay, and jitter. It cannot tolerate throughput variations based on network load level. In this architecture, a Circuit Emulation, commonly identified as a mechanism, has been included in this category to meet special DoD messaging requirements.

Information Assurance (IA) Enabled Product A system whose primary function is not IA, but does have some IA functions.

Information Assurance (IA) Product A system that provides IA functions consistent with the IA services and categories (i.e. authentication, confidentiality). An IA product's primary purpose is to provide IA functions.

Information Technology (IT) Products Systems that receive, process, store, display, or transmit DoD real time services (RTS).

Instant Messaging (IM) The capability for users to exchange one-to-one ad hoc text messages over a network in real time. IM is not the same as and must not be confused with signaling or equipment messaging; IM is always user generated and user initiated.

Integrated Access Switch (IAS) Customer premise equipment (CPE) system that interconnects a Defense Switched Network (DSN) switch and terminal equipment (TE), such as inverse multiplexers (IMUXs), routers, video teleconferencing (VTC) codecs, VTC monitors, and multipoint control units (MCUs) (see Figure 5.2.12-6, Typical Connections for an IAS). The IAS is able to originate multiple data and/or video calls according to the worldwide numbering and dialing plan (WWNDP). 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 multilevel precedence and preemption (MLPP), but is 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 is be provisioned so 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 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 Customer Premise Equipment (CPE) system that interconnects a Defense Switched Network (DSN) switch and Terminal Equipment (TE), such as Inverse Multiplexers (IMUXs), routers, video teleconferencing (VTC) codecs, VTC monitors, and Multipoint Control Units (MCU) (see [Figure A-1](#), Typical Connections for an IAS).

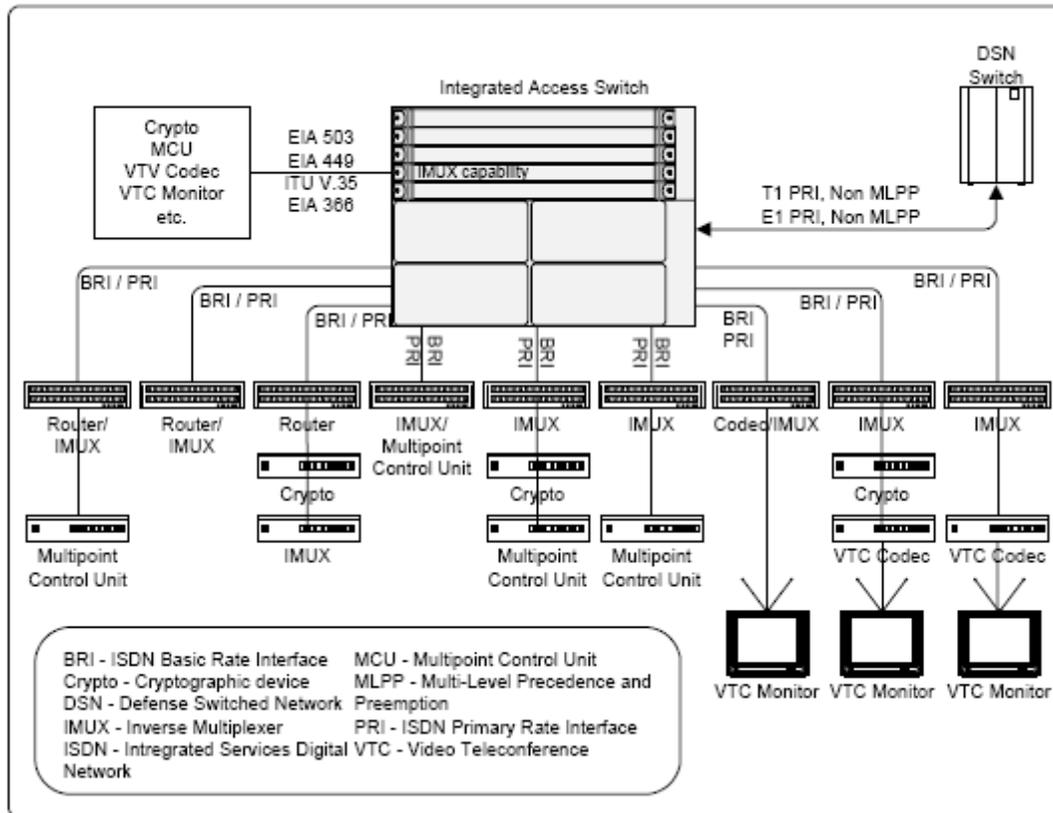


Figure A-1. Typical Connections for an IAS

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 A-2](#), MLPP Implementation and the IAS).

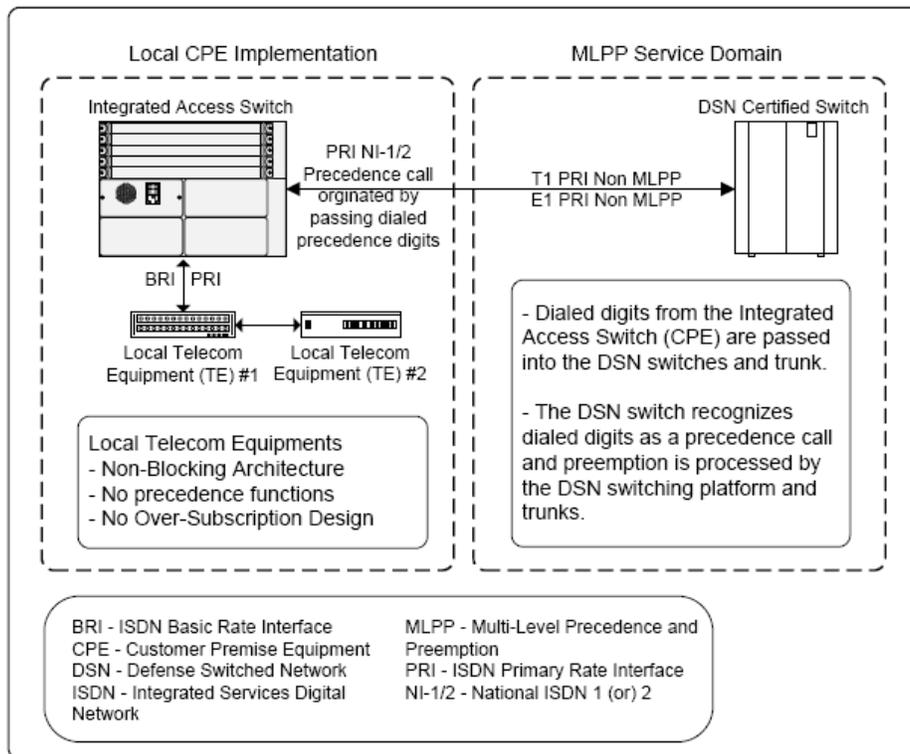


Figure A-2. MLPP Implementation and the IAS

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 A-1](#).

[Figure A-3](#), Applications for the IAS, shows the applications for the IAS.

Integrated Services Digital Network (ISDN) Devices ISDN specifies a number of reference points that define logical interfaces between functional ISDN devices such as terminals, terminal adapters, network termination devices, and line termination equipment. ISDN specifies a number of reference points that define the interconnection of these devices.

ISDN devices are defined as:

TE1 Terminals with built-in ISDN connection capability (also referred to as TE).

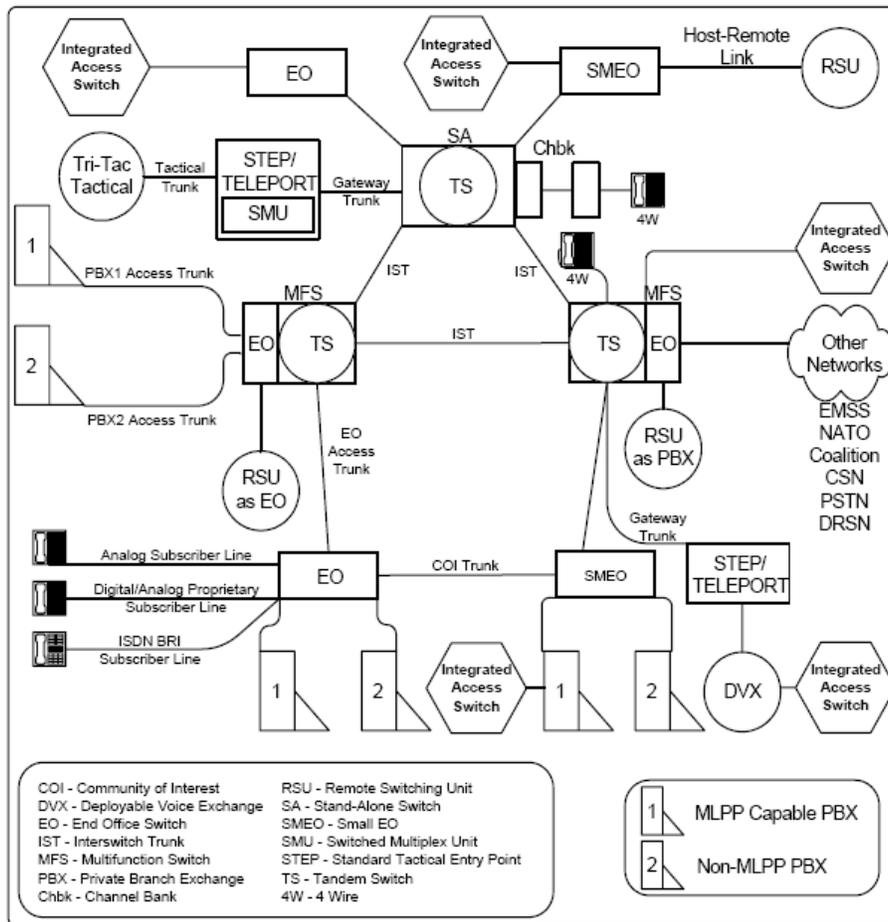


Figure A-3. Applications for the IAS

TE2 An existing terminal device, designed for existing protocols. It is not capable of directly interoperating with ISDN.

TA An adaptive device designed to permit TE2s to interoperate with ISDN.

Integrated Services Digital Network (ISDN) Integrated Access Interface An ISDN user-network interface in which the interface structure is composed of multiple B-channels and one D-channel.

Integrated Services Digital Network (ISDN) NT 1 A single (physical) layer device that contains all the necessary interface elements to communicate with the network. It terminates the local loop and provides the user interface to the network while isolating this user from the operation of the network.

Section A2 – Glossary and Terminology Description

Integrated Services Digital Network (ISDN) R The reference point representing a standardized non-ISDN interface, such as EIA-232, EIA-422, V.24, V.35, and others. The combination of a TA and TE2 is equivalent to a TE1.

Integrated Services Digital Network (ISDN) Reference Points The reference points applicable for Defense Switched Network (DSN) customer premises equipment (CPE) are as follows:

- 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.
- 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, and others. The combination of a TA and TE2 is equivalent to a TE1.

Integrated Services Digital Network (ISDN) 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.

Integrated Services Digital Network (ISDN) TA An adaptive device designed to permit TE2s to inter-operate with ISDN.

Integrated Services Digital Network (ISDN) TE1 Terminals with built-in ISDN connection capability (also referred to as TE).

Integrated Services Digital Network (ISDN) TE2 An existing terminal device designed for existing protocols. It is not capable of directly interoperating with ISDN.

Integrated Services Digital Network (ISDN) 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.

Internet Protocol (IP) Centric Internet Protocol centric architectures are designed around an IP core packet switching system. These solutions have distributed IP devices that function together to provide voice and video over IP services.

Internet Protocol (IP) Data Subscriber A user connected to an IP network to receive Department of Defense (DoD) IP services, such as data and IP video. Defense Switched Network (DSN) IP telephony is not included.

Internet Protocol (IP) Enabled An approach that utilizes traditional time division multiplexing (TDM) circuit switches that offer Voice over IP (VoIP) at a line-side instrument. This solution has a TDM circuit switch as the core device with VoIP being provided as a line function similar to other analog or digital telephony instruments. The requirements of the UCR 2008 Section 5.2 for nonsecure or secure voice, data, video conferencing (VTC), and facsimile (fax) are met primarily via the circuit switch portion. The Defense Switched Network (DSN) interface requirements (i.e., T1/E1) are provided via the circuit switch and the connectivity to the IP local area network (LAN) is via Ethernet. IP-enabled architectures can be certified for private branch exchange (PBX) through multifunction switch (MFS) applications.

Internet Protocol Packet Delay Variation (IPDV) The one-way IPDV(n) is defined as the difference between the one-way delay of the selected packet and the packet with the lowest IP Packet Transfer Delay (IPTD) in the evaluation interval: $IPDV(n) = IPTD(n) - IPTD(0)$. [ITU-T Y.1540, IETF RFC 3393]. In the case of real time services (RTS)RTS, the measurements are typically taken at the end instruments. This is also referred to as jitter.

Internet Protocol Packet Loss Ratio (IPLR) A metric measured for packets traversing the network segment between the source reference point and destination reference point. The IPLR metric is reported as the number of lost packets at the destination reference point divided by the number of packets sent at the sender reference point to that destination. [ITU-T Y.1540, IETF RFC 2680]. This is also referred to as packet loss.

Internet Protocol Packet Transfer Delay (IPTD) The single instance of the one-way IPTD measurement is defined as the time the test packet traverses the network segment(s) between two reference points. The metric is defined as a time starting from the time the first bit of the packet is put on the wire at the source reference point to the time the last bit of the packet is received at the receiver reference point. [ITU-T Y.1540, IETF RFC 2679] In the case of real time services (RTS), the measurement points are the end instruments. This is also referred to as latency.

Internet Protocol Signaling Gateway (IPSG) Function A signaling appliance that relays, translates, or terminates IP messages between various IP signaling protocols such as Assured Service Session Initiation Protocol (AS-SIP), H.323, H.248, and IP proprietary signaling protocols.

Internet Protocol (IP) Telephony Subscriber A Defense Switched Network (DSN) command and control (C2) or non-C2 user that receives voice service via an IP telephone instrument (also known as an End Instrument).

Section A2 – Glossary and Terminology Description

Internet Protocol (IP) Transport The aggregation of various types of IP traffic, such as voice, video, and data, and that is transmitted over IP link(s).

Internet Protocol Version 6 (IPv6) Capable A system or product capable of receiving, processing and forwarding IPv6 packets and/or interfacing with other systems and protocols in a manner similar to that of IP version 4 (IPv4).

Internet Protocol Version 6 (IPv6) Capable Networks Networks that can receive, process, and forward IPv6 packets from/to devices within the same network and from/to other networks and systems, where those networks and systems may be operating with only Internet Protocol Version 4 (IPv4), only IPv6, or both IPv4 and IPv6.

Internet Protocol Version 6 (IPv6) Capable Products Products (whether developed by commercial vendor or the Government) that can create or receive, process, and send or forward (as appropriate) IPv6 packets in mixed Internet Protocol Version 4 (IPv4)/IPv6 environments.

Internet Protocol Version 6 (IPv6) Enabled Network An IP network that is supporting operational IPv6 traffic through the network end-to-end.

Internet Protocol (IP) Video Subscriber A Defense Switched Network (DSN) non-command and control (C2) user that receives video service via an IP video system.

J

Jitter The one-way jitter is defined as the difference between the one-way delay of the selected packet and the packet with the lowest IP Packet Transfer Delay (IPTD) in the evaluation interval: $IPDV(n) = IPTD(n) - IPTD(0)$. [ITU-T Y.1540, IETF RFC 3393]. In the case of real time services (RTS), the measurements are taken at the end instruments. This is also referred to as the IP Packet Delay Variation (IPDV).

K

KG-194/194A (National Security Agency (NSA) cryptographic device nomenclature) A Federally-certified cryptographic device used to provide data encryption at data rates from 9.6 kilobits per second (kbps) up to 13 megabits per second (Mbps) over synchronous serial links, typically on dedicated circuit networks.

KIV-7/KIV-7HS (National Security Agency (NSA) cryptographic device nomenclature) A Federally-certified cryptographic device used to provide data encryption at data rates up to 2.048 megabits per second (Mbps) over synchronous serial links on dial-up and other nondedicated networks.

KIV-19/19A (National Security Agency (NSA) cryptographic device nomenclature) A Federally-certified cryptographic device used to provide data encryption at data rates from 9.6 kilobits per second (kbps) up to 13 megabits per second (Mbps) over synchronous serial links on dedicated circuit or dial-up network paths. The KIV-19/19A is interoperable with the KG-194/194A.

L

Latency The single instance of the one-way latency measurement is defined as the time the test packet traverses the network segment(s) between two reference points. The metric is defined as a time from the time first bit of the packet is put on the wire at the source reference point to the time the last bit of the packet is received at the receiver reference point. [ITU-T Y.1540 and IETF RFC 2679] In the case of RTS, the measurement points are typically the end instruments. This is also referred to as IP Packet Transfer Delay (IPTD).

Link The communications facilities between adjacent nodes of a network. For VoIP systems, links are Ethernet connections used for IP transport as opposed to trunks used for Time Division Multiplexing (TDM) transport.

Link Pair To ensure no single point of failure to more than 64 Internet Protocol telephony subscribers, IP network links shall have a second link (standby or load sharing). The combination of the two links is called a link pair.

Local Area Network (LAN) Access or Edge Layer The point at which local end users are allowed into the LAN. In addition, these layers may use access lists or filters to further optimize the needs of a particular set of users. This term should not be confused with the WAN Edge or WAN Access Layer.

Section A2 – Glossary and Terminology Description

Local Area Network (LAN) Core Layer A high-speed switching backbone and is designed to switch packets as fast as possible within the LAN. This term should not be confused with the WAN Core Layer.

Local Area Network (LAN) Distribution or Building Layer The distribution or building layer of the LAN 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.

Local Area Network (LAN) Network Links Internal IP/Ethernet links that interconnect LAN components.

Local Area Network (LAN) Switch A LAN switch is an appliance that reduces contention on LANs by reducing the number of nodes on a segment using microsegmentation techniques. On a microsegmented network, a LAN segment may have many nodes or a single node. The LAN switch handles all the connections between nodes on different LAN segments when they need to communicate through an internal matrix switch that processes the packets at the Media Access Control (MAC) layer. When a packet arrives at the switch, its destination MAC address is quickly noted and a connection is set up to the appropriate end segment. Subsequent packets are relayed through the switch without the need to store and forward packets, as is necessary with bridges. Many LAN switches in the DoD Internet Protocol (IP) Real Time Services (RTS) architecture include router functions.

Local Session Controller (LSC) A call stateful Assured Service (AS) Session Initiation Protocol (SIP) (AS-SIP) signaling appliance at a base/post/camp/station (B/P/C/S) that directly serves Internet Protocol (IP) end instruments. The LSC MAY consist of one or more physical platforms. On the trunk side, the LSC employs AS-SIP signaling. On the line side, the LSC may serve any combination of SIP end instruments, H.323 end instruments, and proprietary end instruments. The LSC MUST be an intermediary for every inbound and outbound call signaling message received and transmitted by each IP end instrument served by the given LSC.

Local Session Controller (LSC) Level Assured Services Admission Control (L-ASAC) The processes on an LSC that ensure that quality of service requirements of a higher precedence service will be met at the expense of a lower precedence service if the network conditions do not allow meeting quality of service requirements of all services. The processes are typically associated with the preemption of lower precedence sessions to an end instrument to ensure that higher precedence sessions can be completed.

Location Server The purpose of the location server is to provide information on call routing and called address translation (where a called address is contained within the called Session Initiation Protocol Secure (SIPS) Uniform Resource Identifier (URI) in the form of the called

number). The service provided by the server is typically referred to as location services. The Call Connection Agent (CCA) uses the routing information stored in the location server

- a. to route internal calls from one Local Session Controller (LSC) end instrument to another end instrument on the same LSC,
- b. to route outgoing calls from an LSC end instrument to another LSC, a multifunction softswitch (MFSS), or a time division multiplexing (TDM) network, and
- c. to route incoming calls from another LSC, an MFSS, or a TDM network to an LSC end instrument or MFSS.

Long Local A long-local telephone is connected remotely through an assured transmission means, TDM or IP, to a distant site. This interface is handled as a local loop to the host DSN switch.

M

Management Plane A quality of service mechanism to access network elements for network management purposes, such as provisioning and policy setting. This plane is used to define the configuration, startup conditions, and instability conditions of the management protocols and features including Simple Network Management Protocol (SNMP), Logging/Debug, statistics collection, and management configuration sessions such as telnet, Secure Shell (SSH), and serial console.

Mean Time Between Failures (MTBF) For a particular interval, the total functional life of a population of an item divided by the total number of failures (requiring corrective maintenance actions) within the population.

Mean Time To Repair (MTTR) The total amount of time spent performing all corrective maintenance repairs divided by the total number of those repairs.

Measurement-Based Admission Control An approach that bases a call control decision on the monitoring of network capacity. Admits, rejects, or redirects calls based on current network congestion.

Media Gateway (MG) A media gateway within the DoD environment is defined in accordance with the Internet Engineering Task Force (IETF) Request for Comments (RFC) 2805 and provides the media mapping and/or transcoding functions between Time Division Multiplexing (TDM) and Internet Protocol (IP) networks. The media gateway terminates switched circuit

Section A2 – Glossary and Terminology Description

network (SCN) facilities (e.g., trunks, loops), packetizes the media stream, if it is not already packetized, and delivers packetized traffic to an IP network. It would perform these functions in the reverse order for media streams flowing from the IP network to the SCN.

Media Gateway Controller (MGC) The function in a signaling appliance that controls a media gateway.

Media Server A platform in an Internet Protocol (IP) telephony network that transmits dial tones, busy signals, and announcements.

Meet-Me Conferencing A conference that is established when each conferee dials into the conference bridge at a scheduled time as directed by a conference attendant.

Message A unit of data transfer from an application in one host to an application in another host.

Message Discrimination and Distribution Function A function that examines the Destination Point Code (DPC) of a received signaling message to determine whether or not it is destined to the receiving signaling point.

Metering The process of measuring the temporal properties (e.g., rate) of a traffic stream selected by a classifier. The instantaneous state of this process may be used to affect the operation of a marker, shaper, or dropper, and/or may be used for accounting and measurement purposes. [RFC 2475]

Metric A quality of service delivery parameter such as delay, packet loss, data rates, availability, etc.

Microflow A single instance of an application-to- application flow of packets that is identified by source address, source port, destination address, destination port, and protocol identification. [RFC 2475]

Minimum Requirements 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 DSN.

Mobile Code Software modules obtained from or provided by remote systems, transferred or downloaded across a network, and then executed on local systems without explicit installation or execution by the recipient.

Modem over IP (MoIP) The transport of modem data across an IP network, via either modem relay or voiceband data (modem pass-through) techniques.

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.

Multifunction Softswitch (MFSS) A network appliance that provides the following functions:

Provides all multifunction switch (MFS) functions:

- Tandem Switch
- End Office
- Softswitch functions
- Global directory services
- Local Session Controller (LSC) functions
- Media gateway functions
- Signaling gateway functions
- Network management
- Fault, configuration, accounting, performance, and security (FCAPS)

Supports Policy Based Network Management (PBNM):

- Assured Services Admission Control (ASAC) budget controls
- Customer Edge Router (CE-R) queue bandwidth allocations
- End instrument session origination control (according to designated groups)
- End instrument session destination control (according to designated groups)

The MFSS is a logical entity and its functionality MAY be implemented in one or more physical platforms.

The MFSS is a multifunction switch that is enhanced with an IP interface. As with any multifunction switch, the MFSS supports end office and tandem switch capabilities. In addition, the MFSS also includes LSC and Assured Real Time Services (ARTS) Softswitch (SS) functions to support line side IP end instrument and trunk side Assured Service Session Initiation Protocol (AS-SIP) and AS-SIP for Telephones (AS-SIP-T) signaling. For tandem switch end instruments connected to the MFSS, the MFSS is the media endpoint for sessions connected to an IP end instrument at the terminating location

Multifunction Switch (MFS) “A switch that combines the tandem function of the SA [Stand-Alone] switch with the EO [End Office] function of connecting the user’s lines to the backbone

Section A2 – Glossary and Terminology Description

trunks. Logically the SA and EO are separate, but within the same physical configuration. [CJCSI 6215.01C]

Multilevel Precedence and Preemption (MLPP) In circuit-switched systems, a priority scheme:

1. For assigning one of several precedence levels to specific calls or messages so that the system handles them in a predetermined order and time frame,
2. For gaining controlled access to network resources in which calls and messages can be preempted only by higher priority calls and messages,
3. That is recognized only within a predefined domain, and
4. In which the precedence level of a call outside the predefined domain is usually not recognized.

Multilevel Precedence and Preemption (MLPP) Call A call that has a precedence level established and is either being setup or is setup. In Digital Subscriber Signaling System No. 1 (DSS1: ISDN Q.931 signaling), an MLPP call is a call from an MLPP subscriber for which a setup has been sent but no DISCONNECT has been sent or received.

Multilevel Precedence and Preemption (MLPP) Service Domain A set of MLPP subscribers (MLPP users) and the network and access resources that are in use by that set of MLPP subscribers at any given time. Connections and resources that are in use by MLPP subscribers may be preempted only by higher precedence calls from MLPP subscribers within the same domain. The service domain consists of a 3-octet field ranging from 00 00 00 to FF FF FF in hexadecimal. The DSN service domain is zero (0).

Multipoint Control Unit (MCU) An endpoint that enables intercommunication of three or more VTC endpoints in a conference call. It can be used with two VTC endpoints, e.g., while beginning or ending a multipoint conference. The MCU may perform mixing or switching of audio, video, and data.

N

Nailed Up Connections A special use permanently established path through a switch for either a network circuit (trunk) or a special service facility.

FOR OFFICIAL USE ONLY

Appendix A1 – Definitions, Abbreviations and Acronyms, and References

Section A2 – Glossary and Terminology Description

Network All telecommunications equipment that has any part in processing a call or a supplementary service for the user referred to. It may include local exchanges, transit exchanges, and Network Termination 2 (NT2) but does not include the integrated services digital network (ISDN) terminal and is not limited to the “public” network or any other particular set of equipment.

Network Domain A contiguous set of network elements that belongs to the same administrative authority.

Network Element (NE) A component of a network through which the DSN bearer and/or signaling traffic transits. For IP transport, the IP connection may transit a Local Area Network (LAN), Metropolitan Area Network (MAN), Campus Area Network (CAN), or Wide Area Network (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, shown in [Figure A-4](#), 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.

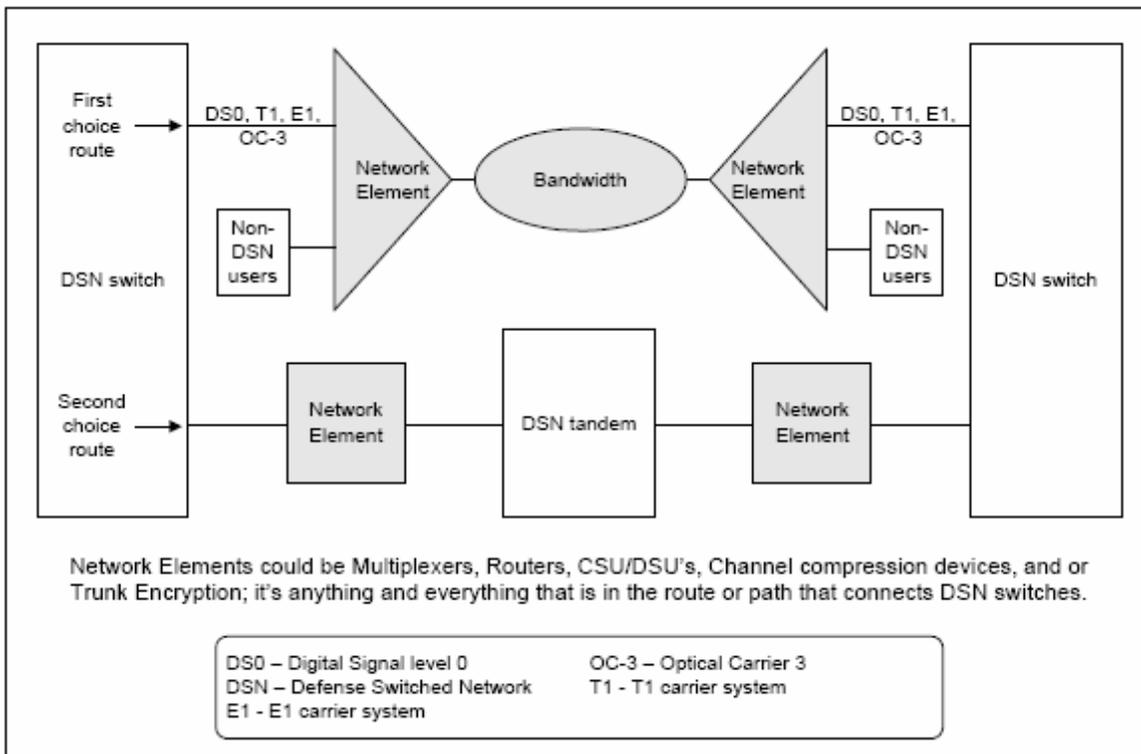


Figure A-4. Network Element Diagram

Section A2 – Glossary and Terminology Description

Network Signaling Based Admission Control Determines based on requests indicated through a signaling protocol whether a node or network has sufficient available resources to meet the requested quality of service. [RFC 2205]

New Call The event that precipitates a trunk seizure or when preemption for reuse of a trunk is used to support multilevel precedence and preemption (MLPP) calls in the Defense Switched Network (DSN).

Nomadic Wireless End Instrument (WEI) Those wireless end instruments (WEIs) that are mobile and may traverse different wireless LAN access systems (WLASs) during a single session.

Non-Assured Service Local Area Network (Non-ASLAN) The IP network infrastructure components used to provide services (i.e., voice, video, and data) to end users. Non-ASLANs are “commercial grade” and provide support to C2 (ROUTINE only calls) (C2(R)) or non-C2 voice subscribers.

Non-Blocking Local Area Network (LAN) A LAN that is provisioned so all Internet Protocol (IP) telephone instruments can be off hook simultaneously and successfully engaged in a full duplex voice call.

Non-Command and Control (C2) Users Those users, Department of Defense (DoD), non-DoD, non-U.S. Government and foreign government users that have no missions or communications (equipment) requirements to originate or receive C2 communications under the existing military scenarios. These users are provided access to the Defense Switched Network (DSN) for economic benefit of the DoD. During a crisis or contingency, these users may be denied access to the DSN. It is the primary means of secure (Secure Telephone Unit, Third Generation (STU-III)/Secure Terminal Equipment (STE) family) communications for non-tactical C2 users. The DSN must be the user’s first choice; however, if the DSN is not immediately available, or if the called party does not have access to DSN service, other long-distance calling methods may be used.

Non-Converged Network A network that is used solely to provide Defense Switched Network (DSN) Voice over Internet Protocol (IP) (VoIP) services. A separate IP network will be used to provide IP data services.

Non-Preemptive Service A Global Information Grid (GIG) service which offers a committed information rate (CIR) between two or more Edge networks, where the bandwidth cannot be preempted for the use of any other party than the one contracting for the service.

Non-Signaled Flow A flow which does not require signaling to enter a network.

O

Objective Requirement [Objective] A requirement that does not have to be met in the initial operational capability (IOC), but must be met in the final operational capability (FOC). The time frame associated with the IOC is fiscal year (FY) 2008 and the time frame associated with the FOC is FY12 unless specifically stated.

Offered Load Control A mechanism that allows control of packet transfer loads to keep them within specified bounds (possibly described in Service Level Agreements (SLAs)) so that network domains can deliver the promised quality of service.

Operations, Administration, and Maintenance (OA&M) A set of network management functions, providing network fault indication, performance information, and data and diagnosis functions.

Originating Internet Protocol (IP)/Time Division Multiplexing (TDM) Signaling Gateway Function The function related to receiving an Initial Address Message (IAM) from the Signaling System No. 7 (SS7) network and generating an Assured Service Session Initiation Protocol (AS-SIP) INVITE with the encapsulated Integrated Services Digital Network User Part (ISUP) IAM that is sent over the IP network – identical to Outgoing Interworking Unit (O-IWU) in International Telecommunications Union – Telecommunication Standardization Sector (ITU-T) Recommendation Q.1912.5, Interworking between Session Initiation Protocol (SIP) and Bearer Independent Call Control Protocol or ISDN User Part.

Originating Gateway An Assured Service Session Initiation Protocol for Telephones (AS-SIP-T) signaling appliance performing the originating Internet Protocol (IP)/Time Division Multiplexing (TDM) signaling gateway function.

Outgoing Call Trace A feature that 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.

Out-of-band A term used to describe network management systems that connect to the network device using a physically separated network from the network used for user traffic. This requires an additional network infrastructure to support management traffic.

Section A2 – Glossary and Terminology Description

Overflow Process A process that allows calls of a lower precedence level and narrower calling area to utilize unused calling capacity of a higher precedence level and equal and wider calling area, and equal precedence level and wider calling area call types without blocking calls of a higher precedence level and wider calling area.

P

Packet Loss A metric measured for packets traversing the network segment between the source reference point and destination reference point. The Packet Loss metric is reported as the number of lost packets at the destination reference point divided by the number of packets sent at the sender reference point to that destination. [ITU-T Y.1540, IETF RFC 2680]. This is also referred to as Internet Protocol Packet Loss Ratio (IPLR).

Packet Marking Marking in packets following their classification for a given service delivery; which includes Differentiated Services Code Point (DSCP), Flow Label, or Security Parameter Index (SPI) bit fields.

Path Communications link between two network components. A path may include a number of communications links.

Per-Domain Behavior (PDB) An externally observable edge-to-edge functional and performance quality of service behavior on a per-domain basis.

Per Hop Behavior (PHB) An externally observable forwarding behavior applied at a DiffServ-compliant node to a DiffServ behavior aggregate based on the Differentiated Services Code Point (DSCP) marking in the packet. [RFC 2475]

Policing The process of discarding packets (by a dropper) within a traffic stream in accordance with the state of a corresponding meter enforcing a traffic profile. [RFC 2475]

Precedence The designation assigned to a message by the originator to indicate its relative level of importance of the message up to the originator's maximum authorization level as defined by DoD requirements documents.

Precedence-Based Assured Service (PBAS) This service implies that, in general, quality of service requirements of a higher precedence class will be met at the expense of a lower precedence class if the network conditions do not allow meeting quality of service requirements of all service classes.

Precedence Based Treatment The process of allocating network resources to the higher-precedence messages more favorably while restricting lower-precedence traffic during periods of resource shortage.

Precedence Inversion The phenomenon that occurs when a higher precedence flow or flow aggregate does not receive its quality of service commitments, while a lower-precedence flow or flow aggregate competing for the same communications source does receive its quality of service commitments.

Precondition "A precondition is a set of constraints about the session that are introduced in the offer. The recipient of the offer generates an answer, but does not alert the user or otherwise proceed with session establishment. That only occurs when the preconditions are met. This can be known through a local event (such as a confirmation of a resource reservation), or through a new offer sent by the caller." [RFC 3312]

Preemptable Circuit A circuit that is active with or reserved for an MLPP call: (a) within the same domain as the preempting call and (b) with a lower precedence than the preempting call. A busy or reserved circuit for which a precedence level has not been specified is not a preemptable circuit.

FOR OFFICIAL USE ONLY

Appendix A1 – Definitions, Abbreviations and Acronyms, and References

Section A2 – Glossary and Terminology Description

Preemption Initiating Exchange An exchange that is congested (i.e., no idle circuits) and has received a preempting call setup.

Preferred Elastic A specially created service class category to meet unique DoD application requirements; it has varying degrees of service class categories. Examples include short, interactive transactions and delay-sensitive file transfers.

Presence/Awareness A status indicator that conveys ability and willingness of a potential user to communicate. A user's client provides presence information (presence state) via network connection to a presence service, which is stored in what constitutes the user's personal availability record (called a presentity) and can be made available for distribution to other users (called *watchers*) to convey the user's availability for communication. Presence information has wide application in many communication services and is one of the innovations driving the popularity of instant messaging (IM) or recent implementations of voice over IP clients.

A user client may publish a presence state to indicate its current communication status. This published state informs others that wish to contact the user of the user's availability and willingness to communicate. The most common use of presence is to display a status indicator icon on IM clients, and a list of corresponding text descriptions of each of the states. Even when technically not the same, the "on-hook" or "off-hook" state of a called telephone is an analogy; the caller receives a distinctive tone indicating unavailability ("line busy") or availability ("ring-back tone" followed by voice mail).

Private Branch Exchange (PBX) PBX Line 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.

Private Branch Exchange (PBX) Type 1 (PBX1) A PBX with MLPP capabilities. Based on mission requirements, this switch may serve those non-C2 users defined as DoD users having a military mission that might receive C2 calls for orders or direction at precedence levels above a ROUTINE precedence, even though they do not have a C2 mission for issuing guidance or orders. Special C2 users are not authorized to be served by a PBX1 and must connect to an EO or SMEO.

Private Branch Exchange (PBX) Type 2 (PBX2) A PBX with no MLPP capabilities. This switch can serve only DoD, non-DoD, non-governmental, and foreign government users having no missions or communications requirement to ever originate or receive C2 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 Public Telephone and Telegraph (PTT) ordinances. During a crisis or contingency, they may be denied access to the DSN. The C2 and Special C2 users are not authorized to be served by a PBX2.

Propagation Delay Travel time of an electromagnetic signal from one measurement point to another.

Proprietary IP Trunk (PIPT) A virtual network element that provides a virtual IP trunk connection between a pair of certified switches (e.g., DVX to DVX, DVX to Private Branch Exchange Type 1 (PBX1), DVX to Private Branch Exchange Type 2 (PBX2), etc.). The PIPT may use proprietary signaling but must support the equivalent features and functions of a primary rate interface (PRI), multilevel precedence and preemption (MLPP) (T1.619a), or non-MLPP (NI 1/2), as appropriate.

Proxy Server “An intermediary entity that acts as both a server and a client for the purpose of making requests on behalf of other clients. A proxy server primarily plays the role of routing, which means its job is to ensure that a request is sent to another entity “closer” to the targeted user. Proxies are also useful for enforcing policy (for example, making sure a user is allowed to make a call). A proxy interprets, and, if necessary, rewrites specific parts of a request message before forwarding it.” [RFC 3261]

Q

Quality of Service (QoS) The capability to provide resource assurance and service differentiation in a network. Used with the LAN to provide different priority to traffic flows/sessions, or guarantee a certain level of performance to a traffic flow/session in accordance with requests from the application program. Quality of Service is used in conjunction with traffic tagging to guarantee that prioritized traffic flows/sessions are given preferential treatment.

Quality of Service Domain An administrative network domain that is designed based on a single quality of service architecture and operated under the same set of quality of service policies.

Quality of Service Network A quality of service aware or enabled network; it consists of one or more interconnected quality of service domains.

Queuing Delay Waiting time of a packet for its turn to be serviced at the interface of a network device, such as a router.

R

Reliability The ability of a system and its parts to perform its mission without failure, degradation, or demand on the support system. See Mean Time Between Failures (MTBF) and Mean Time Between Maintenance (MTBM).

Release to Pivot (RTP) 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. An application that determines the new destination for the call (in this case, the operator services switch) can release the call then 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.

Remote Switching Unit (RSU) A telecommunications switch that is connected to and dependent upon a host switch (EOS, MFS, or SMEO) for some or all centralized operations, administrative, and maintenance capabilities. It is a switching function integral to the DSN (and part of the GIG). The RSU may be used to provide different functions: EO/SMEO or PBX. If used as an EO/SMEO, the RSU must meet all the requirements of an EO/SMEO; and be connected via the host-remote link to a DSN backbone stand-alone switch or MFS. If used as a PBX, the RSU must meet all the requirements of a PBX; and be connected via a host-remote link to an installation EO/SMEO. Mission requirements of the users connected to the RSU dictate site-specific application as an EO/SMEO or PBX. The RSUs will be tested with and without the host switch for interoperability certification.

Remote Switching Unit (RSU) Degraded Operations RSU operations when one of two conditions are met; (1) stand-alone, when the host link umbilical has been severed; and (2) partial stand-alone, when the host link umbilical is saturated with traffic or the host link is partially “out-of-service.”

Remote Switching Unit (RSU) Normal Operations RSU operations when the umbilical line or trunk is fully connected to the host switch, and neither the host nor the RSU is in a degraded condition

Remote Switching unit (RSU) Standalone Operations RSU operations when the umbilical links between the host and the RSU are completely severe.

Required Requirement [Required] A requirement is required if it must be met in the initial operational capability (IOC). The IOC is associated with the fiscal year (FY) 2008 time frame. An IOC requirement is often labeled a Threshold requirement to differentiate the requirement from an Objective requirement.

Resource Reservation Protocol (RSVP) A protocol developed by the Internet Engineering Task Force (IETF) for hosts (applications) and routers to communicate service requirements to the network and to enable the routers in the network to set up the reservations.

Response Time Round-trip delay from a network application source through destination, back to the application source.

Route Code 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.

Router A router is an appliance that is a packet switch that operates at the network layer of the Open Systems Interconnection (OSI) protocol model. Routers within the Internet Protocol (IP) Real Time Services (RTS) architecture interconnect networks over local and wide areas, and provide traffic control and filtering functions when more than one pathway exists between two endpoints on the network. The primary function of routers is to direct IP packets along the most efficient or desired path in a meshed network that consists of redundant paths to a destination. Many routers in the DoD IP RTS architecture include local area network (LAN) switch functions and the distinction between the two types of appliances continues to blur.

S

Secure Communications over IP (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.

Secure Cryptographic Processes Secure cryptographic processes constitute the basic requirement for effective data security and effective data protection in the use of information technology. The basic requirements include digital signatures, authentication and access control, and encryption.

FOR OFFICIAL USE ONLY

Appendix A1 – Definitions, Abbreviations and Acronyms, and References

Section A2 – Glossary and Terminology Description

Secure End Instrument (SEI) An end instrument that is able to operate in the normal real time services (RTS) mode and in a secure (typically type 1 encryption) mode. The primary function of the SEI is to maintain RED/BLACK separation by applying upstream media encryption for secure calls while maintaining multilevel security (MLS) filtering to allow a user to talk in either secure or non-secure mode. The Internet Protocol (IP) SEI is not currently designed to support secure video. It is hoped that the Voice over IP (VoIP) secure terminal equipment (STE) will adopt the Assured Service Session Initiation Protocol (AS-SIP) as the RTS signaling protocol, which will allow it to interoperate with any AS-SIP-based Local Session Controller (LSC). However, it is not known if that capability will be included and the earliest that it might occur is fiscal year (FY) 2012. For the purposes of this document, the term end instrument shall apply to an end instrument or SEI unless specifically noted.

Secure Telephone Equipment (STE) This term refers to both a DSCD and a mode of operation. It is a DSCD that utilizes any one of the multiple supported protocols to conduct a secure session with another compatible protocol device (e.g., STE, STU-III, or FNBDT/SCIP capable device).

Secure Telephone Unit (STU) This term refers to both a DSCD and a mode of operation. STU has a specific protocol that is used for conducting a secure session with another STU compatible DSCD.

Selective Call Forwarding A feature that allows customers to have only calls from selected calling parties forwarded.

Service Class A set of traffic that requires specific delay, loss, and jitter characteristics from the network for which a consistent and defined per hop behavior (PHB) applies.

Service Level Agreement (SLA) Binding contractual agreement between two parties, Global Information Grid (GIG) networks service provider and GIG users, listing offered services and service-level specifications regarding the technical parameters of the service requested. An SLA may include traffic conditioning rules. An SLA is often the results of the mission planning process.

Service Level Commitment (SLC) A numerical performance value that specifies a commitment made by the provider to the user, in the service level specifications (SLS) of the service level agreement (SLA).

Service Level Specification (SLS) A set of quantitative performance metrics that together define the service offered to a traffic stream by a differentiated services (DS) domain related to a specific service level agreement (SLA).

Service Provisioning Policy A policy that defines how traffic conditioners are configured on differentiated services (DS) boundary nodes and how traffic streams are mapped to DS behavior aggregates to achieve a range of services. [RFC 2475]

Session Initiation Protocol (SIP) The SIP is “...an application-layer control (signaling) protocol for creating, modifying, and terminating sessions with one or more participants. These sessions include Internet telephone calls, multimedia distribution, and multimedia conferences.” [RFC 3261]

Session Initiation Protocol (SIP) End Instrument An end instrument that supports SIP signaling.

Session Initiation Protocol (SIP) User Agents Intelligent IP telephones with SIP software that create and management a SIP session.

Session Initiation Protocol (SIP) Proxy Server Equivalent to time division multiplexing (TDM) call processing software that detects call for service (“off-hook”), analyzes address digits received, and based on data contained in translation tables/local subscriber line tables obtains the called telephone addressing information. Then it forwards the session invitation directly to the called telephone if it is located in the same domain, or to another proxy server if the call telephone resides in another domain.

Session Initiation Protocol (SIP) Redirect Server Equivalent to time division multiplexing (TDM) routing tables that allow SIP proxy servers to direct SIP session invitations to external domains. SIP redirect servers may reside in the same hardware as SIP registrar and ISP proxy servers.

Session Initiation Protocol (SIP) Registrar Server Equivalent to time division multiplexing (TDM) subscriber line database tables and classmarks for all telephones served directly off or by the Local Session Controller (LSC) controlling a domain. In SIP messaging, these servers retrieve and send participant’s IP addresses and other pertinent information to the SIP proxy server.

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. Defense Switched Network (DSN) calls shall use the SETUP message specified in American National Standards Institute (ANSI) T1.607. The Channel Identification, Calling Party Number (when available), and Called Party Number are mandatory information elements (IEs). For a Multilevel Precedence and Preemption (MLPP) call (invoking MLPP feature) on the DSN user-to-network interface, the SETUP message shall include the Precedence Level IE. It shall contain other IEs, such as the Business Group (BG) IE for the Community of Interest (COI) feature, when such unique DSN features are required and

FOR OFFICIAL USE ONLY

Appendix A1 – Definitions, Abbreviations and Acronyms, and References

Section A2 – Glossary and Terminology Description

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 the 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 Look-Ahead for Busy (LFB) option is exercised on the DSN user-to-network interface.

Seven Digit Dialing The ability to dial using the seven digits of the switch code and line number to establish either interswitch or intraswitch calls within the same numbering plan area.

Shaping The process of delaying packets within a traffic stream to cause it to conform to some defined traffic profile. [RFC 2475]

Signaled Flow A flow that requires signaling to determine if there are sufficient resources to support its quality of service requirements. If the resources do not exist or cannot be preempted, the flow is blocked from entering the network.

Signaling The process of exchanging information between two or more parties to initiate or terminate a communication session, and for the management and maintenance of the session.

Signaling Gateway (SG) Function A signaling gateway function receives/sends switched circuit network native signaling at the edge of a data network. For example the signaling gateway function MAY relay, translate or terminate SS7 signaling in an SS7-Internet Gateway. The signaling gateway function MAY also be co-resident with the media gateway function to process switched circuit network signaling associated with line or trunk terminations controlled by the media gateway, such as the “D” channel of an ISDN PRI trunk. The use of the signaling gateway function within the ARTS GSR refers only to SS7 signaling. The use of the signaling gateway within the AS SIP GSS allows for the signaling gateway to be co-resident with the media gateway. [RFC 2805]

Small End Office (SMEO) “A switch that serves as the primary switch, functions as an EO [End Office], but at smaller DOD [Department of Defense] installations. A SMEO does not have full DSN [Defense Switched Network] Network Traffic Management capabilities. It offers limited performance reporting and may not support SS7 [Signaling System No. 7] signaling. Therefore, SMEOs will not serve installations that are critical to combatant command missions where NM [network management] control and network visibility for situational awareness is required.” [CJCSI 6215.01C]

Softphone An end-user software application on an approved operating system that enables a general-purpose computer to function as a telephony end instrument. It will be tested on an

approved operating system as part of the system under test (SUT). The Softphone application is considered an IP End Instrument and is associated with the IP telephone switch.

Softswitch A programmable network appliance that:

- Controls connection services for a media gateway and/or native IP endpoints.
- Selects processes and services that can be applied to a call.
- Provides routing for call control within the network based on signaling and customer database information.

Section A2 – Glossary and Terminology Description

- Transfers control of the call to another network element.
- Interfaces to and supports management functions such as provisioning, fault, and billing.
- Ability to control the access of sessions within and external to its domain. [International Softswitch Consortium]

Special Command and Control (C2) User A special class of user who has access to the DSN for “essential communications for planning, directing, and controlling operations of assigned forces pursuant to assigned missions. This user requires capabilities that provide crises, pre-attack, and theater non-nuclear war telecommunications service for intelligence, alert, and strategic readiness.” This user also requires communications among the President, Secretary of Defense, Chairman of the Joint Chiefs of Staff, and other members of the Joint Chiefs of Staff, Service Chiefs, and the Combatant Commanders. “Specifically, these special C2 users are identified through one or more Chairman of the Joint Staff, combatant commanders, Service, or DOD agency validation processes. The following are required capabilities of special C2 users:

- Chairman of the Joint Staff-approved FLASH, FLASH OVERRIDE, or IMMEDIATE precedence origination.
- Combatant command-validated minimum-essential circuits.
- Combatant command or Service-approved IMMEDIATE and PRIORITY precedence origination.”

Strong Authentication The process of authenticating a user based on at least two of three factors: something you know (i.e., username and password), something you have (i.e., token device), and something you are (i.e., fingerprints).

Subscriber The owner of a public key contained in a Public Key Infrastructure (PKI) certificate. A subscriber may be an appliance or a person.

Survivability The capability of a system to survive in a specified threat environment and accomplish its designated mission.

Synchronization 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.

System An appliance or group of appliances. The systems described in this document include multifunction softswitches, softswitches, Local Session Controllers, media gateways, border controllers, end instruments, LAN switches, and routers.

System Under Test (SUT) The inclusive components required to test an UC Product for APL certification. Examples of a SUT include Time Division Multiplexing (TDM) or circuit switch components, Voice over Internet Protocol (VoIP) system components (e.g., Local Session Controller (LSC) and gateway), local area network (LAN) components (e.g., routers and Ethernet switches), and end instruments.

T

Tactical Network Element (T-NE) A T-NE is any network element used in the tactical network. A T-NE can be used for long local, encapsulated time division multiplexing (TDM), and Proprietary Internet Protocol Trunk (PIPTs).

Tandem Call Trace A feature that 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.

Telecom Switch/Device Hardware or software designed to send and receive voice, data, or video signals across a network that provides customer voice, data, or video equipment access to the Defense Switch Network or public switch telecommunications network.

Ten Digit Dialing The ability to use 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

Terminating Internet Protocol (IP)/Time Division Multiplexing (TDM) Signaling Gateway Function The function related to receiving an Assured Service Session Initiation Protocol (AS-SIP) INVITE from the IP network and sending an Initial Address Message (IAM) onto the Signaling System No. 7 (SS7) network. If the AS-SIP INVITE included an encapsulated Integrated Services Digital Network (ISDN) User Part (ISUP) IAM, then it is decapsulated – identical to Incoming Interworking Unit (I-IWU) in International Telecommunications Union – Telecommunication Standardization Sector (ITU-T) Recommendation Q.1912.5, Interworking between Session Initiation Protocol (SIP) and Bearer Independent Call Control Protocol or ISDN User Part.

Section A2 – Glossary and Terminology Description

Terminating Gateway Assured Service Session Initiation Protocol for Telephones (AS-SIP-T) signaling appliance performing the terminating Internet Protocol (IP)/Time Division Multiplexing (TDM) signaling gateway function in the case of TDM bridging call flows and IP-to-TDM call flows, and either directly serving the destination IP end instruments or the Assured Service Session Initiation Protocol (AS-SIP) signaling appliances representing the destination IP end instruments in the case of TDM-to-IP call flows.

Three-Way Calling A feature that allows a station in the talking state to add a third party to the call without operator assistance.

Throughput The number of octets is successfully transmitted (IP) during the measurement interval (typically seconds). Assumes the packets sent do not exceed capacity of the link. [NCIDv3 QoS (T300)]

Tracing of Terminating Calls A feature that 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.

Trace Call in Progress A feature that 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.

Traffic Classification A mechanism that allows the networks to distinguish among different categories of traffic, connection requests, and provisioning requests. The classification may be performed at the Edge and Core nodes during packet transport, as well as through indications in the control and management planes for setting up connections and provisioning. Classification can be based on fields in the packets and/or indications in control and management messages.

Traffic Conditioner An entity that performs traffic conditioning functions and may contain meters, markers, droppers, and shapers. Traffic conditioners are typically deployed in Differentiated Services boundary nodes only. A traffic conditioner may re-mark a traffic stream or may discard or shape packets to alter the temporal characteristics of the stream and bring it into compliance with a traffic profile. [RFC 2475]

Traffic Conditioning Control functions performed to enforce traffic classification rules and may include traffic metering, marking, shaping, and policing. Traffic conditioning, when used, will be tied to the parameters chosen for the offered load control.

Traffic Conditioning Agreement (TCA) An agreement specifying classifier rules and any corresponding traffic profiles and metering, marking, discarding, and/or shaping rules that are to apply to the traffic streams selected by the classifier. A TCA encompasses all traffic conditioning rules explicitly specified within a service level agreement (SLA) along with all the rules implicit from the relevant service requirements and/or from a Differentiated Services (DS) domain's service provisioning policy. [RFC 2475]

Traffic Engineering An operator or automaton with the express purpose of minimizing congestion in a network. It encompasses the application of technology and scientific principles to the measurement, modeling, characterization, and control of Internet traffic, and the application of such knowledge and techniques to achieve specific performance objectives. [RFC 2702]

Trunks Time Division Multiplexing (TDM) links used by a circuit switch system to connect to or interconnect Defense Switched Network (DSN) switches.

Trust Point Public keys (or certificates containing them) that the relying party designates as reliable and trustworthy. The relying party should obtain the public keys (or certificates) through a reliable out-of-band method. Trust points are usually Root Certificates. Under certain circumstances, a relying party may decide to trust an intermediate Certificate Authority (CA) or even an end-entity. Trust is transitive. If the relying party trusts a CA, it also trusts other CAs to which the CA delegates its CA responsibilities. This is also known as a trust anchor.

U

Unified Capabilities The seamless integration of voice, video, and data applications services delivered ubiquitously across a secure and highly available IP infrastructure to provide increased mission effectiveness to the warfighter and business communities. Unified capabilities integrate standards-based communication and collaboration services including, but not limited to, the following:

- Messaging
- Voice, video, and Web conferencing
- Presence
- Unified capabilities clients

In addition, standards-based communication and collaboration services must integrate with available enterprise applications, both business and warfighting.

FOR OFFICIAL USE ONLY

Appendix A1 – Definitions, Abbreviations and Acronyms, and References

Section A2 – Glossary and Terminology Description

User Agent Client (UAC) “A user agent client is a logical entity that creates a new request, and then uses the client transaction state machinery to send it. The role of UAC lasts only for the duration of that transaction. In other words, if a piece of software initiates a request, it acts as a UAC for the duration of that transaction. If it receives a request later, it assumes the role of a user agent server for the processing of that transaction.” [RFC 3261]

User Agent Server (UAS) “A user agent server is a logical entity that generates a response to a SIP request. The response accepts, rejects, or redirects the request. This role lasts only for the duration of that transaction. In other words, if a piece of software responds to a request, it acts as a UAS for the duration of that transaction. If it generates a request later, it assumes the role of a user agent client for the processing of that transaction.” [RFC 3261]

User Roles Common privileges assigned to users or appliances based on need. The following user roles are defined within the Real Time Services (RTS) Information Assurance (IA) architecture:

- System Security Administrator
 - Defines and assigns user privileges.
 - Adds and deletes user identifications (IDs).
 - Disables or enables the use of specific user IDs as login IDs.
 - Initializes and resets login passwords.
 - Initializes and changes cryptographic keys.
 - Sets the system password aging thresholds.
 - Sets the system limit on the number of failed login attempts.
 - Removes a lockout or changes the system lockout timer value.
 - Sets the system’s inactivity timer value.
 - Sets system security logging and alarm configuration.
 - Manages the system security logging processes.
 - Upgrades security software.
 - Terminates any user of system session.

- System Administrator
 - Installs appliance.
 - Defines and assigns new user and group privileges at the operating system level.
 - Maintains a record of all requests for login IDs.
 - Adds and deletes users at the operating system level.
 - Disables the use of specific IDs as login IDs (e.g., bin, sys, etc.).
 - Installs operating system updates and patches.

- Monitors system logs.
- Maintains and monitors access and changes to SUPERUSER password.
- Controls access to SUPERUSER account.
- Manages system logging processes.
- Delegates administration authorizations to specific persons in other roles.
- Terminates any user or system session.

- Application Administrator
 - A role responsible for the proper activation, maintenance, and usage of an application on an appliance. Application administrator tasks include upgrading application software.

- Privileged Application User
 - A user with the capability to originate Routine and above Routine precedence real time service (RTS) sessions

- Application User
 - A user who may execute applications on a system or may originate Routine precedence sessions

V

Video Teleconferencing (VTC) Two-way electronic form of communications that permits two or more people in different locations to engage in face-to-face audio and visual communication. Meetings, seminars, and conferences are conducted as if all the participants are in the same room.

Video Teleconferencing Unit (VTU) VTC endpoint equipment that performs the following functions: coding/decoding of audio and video; multiplexing of video, audio, data, and control signals; system control; and end-to-end signaling. It may include I/O functions, embedded cryptographic functions, network interface functions, end-to-network signaling, and connections to networks.

Section A2 – Glossary and Terminology Description

Virtual Network Element (VT-NE) A VT-NE is any network element integrated into a certified DSN switch. A T-NE can be used for long local, encapsulated time division multiplexing (TDM), and Proprietary Internet Protocol Trunk (PIPTs).

Voice over IP (VoIP) System A set of components required to provide Defense Switched Network (DSN) Internet Protocol (IP) voice services from end instrument to DSN trunk, or IP phone to IP phone. The VoIP system includes, but is not limited to, the IP telephony instrument, the local area network (LAN), the Local Session Controller (LSC), and the IP gateway.

Voiceband Data (Modem Pass-Through) A subset of Modem over IP in which modem signals are transmitted over the voice channel of a packet network.

W

Wide Area Network (WAN) Level Assured Services Admission Control (W-ASAC) The processes on a multifunction softswitch (MFSS) or Assured Real Time Services (ARTS) Softswitch (SS) that ensure that quality of service requirements of a higher precedence service will be met at the expense of a lower precedence service if the WAN conditions do not allow meeting quality of service requirements of all services. The processes are typically associated with the preemption of lower precedence sessions within the WAN to ensure that higher precedence sessions can be completed. In addition, the W-ASAC ensures that its subtended Local Session Controllers (LSCs) remain within their traffic engineered real time service (RTS) allocations.

Wireless Can refer to either 802.x devices or cellular telephones (see UCR 2008, Section 5.3.1.6.2, Operational Changes, for more details).

Wireless Device A 802.x device or cellular phone.

Wireless Access Bridge (WAB) A device that connects two local area network (LAN) segments together via wireless transmission.

Wireless End Instrument (WEI) A Defense Switched Network (DSN) command and control (C2) or non-C2 user device that receives voice service via an IP telephone instrument using wireless technologies, such as 802.11 or 802.16. Also known as a wireless telephony subscriber.

Wireless Local Area Network (LAN) (WLAN) Generic term used to describe the use of wireless technologies in the LAN. The WLAN includes all the wireless terminology (i.e., wireless access bridge (WAB), wireless end instrument (WEI), and Wireless LAN Access System (WLAS)).

Wireless Local Area Network (LAN) Access System (WLAS) An implementation of wireless technologies considered to be the replacement of the physical layer of the wired Access Layer of a LAN.

**SECTION A3
ACRONYMS AND ABBREVIATIONS**

1R	Reamplification
2R	Reamplification and Reshaping
2W	Two Wire
3R	Reamplification, Reshaping, and Retiming
4W	4-Wire
24/7	24-Hours, 7 Days A Week
A/D	Analog/Digital
AAR	Automatic Alternate Routing
ABBT	Automatic Board-to-Board Testing
AC	Admission Control
ACA	Automatic Circuit Assurance
ACAT	Acquisition Category
ACC	Automatic Congestion Control
ACD	Attendant/Call Director
ACD	Automatic Call Distribution
ACD	Automatic Call Distributor
ACG	Automatic Call Gap
ACL	Access Control List
ACM	Address Complete Message
ACMOS	Automatic Customer Measurement Outputting System
ACR	Anonymous Call Rejection
ACTA	Administrative Council for Terminal Attachments
ADIMSS	Advanced DSN Integrated Management Support System
ADM	Add-Drop Multiplexing
ADSI	Analog Display Services Interface
AES	Advanced Encryption Standard
AF	Assured Forwarding
AFR	Automatic Flexible Routing
AG	Access Gateway
AHWG	Ad Hoc Working Group
AIN	Advanced Intelligent Network
AIOD	Automatic Identified Outward Dialing
AIS	Alarm Indication Signal
AIS	Automated Information Systems
AIS-CI	Alarm Indication Signal – Customer Installation
ALI	Automatic Location Identification

FOR OFFICIAL USE ONLY

Appendix A1 – Definitions, Abbreviations and Acronyms, and References

Section A3 – Abbreviations and Acronyms

A-link	Access Link
ALIT	Automatic Line Insulation Test
AMA	Automatic Message Accounting
AMI	Alternate Mark Inversion
AMR	Adaptive Multi-Rate
ANAT	Alternative Network Address Types
AND	Area Distribution Node
ANI	Automatic Number Identification
ANM	Answer Message
ANS	Answer Message
ANSI	American National Standards Institute
AOR	Address of Record
AOR	Area of Responsibility
APL	Approved Products List
APRI	Address Presentation Restricted Indicator
APS	Automatic Protection Switching
AR	Aggregation Router
AR	Automatic Recall
ARD	Automated Receiving Device
ARP	Address Resolution Protocol
ARS	Automatic Route Selection
ARTS	Assured Real Time Services
AS	Assured Services
AS	Autonomous System
ASAC	Assured Service Admission Control
ASCII	American Standard Code for Information Interchange
ASD(NII)	Assistant Secretary of Defense for Networks & Information Integration
ASLAN	Assured Service Local Area Network
ASP	Application Server Process
AS-SIP	Assured Services Session Initiation Protocol
AS-SIP-T	Assured Services Session Initiation Protocol for Telephones
AT	Access Tandem
ATC	Authority to Connect
ATIS	Alliance for Telecommunications Industry Solution
ATM	Asynchronous Transfer Mode
ATO	Authority to Operate
ATP	Acceptance Test Procedure/Plan
ATQA	Attendant Queue Announcement
AUC	Authentication Center
Auth	Authorization

FOR OFFICIAL USE ONLY

Appendix A1 – Definitions, Abbreviations and Acronyms, and References

Section A3 – Abbreviations and Acronyms

AVC	Advanced Video Coding
B/P/C/S	Base/Post/Camp/Station
B2BUA	Back-to-Back User Agent
B3ZS	Bipolar 3 Zero Substitution
B8ZS	Bipolar with Eight-Zero Substitution
BA	Billing Agent
BAF	Bellcore AMA Format
Base	Baseband
BB	Backbone
BBG	Basic Business Group
BC	Bearer Capability
BC	Border Controller
BCC	Bellcore Client Company
BCE	Bridged Call Exclusion
BCI	Backwards Call Indicator
BCLID	Bulk Calling Line Identification
BE	Block Error
BE	Best Effort
BEHAVE	Behavior Engineering for Hindrance Avoidance
BER	Bit Error Rate
BERT	Bit Error Rate Tester
BG	Business Group
BGAC	Business Group Automatic Callback
BGCW	Business Group Call Waiting
BGL	Business Group Line
BGMP	Border Gateway Multicast Protocol
BGP	Border Gateway Protocol
BGP-4	Border Gateway Protocol 4
BICC	Bearer-Independent Call Control
BIP-N	Bit Interleaved Parity-Number
BITS	Building Integrated Timing Supply
BLSR	Bidirectional Line Switched Ring
BNEA	Busy Not Equipped Announcement
BNF	Backus-Naur Form
BOOTP	Bootstrap Protocol
BPA	Blocked Precedence Announcement
BRA	Basic Rate Access
BRAC	Base Realignment and Closure
BRI	Basic Rate Interface
BSC	Base Station Controller
BSS	Base Station Subsystem

FOR OFFICIAL USE ONLY

Appendix A1 – Definitions, Abbreviations and Acronyms, and References

Section A3 – Abbreviations and Acronyms

BTS	Base Transceiver Station
BW	Bandwidth
C&A	Certification and Accreditation
C/P/S	Camp, Post, or Station
C2	Command and Control
C2(R)	C2 User (Originate ROUTINE Only Calls)
C4	Command, Control, Communications, and Computers
C4ISP	C4 Information Support Plan
CA	Certificate Authority
CAA	Configuration Control Authority
CAC	Call Admission Control
CAC	Common Access Card
CAD	Computer-Assisted Dispatch
CALEA	Communications Assistance to Law Enforcement Act
CAMA	Centralized Automatic Message Accounting
CAN	Campus Area Network
CANF	Cancel From
CANT	Cancel To
CAP	Competitive Access Provider
CAROT	Centralized Automatic Reporting On Trunks
CAS	Channel Associated Signaling
CAT	Customer Access Treatment
Cat	Category
CBCS	Common Baseline Circuit Switch
CBWFQ	Class-Bases WFQ
CC/S/A	Combatant Commander/Service/Agency
CCA	Call Connection Agent
CCB	Configuration Control Board
CCC	Clear Channel Capability
CCEP	Commercial COMSEC Evaluation Program
CCI	Controlled Cryptographic Item
CCITT	International Telegraph and Telephone Consultative Committee [now ITU-T]
CCM	Configuration Control and Management
CCMP	Counter with Cipher Block Chaining-Message Authentication Code Protocol
ccs	Hundred Call Seconds
CCS	Common Channel Signaling
CCS7	Common Channel Signaling System No. 7
CCSA	Common Control Switching Arrangement

FOR OFFICIAL USE ONLY

Appendix A1 – Definitions, Abbreviations and Acronyms, and References

Section A3 – Abbreviations and Acronyms

CCSN	Common Channel Signaling Network
CDAR	Customer- Dialed Account Recording
CdPA	Called Party Address
CDR	Call Detail Recording
CDR	Critical Design Review
CE Router	Customer Edge Router
CE	Customer Edge
CE	Customer Edge
CEPT	Commission of European Post and Telecommunication
CES	Circuit Emulation Service
CESoP	Circuit Emulation Service over Packet
CF	Call Forwarding
CFBL	Call Forwarding Busy Line
CFDA	Call Forwarding - Don't Answer
CFI	Canonical Format Indicator
CFV	Call Forwarding Variable
CGA	Carrier Group Alarm
CGAP	Call Gapping
CGB	Circuit Group Blocking Message
CgPA	Calling Party Address
CgPN	Calling Party Number
CHBK	Channel Bank
CI	Customer Installation
CIC	Circuit Identification Code
CID	Calling Identity Delivery
CID	Craft Input Device
CID	Craft Interface Device
CIDCW	Calling Identity on Call Waiting
CIDR	Classless Inter-Domain Routing
CIDS	Calling Identity Delivery and Suppression
CIO	Chief Information Officer
CIR	Committed Information Rate
CJCS	Chairman of the Joint Chiefs of Staff
CJCSI	Chairman of the Joint Chiefs of Staff Instruction
CJCSM	Chairman of the Joint Chiefs of Staff Manual
CLAN	Converged Local Area Network
CLI	Calling Line Identification
CLID	Calling Line Identifier
CM	Configuration Management
CM	Countermeasure
CM	Cryptographic Modernization

FOR OFFICIAL USE ONLY

Appendix A1 – Definitions, Abbreviations and Acronyms, and References

Section A3 – Abbreviations and Acronyms

CMC	Cellular Mobile Carrier
CMI	Cryptographic Modernization Initiative
CN	Core Network
CNAB	Calling Name Delivery Blocking
CNAM	Calling Name Delivery
CND	Calling Number Delivery
CND	Computer Network Defense
CNDB	Calling Number Delivery Blocking
CO	Central Office
COA	Changeover Acknowledgement
COCOM	Combatant Commander
codec	Coder/Decoder
COI	Community of Interest
COMSEC	Communications Security
CONOPS	Concept of Operations
CONUS	Continental United States
COO	Changeover Order
COP WAT	Customer-Owned Premises Wiring Acceptance Test
COPS	Common Open Policy Service
CoS	Class of Service
COT	Continuity Testing
COT	Customer Originated Trace
COTS	Commercial Off-the-Shelf
CPC	Calling Party Category
CPE	Customer Premises Equipment
CPG	Call Progress Message
CPS	Customer Premises System
CPSG	Call Park Subscriber Group
CPT	Cryptographic Products Testing
CPTe	Customer Premises Terminal Equipment
CPU	Central Processing Unit
CQ	Custom Queuing
CR	Customer Router
CRC	Cyclic Redundancy Check
CRD	Capstone Requirements Document
CS	Call Screening
CS	Circuit-Switched
CS	Content Staging
CS/IDM	Content Staging/Information Dissemination Management
CS-ACELP	Conjugate-Structure Algebraic-Code-Excited Linear Prediction
CSeq	Command Sequence

FOR OFFICIAL USE ONLY

Appendix A1 – Definitions, Abbreviations and Acronyms, and References

Section A3 – Abbreviations and Acronyms

CSN	Canadian Switched Network
CSR	Customer Station Rearrangement
CSU	Channel Service Unit
CT	Call Trace
CTI	Computer Telephony Integration
CTL	Certificate Trust List
CUG	Closed User Group
CV	Coding Violations
CVSD	Continuously Variable Slope Delta
CW	Call Waiting
CWD	Call Waiting Deluxe
CWI	Call Waiting Indication
CWT	Call Waiting Terminating
CY	Calendar Year
D/A	Digital/Analog
D4	Fourth Generation Channel Bank
DA	Destination Address
DA	Directory Assistance
DAA	Designated Approval Authority
DAC	Discretionary Access Control
DAD	Duplicate Address Detection
DARTS	DISN Assured Real Time Services
dB	Decibel
DBMS	Database Management System
dc	Direct Current
DCIO	Deputy Chief Information Officer
DCP	Designated Called Party
DCVX	Deployed Cellular Voice Exchange
DDD	Direct Distance Dialing
DES	Data Encryption Standard
DFSU	Dual Frequency Signaling Unit
DHCP	Dynamic Host Configuration Protocol
DIACAP	Defense Information Assurance Certification and Accreditation Process
DICE	DoD Interoperability Communications Exercise
DID	Direct Inward Dialing
DiffServ	Differentiated Services
DISA	Defense Information Systems Agency
DISAC	Defense Information Systems Agency Circular
DISN	Defense Information System Network

FOR OFFICIAL USE ONLY

Appendix A1 – Definitions, Abbreviations and Acronyms, and References

Section A3 – Abbreviations and Acronyms

DISR	DoD Information Technology Standards Registry
DITSCAP	DoD Information Technology Security Certification and Accreditation Process
DIU	Digital Interface Unit
DLC	Digital Loop Carrier
DMS	Defense Message System
DMSC	Deployed Mobile Switching Center
DN	Directory Number
DNS	Domain Name System
DOC	Dynamic Overload Control
DoD	Department of Defense
DOD	Direct-Outward-Dialing
DoDAF	Department of Defense Architecture Framework
DoDD	DoD Directive
DoDI	DoD Instruction
DoS	Denial of Service
DP	Dial Pulse
DPC	Destination Point Code
DRCW	Distinctive Ringing/Call Waiting
DRE	Directional Reservation Equipment
DRSN	Defense RED Switch Network
DS	Data Set
DS	Differentiated Services
DS	Digital Signal
DS0	Digital Signal Level 0
DS1	Digital Signal Level 1
DS3	Digital Signal Level 3
DSAWG	DISN Security Accreditation Working Group
DSCD	DoD Secure Communications Device
DSCP	Differentiated Services Code Point
DSField	Differentiated Services Field
DSN	Defense Switched Network
DSS1	Digital Subscriber Signaling System No. 1
DSU	Digital Service Unit
DTAU	Digital Test Access Unit
DTE	Data Terminal Equipment
DTG	Date Time Group
DTMF	Dual-Tone Multifrequency
DTU	Digital Test Unit
DVMRP	Distance Vector Multicast Routing Protocol
DVS	DISN Video Services

FOR OFFICIAL USE ONLY

Appendix A1 – Definitions, Abbreviations and Acronyms, and References

Section A3 – Abbreviations and Acronyms

DVX	Deployable Voice Exchanges
DVX-C	Deployable Voice Exchange – COTS
DVX-L	Deployable Voice Exchange – Legacy
E&M	Ear and Mouth
E/NM	Enterprise and Network Management
E2E	End-to-End
E911	Enhanced 911
EA	Enterprise Architecture
EA1	Emergency Announcement 1
EA2	Emergency Announcement 2
EADAS	Engineering and Administration Data Acquisition System
EAE0	Equal Access End Office
EAOSS	Exchange Access Operator Services System
EA-TJTN	Executive Agent for Theater Joint Tactical Networks
EAP	Extensible Authentication Protocol
EBC	Edge Boundary Controller
EBER	Excessive Bit Error Rate
EC	Echo Canceller
ECAR-1	Enclave and Computing Environment Audit Record Content-1
ECAR-2	Enclave and Computing Environment Audit Record Content-2
ECAR-3	Enclave and Computing Environment Audit Record Content-3
ECN	Explicit Congestion Notification
ECO	Embedded Operations Channel
ECTP-1	Enclave and Computing Environment Audit Trail Protection-1
ECU	End Cryptographic Unit
EF	Expedited Forwarding
EF	Extended Frame
EF&I	Engineer, Furnish, and Install
EGP	Exterior Gateway Protocol
EI	End Instrument
EIA	Electronics Industries Alliance
EIR	Equipment Identity Register
EIS	Expanded Inband Signaling
EKTS	Electronic Key Telephone System
E-LSP	EXP-Inferred LSP
ELEAF	Expanded Large Effective Area Fiber
EMSS	Enhanced Mobile Satellite Systems
ENUM	Electronic Numbering
EO	End Office
EOC	Embedded Operations Channel

FOR OFFICIAL USE ONLY

Appendix A1 – Definitions, Abbreviations and Acronyms, and References

Section A3 – Abbreviations and Acronyms

EOL	End of Life
EOS	End Office Switch
EPSCS	Enhanced Private Switched Communication Service
ertPS	Extended Real-Time Polling Service
ES	Enterprise Services
ES	Errored Seconds
ESCON	Enterprise Systems Connection
ESF	Extended Superframe
ESN	Extended Sequence Number
ESOP	Enhanced Switch Operation Program
ESP	Encapsulating Security Payload
ESP	Essential Service Protection
ETN	Electronic Tandem Network
ETS	Electronic Tandem Switching
ETSI	European Telecommunications Standards Institute
EUB	End User Building
EVDO	Evolution-Data Optimized
F	FLASH
FA	Forwarding Adjacency
FC	Facility Code
FCAPS	Fault, Configuration, Accounting, Performance, and Security
FCC	Federal Communications Commission
FCI	Forward Call Indicator
FD	Feature Definition
FE	Fast Ethernet
FEAC	Far-End Alarm and Control
FEBE	Far-End Block Error
FEC	Forward Error Correction
FEMF	Foreign Electromotive Force
FEOOF	Far-End Out of Frame
F-F	Fixed-to-Fixed
FFR	Fast Failure Recovery
FICON	Fiber Connectivity
FIPS	Federal Information Processing Standard
FGA	Feature Group A
FGB	Feature Group B
FGC	Feature Group C
FGD	Feature Group D
FGE	Feature Group E
FGF	Feature Group F

FOR OFFICIAL USE ONLY

Appendix A1 – Definitions, Abbreviations and Acronyms, and References

Section A3 – Abbreviations and Acronyms

FIFO	First-In First-Out
FISMA	Federal Information Security Management Act
FISU	Fill-In Signaling Unit
FNPA	Foreign Numbering Plan Area
FO	FLASH OVERRIDE
FOC	Full Operational Capability
FoIP	Fax over Internet Protocol
FOO	FLASH OVERRIDE OVERRIDE
FQDN	Fully Qualified Domain Name
FR	Family of Requirements
FRL	Facility Restriction Level
FSD	Feature Service Description
FSD	Feature Specific Document
FSDP	Fiber Service Delivery Point
FSO	Field Security Office
F-T	Fixed-to-Tactical
FTR	Federal Telecommunications Recommendation
FTS	Federal Technology Service
FTS	Federal Telecommunications Systems
FTP	File Transfer Protocol
FX	Foreign Exchange
FY	Fiscal Year
G3	Group 3
G3 Fax	Group 3 Facsimile
GAO	Government Accounting Office
GBNP	Global Block Numbering Plan
Gbps	Gigabits per Second
GCIRD	Generic Cryptographic Interoperability Requirements Document
GE	Gigabit Ethernet
GETS	Government Emergency Telecommunications System
GIG	Global Information Grid
GLS	Global Location Server
GMPLS	Generalized Multiprotocol Label Switching
GNSC	Global Network Support Center
GOS	Grade of Service
GPS	Global Positioning System
GR	Generic Requirement
GRE	Generic Routing Encapsulation
GRS	Circuit Group Reset Message
GSCR	Generic Switching Center Requirements

FOR OFFICIAL USE ONLY

Appendix A1 – Definitions, Abbreviations and Acronyms, and References

Section A3 – Abbreviations and Acronyms

GSM	See the definition of DSCD
GSR	Generic System Requirement
GSS	Generic System Specification
GSTP	Generic Switching Test Plan
GTT	Global Title Translation
GUI	Graphical User Interface
HAIPE	High Assurance Internet Protocol Encryptor
HDB3	High Density Bipolar 3 Code
HEMP	High-Altitude Electromagnetic Pulse
HEX	Hexadecimal
HLR	Home Location Register
HNPA	Home Numbering Plan Area
H-R	Host Remote (Link)
HTTP	HyperText Transfer Protocol
HTTPS	HyperText Transfer Protocol, Secure
HTR	Hard-To-Reach
Hz	Hertz
I	IMMEDIATE
I&S	Interoperability and Supportability
IA	Information Assurance
IA/CND	Information Assurance/Computer Network Defense
IAA	Information Assurance Accreditation
IAD	Integrated Access Device
IAM	Initial Address Message
IANA	Internet Assigned Numbers Authority
IAO	Information Assurance Officer
IAS	Integrated Access Switch
IASRD	Information Assurance Security Requirements Document
IATO	Interim Authority to Operate
IATP	Information Assurance Test Plan
IATT	Information Assurance Test Team
IATT	Interim Authority to Test
IAVA	Information Assurance Vulnerability Alert
IAW	In Accordance With
ICA	Isolated Code Announcement
IC	Inter-LATA Carrier
IC	Interexchange Carrier
ICE	Interactive Connectivity Establishment
ICMP	Internet Control Message Protocol

FOR OFFICIAL USE ONLY

Appendix A1 – Definitions, Abbreviations and Acronyms, and References

Section A3 – Abbreviations and Acronyms

ICMPv6	Internet Control Message Protocol for IPv6
ICTO	Interim Certification to Operate
ID	Identification
IDDD	International Direct Distance Dialing
IDLC	Integrated Digital Loop Carrier
IDM	Information Dissemination Management
IDR	Inter-Domain Routing
IDS	Integrated Data Services
IDS	Intrusion Detection System
IDT	Integrated Digital Terminal
Ie	Equipment Impairment Factor
IE	Information Element
IEEE	Institute of Electrical and Electronics Engineers, Inc.
IESG	Internet Engineering Steering Group
IETF	Internet Engineering Task Force
IGMP	Internet Group Multicast Protocol
IGMPv3	Internet Group Management Protocol, Version 3
IGP	Interior Gateway Protocol
I-IWU	Incoming Interworking Unit
IKE	Internet Key Exchange
IKEv1	Internet Key Exchange Version 1
IKEv2	Internet Key Exchange Version 2
IM	Instant Messaging
IMASS	Integrated Multiple Access Switched Service
IMUX	Inverse Multiplexer
INC	International Carrier
INE	In-Line Network Encryptor
Intserv	Integrated Services
INWATS	Inward Wide Area Telecommunications Service
I/O	Input/Output
IO	Interoperability
IOC	Initial Operational Capability
IP	Internet Protocol
IPM	Impulses Per Minute
IPSec	Internet Protocol Security
IPSG	Internet Protocol Signaling Gateway
IPT	Integrated Product Team
IPv4	Internet Protocol Version 4
IPv6	Internet Protocol Version 6
IR	Intermediate Reach
IRR	Immediate Reroute

FOR OFFICIAL USE ONLY

Appendix A1 – Definitions, Abbreviations and Acronyms, and References

Section A3 – Abbreviations and Acronyms

IS	Information System
IS	Interoperability Specification
ISAKMP	Internet Security Association and Key Management Protocol
ISDN	Integrated Services Digital Network
IS-IS	Intermediate System-Intermediate System
ISIS	Intermediate System to Intermediate System
ISP	Information Support Plan
IST	Interswitch Trunk
ISUP	ISDN User Part
IT	Information Technology
ITU	International Telecommunications Union
ITU-T	International Telecommunications Union – Telecommunication Standardization Sector
IUA	Integrated Services Digital Network User Adaptation
IVM	Internet Voice Mail
IVR	Interactive Voice Response
IVSN	Initial Voice Switched Network
IWF	Interworking Function
IWU	Interworking Unit
JCIDS	Joint Capabilities Integration and Development System
JCPAT-E	Joint C4I Program Assessment Tool-Empowered
JIC	Joint Interoperability Certification
JITC	Joint Interoperability Test Command
JNO	Joint Net-Centric Operations
JROCM	Joint Requirements Oversight Council Memorandum
JSCMWG	Joint Services Cryptographic Modernization Working Group
JTA	Joint Technical Architecture
JTF	Joint Task Force
JUICE	Joint User Interoperability Communications Exercise
kb/s	Kilobits per second
kbit/s	Kilobits per Second
KEYMAT	Keying Material
kHz	Kilohertz
Km	Kilometer
KMI	Key Management Infrastructure
KPP	Key Performance Parameter
L2	OSI Layer 2

FOR OFFICIAL USE ONLY

Appendix A1 – Definitions, Abbreviations and Acronyms, and References

Section A3 – Abbreviations and Acronyms

L3	OSI Layer 3
LAMA	Local Automatic Message Accounting
LAN	Local Area Network
LATA	Local Access and Transport Area
L-ASAC	LSC Level ASAC
LASD	Local Assured Service Domain
LC	Loop Closure
LCAS	Link Capacity Adjustment Scheme
LDAP	Lightweight Directory Access Protocol
LDIF	LDAP Interchange Format
LDN	Local Directory Number
LDP	Label Distribution Protocol
LDS	Local Digital Switch
LEC	Local Exchange Carrier
LED	Light Emitting Diode
LEF	Link Encryptor Family
LER	Label Edge Router
LFB	Look-Ahead for Busy
LFB	Look Forward Busy
LLS	Local Location Server
L-LSP	Label-Only-Inferred LSP
LNP	Local Number Portability
LO	Loop Open
LOC	Lines of Communications
LOC2	Loss of Command and Control
LOF	Loss of Frame
LOP	Loss of Pointer
LOS	Loss of Signal
LOSS	Loss of Signal Seconds
LR	Long Reach
LSC	Local Session Controller
LSP	Label Switched Path
LSP	Link State PDU
LSR	Label Switched Router
LSR	Label Switching Router
LSSGR	LATA Switching Systems Generic Requirements
LSSU	Link Status Signaling Unit
LU	Line Unit
LUTS	Locked-Up Trunk Scan
M&S	Modeling and Simulation

FOR OFFICIAL USE ONLY

Appendix A1 – Definitions, Abbreviations and Acronyms, and References

Section A3 – Abbreviations and Acronyms

M2PA	MTP2 User Peer-to-Peer Adaptation
M2UA	MTP2 User Adaptation
M3UA	MTP3 User Adaptation
MA	Mission Area
MAC	Media Access Control
MAC	Mission Assurance Capability
MA ICD	Mission Area Initial Capabilities Document
MAN	Metropolitan Area Network
Mbps	Megabits per Second
MCC	Maintenance Control Center
MCEB	Military Communications-Electronics Board
MCN	Main Communication Node
MCS	Mobile Cellular Systems
MDII	Machine-Detected Interoffice Irregularities
MDR	Message Detail Recording
MDT	Mean Downtime
MER	Minimum Essential Requirements
MF	Multi-Frequency
MFS	Multifunction Switch
MFSS	Multifunction Softswitch
MG	Media Gateway
MGC	Media Gateway Controller
MGCP	Media Gateway Control Protocol
MHz	Megahertz
MIB	Management Information Base
MIDCOM	Middlebox Communication
MIME	Multipurpose Internet Mail Extension
MIPv6	Mobile IP Version 6
MIS	Management Information System
MLD	Multicast Listener Discovery
MLDv2	Multicast Listener Discovery Version 2
MLHG	Multiline Hunt Group
MLPP	Multilevel Precedence and Preemption
MLS	Multilevel Security
MLT	Mechanized Loop Test
MMF	Multi Mode Fiber
MOE	Measure of Effectiveness
MoIP	Modem over Internet Protocol
MOS	Mean Opinion Score
MOSFP	Multicast Open Shortest Path First
MP-BGP	Multi-Protocol Border Gateway Protocol

FOR OFFICIAL USE ONLY

Appendix A1 – Definitions, Abbreviations and Acronyms, and References

Section A3 – Abbreviations and Acronyms

MPEG	Motion Picture Experts Group
MPI	Minimum Picture Interval
MPLS	Multiprotocol Label Switching
ms	Microsecond
MS	Multiplex Section
MSAG	Master Street Address Guide
MSDP	Multicast Source Discovery Protocol
msec	Milliseconds
MSL-100	Meridian SL-100
MSO	Mobile Switching Office
MSPP	Multi-Service Provisioning Platforms
MSR	Message Storage and Retrieval System
MSU	Message Signaling Unit
MTBF	Mean Time between Failures
MTBM	Mean Time between Maintenance
MTIE	Maximum Time Interval Error
MTP	Message Transfer Part
MTP1	Message Transfer Part 1
MTP2	Message Transfer Part 2
MTP3	Message Transfer Part 3
MTS	Message Telephone Service
MTTR	Mean Time To Repair
MTU	Maximum Transmission Unit
MU	Message Unit
MUF	Military Unique Features
MVP	Multiline Variety Package
mW	Milliwatt
MWR	Morale, Welfare, and Recreation
NAC	Network Administration Center
NANP	North American Numbering Plan
NAP	Network Access Point
NAPT	Network Address Port Translation
NAT	Network Address Translation
NATO	North Atlantic Treaty Organization
NAVSTAR	Navigation Satellite Timing and Ranging
NC	Network Cluster
NCA	No Circuit Announcement
NCID	Net-Centric Implementation Document
NCM	Network Cluster Member
NCO	Net-Centric Operations

FOR OFFICIAL USE ONLY

Appendix A1 – Definitions, Abbreviations and Acronyms, and References

Section A3 – Abbreviations and Acronyms

NCTAMS	Naval Computer and Telecommunications Area Master Station
NDAA	National Defense Authorization Act
NDC	Network Data Collection
NE	Near End
NE	Network Element
NEMO	Network Mobility
NETOPS	Network Operations
NEXT	Near End Crosstalk
NI	Network Identifier
NI	Network Identity
NI-1	National ISDN 1
NI-2	National ISDN 2
NIAP	National Information Assurance Partnership
NIC	Network Indicator Code
NIC	Network Interface Card
NIPRNet	Non-Secret IP Router Network
NIPRNET	Non-Secure Internet Protocol Router Network
nm	nanometer
NM	Network Management
NMC	Network Management Center
NMCC	National Military Command Center
NMS	Network Management System
NOA	Nature of Address
NOC	Network Operations Center
NORAD	North American Air Defense
NP	Number Portability
NPA	Numbering Plan Area
npdi	Number Portability Database Dip Indicator
NR-KPP	Net-Ready Key Performance Parameter
nrtPS	Non-Real-Time Polling Service
ns	Nanosecond
NSA	National Security Agency
NSE	Network Switching Element
NSLP	Netware Link Services Protocol
NS/EP	National Security Emergency Preparedness
NSS	National Security Systems
NT1	Network Termination 1
NT2	Network Termination 2
NTI	Northern Telecom, Inc.
NTM	Network Traffic Management
NTMOS	Network Traffic Management Operating System

FOR OFFICIAL USE ONLY

Appendix A1 – Definitions, Abbreviations and Acronyms, and References

Section A3 – Abbreviations and Acronyms

NTP	Network Time Protocol
NUTS	Non-Usage Trunk Scan
OADM	Optical Add Drop Multiplexer
OAN	Operational Area Network
OA&M	Operations, Administration, and Maintenance
OC3	Optical Carrier Level 3
OC-3	Optical Carrier Level 3
OCONUS	Outside the Continental United States
OCN	Original Called Number
OCS	Outgoing Call Screening
OEO	Optical-to-Electrical-to-Optical
OIF	Optical Internetworking Forum
OIM	Operations Interface Module
O-IWU	Outgoing Interworking Unit
OLA	Optical Line Amplifiers
O&M	Operations and Maintenance
ONI	Operator Number Identification
OO	Optical-to-Optical
OOF	Out of Frame
OP	Optical Protection
OPC	Originating Point Code
ORR	Overflow Reroute
OS	Operations System
OSA	Optical Spectrum Analyzer
OSC	On-Line Status Check
OSC	Optical Service Channel
OSC	Optical Supervisory Channel
OSD	Office of the Secretary of Defense
OSI	Open Systems Interconnection
OSNR	Optical Signal to Noise Ratio
OSP	Outside Plant
OSPF	Open Shortest Path First
OTAR	Over-The-Air-Rekey
OTGR	Operations Technology Generic Requirements
OTM	Optical Terminal Multiplexer
OTN	Optical Transport Network
OUTWATS	Outward Wide Area Telecommunications Service
P	PRIORITY
P	Provider

FOR OFFICIAL USE ONLY

Appendix A1 – Definitions, Abbreviations and Acronyms, and References

Section A3 – Abbreviations and Acronyms

PAA	Principal Accrediting Authority
PABX	Private Automatic Branch Exchange
PALA	Precedence Access Limitation Announcement
PAM	Pass Along Message
P/AR	Peak-To-Average Ratio
PAT	Precedence Access Threshold
PBAS	Precedence-Based Assured Service
PBNM	Policy-Based Network Management
PBX	Private Branch Exchange
PBX1	Private Branch Exchange 1
PBX2	Private Branch Exchange 2
PC	Personal Computer
PC	Point Code
PCM	Pulse Code Modulation
PCMA	Paired Carrier Multiple Access
PCMU	Power Control Monitoring Unit
PDA	Personal Digital Assistant
PDB	Per-Domain Behavior
PDMA	Provisioning-Driven Memory Administration
PDU	Protocol Data Unit
PE	Provider Edge
PED	Personal Equipment Device
PE-R	Provider Edge Router
PESQ	Perceptual Evaluation of Speech Quality
PFAC	Private Facility Access
PGS	Pair Gain System
PHB	Per Hop Behavior
PHY	Physical
PIC	Primary Inter-LATA Carrier
PIM-SM	Protocol Independent Multicast-Sparse Mode
PIN	Personal Identification Number
PING	Packet Internet Groper
PIPT	Proprietary Internet Protocol Trunk
PKE	Public Key Enabled
PKI	Public Key Infrastructure
PLAM	Public Line Activity Monitoring
PL/CA	Precedence Level/Calling Area
PLCP	Physical Layer Convergence Protocol
PLL	Phase Locked Loop
PM	Performance Monitoring
PM	Program Manager

FOR OFFICIAL USE ONLY

Appendix A1 – Definitions, Abbreviations and Acronyms, and References

Section A3 – Abbreviations and Acronyms

PMD	Polarization Mode Dispersion
PMO	Program Management Office
POP	Point Of Presence
POTS	Plain Old Telephone Service
ppm	Parts Per Million
PPP	Point-to-Point Protocol
pps	Pulses per Second
PPSM	Ports, Protocols, and Services Management
PPSN	Public Packet-Switched Network
PQ	Priority Queuing
PRA	Primary Rate Access
PRE	Protectional Reservation Equipment
PRI	Primary Rate Interface
PSAP	Public Safety Answering Point
PSDS	Public Switched Digital Service
PSQM	Perceptual Speech Quality Measure
PSTN	Public Switch Telephone Network
PTS	Public Telecommunications Service
PTT	Public Telephone and Telegraph
PV	Proprietary VoIP
PVN	Private Virtual Network
QoR	Query on Release
QoS	Quality of Service
R	ROUTINE
RADIUS	Remote Authentication Dial In User Service
RAI	Remote Alarm Indication
RAI-CI	Remote Alarm Indication - Customer Installation
RAO	Revenue Accounting Office
RC	Ring Control
RCD	Route Control Digit
RCF	Remote Call Forwarding
RLC	Release Complete Message
RCMAC	Recent Change Memory Administration Center
RDI	Remote Defect Indication
RDT	Remote Digital Terminal
REL	Release
RES	Resume Message
RFC	Request for Comment
RFI	Remote Failure Indication

FOR OFFICIAL USE ONLY

Appendix A1 – Definitions, Abbreviations and Acronyms, and References

Section A3 – Abbreviations and Acronyms

RGTR	Regenerator
RIB	Routing Information Base
RIP	Routing Management Information
RIPv1	Routing Management Information Version 1
RIPv2	Routing Management Information Version 2
RJ	Registered Jack
RLR	Receive Loudness Rating
RLT	Release Link Trunk
RMON	Remote Monitoring
RMAS	Remote Memory Administration System
RMS	Root Mean Square
ROP	Receive Only Printer
ROTL	Remote Office Test Line
RP	Rendezvous Point
RP	Request-Priority
RPF	Reverse Path Forwarding
RPH	Resource Priority Header
RPOA	Recognized Private Operating Administration
RPR	Resilient Packet Ring
RQGR	Reliability and Quality Generic Requirements
RQSSGR	Reliability and Quality Switching Systems Generic Requirements
RR	Reroute
RSB	Repair Service Bureau
RSC	Reset Circuit Message
RSU	Remote Switching Unit
RSVP	Resource Reservation Protocol
RTCP	Real-Time Control Protocol
RTP	Real Time Protocol
RTP	Release to Pivot
rtPS	Real-Time Polling Service
RTS	Real Time Services
RTS	Routing and Translation Server
RTU	Remote Test Unit
Rx AIS	Receive AIS
S&NM	Systems and Network Management
S&U	Secure and Unsecure
SA	Stand-Alone (Switch)
SA	Security Association
SA	Services Agent
SA	Source Address

FOR OFFICIAL USE ONLY

Appendix A1 – Definitions, Abbreviations and Acronyms, and References

Section A3 – Abbreviations and Acronyms

SAC	Service Access Code
SAC	Session Admission Control
SAD	Security Association Database
SAFI	Sub-Address Family Identifier
SAN	Storage Area Network
SAS	Standalone Switch
SATCOM	Satellite Communications
SBC	Session Border Controller
SBU	Sensitive but Unclassified
SC/A	Signal Converter/Allotter
SCCP	Signaling Connection Control Protocol
SCCP	Signaling Connection Control Part
SCCS	Switching Control Center System
SCF	Selective Call Forwarding
SCIP	Secure Communications Interoperability Protocol
SCOF	Selective Control of Facilities
SCN	Switched Circuit Network
SCP	Service Control Point
SCR	Selective Call Rejection
SCS	Session Control and Signaling
SCSF	Session Control and Signaling Function
SCTP	Stream Control Transmission Protocol
SD	Signal Degrade
SDES	Session Descriptions
SDH	Synchronous Digital Hierarchy
SDN	Service Delivery Node
SDP	Session Description Protocol
SDTI	SONET Digital Trunk Interface
SEF	Severely Errored Frame
SEFS	Severely Errored Framing Seconds
SMU	Switch Multiplex Unit
SEF	Severely Errored Framing
SEFS	Severely Errored Framing Seconds
SEI	Secure End Instrument
SEP	Signaling End Point
SES	Severely Errored Seconds
SES	Service Evaluation System
SF	Signal Fail
Sf	Superframe
SFD	Start Frame Delimiter
SFG	Simulated Facilities Group

FOR OFFICIAL USE ONLY

Appendix A1 – Definitions, Abbreviations and Acronyms, and References

Section A3 – Abbreviations and Acronyms

SG	Signaling Gateway
SI	Service Indicator
SIB	Status Indication Busy
SIGTRAN	Signaling Transport
SILC	Selective Incoming Load Control
SIO	Status Indication Out-of Alignment
SIP	Session Initiation Protocol
SIPO	Signal Units Indicating Processor Outage
SIPRNet	Secret Internet Protocol Router Network
SIPRNET	SECRET Internet Protocol Router Network
SIPS	Session Initiation Protocol Secure
SIP-T	Session Initiation Protocol for Telephones
SIP-T(AS)	SIP-T (Assured Service)
SIPv2	Session Initiation Protocol, Version 2
SIT	Special Information Tone
SLA	Service Level Agreement
SLACC	Stateless Address Auto-Configuration
SLC	Signal Link Code
SLC	Service Level Commitment
SLR	Send Loudness Rating
SLS	Service Level Specification
SLS	Signaling Link Selection
SLT	Signaling-Link Test
SLTE	Signaling Link Terminal Equipment
SLU	Subscriber Line Usage
SMC	SONET Minimum Clock
SMDF	Subscriber Main Distributing Frame
SMDI	Simplified Message Desk Interface
SMDR	Station Message Detail Recording
SMEO	Small End Office
SMF	Single Mode Fiber
SMU	Switch Multiplexing Unit
SNAP	System/Network Approval Process
SNCP	Subnetwork Connection Protection
S-NE	Strategic Network Element
SNMP	Simple Network Management Protocol
SNMPv1	Simple Network Management Protocol, Version 1
SNMPv2	Simple Network Management Protocol, Version 2
SNMPv3	Simple Network Management Protocol Version 3
SNR	Signal to Noise Ratio
SOC	Service Observing Circuit

FOR OFFICIAL USE ONLY

Appendix A1 – Definitions, Abbreviations and Acronyms, and References

Section A3 – Abbreviations and Acronyms

SONET	Synchronous Optical Network
SPC	Signal Point Code
SPCS	Stored Program Control System
SPD	Security Policy Database
SPF	Shortest Path First
SPI	Security Parameter Index
SPID	Service Provider Identifier
SpoA	Service Point of Attachment
SPRING	Shared Protection Ring
SPRM	Supplemental Performance Report Message
SQL	Structured Query Language
SR	Selective Router
SR	Short Reach
SRTCP	Secure Real-Time Transport Control Protocol
S RTP	Secure Real-Time Transport Protocol
SS	Softswitch
SS7	Signaling System No. 7
SSA	Subsystem-Allowed
SSAA	System Security Authorization Agreement
SSH	Secure Shell
SSHv2	Secure Shell Version 2
SSM	Single System Manager
SSM	Source-Specific Multicast
SSM	Synchronization Status Message
SSMF	Standard Single Mode Fiber
SSN	Subsystem Number
SSP	Service Switching Point
SSP	Subsystem-Prohibited
SSS	Single Shelter Switch
SST	Subsystem Status Test
ST	Signaling Terminal
STANAG	Standard NATO Agreement
STE	Secure Terminal Equipment
STEP	Standardized Tactical Entry Point
STIG	Security Technical Implementation Guide
STM	Synchronous Transport Module
STP	Signaling Transfer Point
STRATCOM	United States Strategic Command
STS	Synchronous Transport Signal
STU	Secure Telephone Unit
STU	Secure Terminal Unit

FOR OFFICIAL USE ONLY

Appendix A1 – Definitions, Abbreviations and Acronyms, and References

Section A3 – Abbreviations and Acronyms

STU-III	Secure Telephone Unit, Third Generation
STUN	Simple Tunneling of UDP through NAT
SU	Signal Unit
SUA	SCCP User Adaptation
SUS	Suspend Message
SUT	System Under Test
SW64	Switched 64 kbps
SysLog	System Log
T	Ethernet Half-Duplex
T&S	Timing and Synchronization
TA	Terminal Adapter
TAU	Test Access Unit
TC	Tandem Completing
TCA	Threshold Crossing Alert
TCA	Traffic Conditioning Agreement
TCAP	Transaction Capabilities Application Part
TCC	Telephony Country Code
TCI	Tag Control Information
TCLt	Temporarily Weighted Terminal Coupling Loss
TCLw	Weighted Terminal Coupling Loss
TCM	Traveling Class Mark
TCP	Transmission Control Protocol
TDD	Telecommunications Devices for the Deaf
TDEA	Triple Data Encryption Algorithm
TDM	Time Division Multiplexing
TDMA	Time Division Multiple Access
TDM/P	Time Division Multiplexing/Packetized
TDR	Time Domain Reflectometry
TE	Terminal Equipment
TE	Traffic Engineering
TFC	Transfer Control
TFP	Transfer Prohibited
TFR	Transfer Restricted
TG	Trunk Gateway
TG	Trunk Group
THSDN	Tactical High Speed Digital Network
TIA	Telecommunications Industry Association
TID	Trunk ID
TIPHON	Telecommunications and Internet Protocol Harmonization over Networks

FOR OFFICIAL USE ONLY

Appendix A1 – Definitions, Abbreviations and Acronyms, and References

Section A3 – Abbreviations and Acronyms

TISP	Tailored Information Support Plan
TJTN	Theater Joint Tactical Networks
TJTNCCB	Theater Joint Tactical Networks Configuration Control Board
TLP	Transmission Level Point
TLS	Transport Layer Security
TLV	Type-Length-Value
TLWS	Trunk and Line Workstation
TM	Technical Manual
TNC	Theater Network Operations Center
T-NE	Tactical Network Element
ToIP	Text over IP
TOC	Tactical Operations Center
ToS	Type of Service
TOS	Trunk Out of Service
TPID	Tag Protocol Identification
TpoA	Transport Point of Attachment
TR	Technical Reference
TRD	Timed Release Disconnect
TRE	Trunk Reservation
TRI-TAC	Tri-Service Tactical Communications
TS	Tandem Switch
TSA	Time Slot Assignment
TSC	Test System Controller
TSGR	Transport Systems Generic Requirements
TSI	Time Slot Interchange
TSP	Tandem Switching Provider
TSRD	Telecommunications Security Requirements Document
TSSI	Telecom Switched Services Interoperability
T-T	Tactical-to-Tactical
TTA	Telecommunication Technology Association
TTC	Telecommunication Technology Committee
TTL	Time to Live
TTL	Transistor to Transistor Logic
TTY	Teletypewriter
TURN	Traversal Using Relay NAT
TW	True Wave
TWC	Three-Way Calling
TX	Ethernet Full-Duplex
UA	User Agent
UAC	User Agent Client

FOR OFFICIAL USE ONLY

Appendix A1 – Definitions, Abbreviations and Acronyms, and References

Section A3 – Abbreviations and Acronyms

U-AR	Unclassified Aggregation Router
UAS	Unavailable Seconds
UAS	User Agent Server
UAV	Unmanned Aerial Vehicle
UC	Unified Capabilities
UCCO	Unified Capabilities Connection Office
UCR	Unified Capabilities Requirements
UCR 2007	Unified Capabilities Requirements 2007
UCR 2008	Unified Capabilities Requirements 2008
UDP	User Datagram Protocol
UDT	Unitdata
UDTS	Unitdata Service
UFS	User Features and Services
UGS	Unsolicited Grant Service
UI	Unit Interval
UIpp	Unit Interval Peak-to-Peak
UIrms	Unit Interval Root Mean Square
ULCS	Unit Level Circuit Switch
UN	Uniform Numbering
UNI	User Network Interface
UPA	Unauthorized Precedence Announcement
UPS	Uninterruptible Power Supply
UPSR	Unidirectional Path Switched Ring
UPU	User Part Unavailability
URI	Uniform Resource Identifier
URL	Uniform Resource Location
USF	User Service and Feature
USI	User Service Information
USM	User-Based Security Model
USTWC	Usage-Sensitive Three-Way Calling
UTC	Universal Time Coordinated
UTP	Unshielded Twisted Pair
VC	Virtual Circuit
VCA	Vacant Code Announcement
VCAT	Virtual Concatenation
VDT	Video Display Terminal
VF	Voice Frequency
VID	VLAN Identification
VLAN	Virtual Local Area Network
VLR	Visitor Location Register
VMWI	Visual Message Waiting Indicator

FOR OFFICIAL USE ONLY

Appendix A1 – Definitions, Abbreviations and Acronyms, and References

Section A3 – Abbreviations and Acronyms

V _o ATM	Voice over Asynchronous Transfer Mode
V _o IP	Voice over Internet Protocol
VOP	Voice Over Packet
V _o SIP	Voice over Session Initiation Protocol
VPIM	Voice Profile for Internet Mail
VPN	Virtual Private Network
VRRP	Virtual Router Redundancy Protocol
VSC	Vertical Service Code
VSR	Very Short Reach
VSU	Video Switch Unit
VT	Virtual Tributary
VToA	Voice Telephony over ATM
VTC	Video Teleconferencing
VT-NE	Virtual Tactical Network Element
VVoIP	Voice and Video over Internet Protocol
WAB	Wireless Access Bridge
WAN	Wide Area Network
W-ASAC	WAN Level ASAC
WATS	Wide Area Telecommunications Service
WDCS	Wideband Digital Cross-connect System
WEI	Wireless End Instrument
WFQ	Weighted Fair Queuing
WG	Working Group
WIDS	Wireless Intrusion Detection System
WLAN	Wireless Local Area Network
WLAS	Wireless LAN Access System
WLT	Wireline Terminal
WPA	Wi-Fi Protected Access
WPAN	Wireless Personal Area Network
WPS	Wireless Priority Service
WTR	Wait to Restore
WWNDP	World Wide Numbering and Dialing Plan
XUDT	Extended Unitdata
XUDTS	Extended Unitdata Service

THIS PAGE INTENTIONALLY LEFT BLANK

**SECTION A4
REFERENCES**

A4.1 AMERICAN NATIONAL STANDARDS INSTITUTE

American National Standard Institute (ANSI), “Operations, Administration, Maintenance, and Provisioning Security Requirements for Public Telecommunications Network: A Baseline of Security Requirements for the Management Plane,” T1M1.5/2003-007R4, Draft Proposed April 1, 2003.

- ANSI T1.102-1993 *Digital Hierarchy – Electrical Interfaces*, December 1993.
- ANSI T1.105-2001 *Synchronous Optical Network (SONET) – Basic Description including Multiplex Structure, Rates, and Formats*, May 2001.
- ANSI T1.107-2002 *Digital Hierarchy – Formats Specifications*, 2002.
- ANSI T1.111 *Signaling System Number 7 (SS7) – Message Transfer Part (MTP)*, 2001.
- ANSI T1.112 *Signaling System Number 7 (SS7) – Signaling Connection Control Part (SCCP)*, 2001.
- ANSI T1.113 *Signaling System No. 7 (SS7) – Integrated Services Digital Network (ISDN) User Part*, 1995.
- ANSI T1.113-2000 *Signaling System No. 7 (SS7) – Integrated Services Digital Network (ISDN) User Part* (Revision of T1.113-1995; includes two Supplements: T1.113a-2000 and T1.113b-2001).
- ANSI T1.113.3 *Signaling System No. 7 (SS7) – Signaling Link*.
- ANSI T1.114 *Signaling System Number 7 (SS7) – Transaction Capabilities and Application Part (TCAP)*, 2000.
- ANSI T1.601-1999 *ISDN Basic Access Interface for Use on Metallic Loops for Application at the Network Side of NT, Layer 1 Specification*.
- ANSI T1.607-1998 *ISDN Layer 3 Signaling Specifications for Circuit Switched Bearer Service for Digital Subscriber Signaling System No.1 (DSS1)*.

FOR OFFICIAL USE ONLY

Appendix A1 – Definitions, Abbreviations and Acronyms, and References

Section A4 – References

- ANSI T1.605-1991 (1999) *ISDN Basic Access Interface for S and T Reference Points and Layer 1 Specification.*
- ANSI T1.613-1992 *ISDN Call Waiting Supplementary Service.*
- ANSI T1.616-1992 *ISDN Call Hold Supplementary Service.*
- ANSI T1.619-1992 (R2005) *Integrated Services Digital Network (ISDN) – Multi-Level Precedence and Preemption (MLPP) Service Capability, February 1992, Reaffirmed 2005.*
- ANSI T1.619a-1994 (R1999) *Integrated Services Digital Network (ISDN) – Multi-Level Precedence and Preemption (MLPP) Service Capability (MLPP Service Domain and Cause Changes), July 1994, Reaffirmed 1999.*
- 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.*
- ANSI T1.679-2004 *Interworking Between Session Initiation Protocol (SIP) and Bearer Independent Call Control or ISDN User Part, June 2004.*
- ANSI/TIA-810-B *Telecommunications – Telephone Terminal Equipment – Transmission Requirements for Narrowband Voice over IP and Voice over PCM Digital Wireline Telephones, SP-3-4352-RV2 (to become ANSI/TIA-810-B).*

A4.2 CHAIRMAN OF THE JOINT CHIEFS OF STAFF DOCUMENTS

- CJCSI 6211.02C “Defense Information Systems Network (DISN) Policy and Responsibilities,” 9 July 2008.
- CJCSI 6212.01D “Interoperability and Supportability of Information Technology and National Security Systems,” 8 March 2006, Current as of 14 March 2007.

- CJCSI 6215.01B “Policy for Department of Defense Voice Networks,” 23 September 2001, Directive current as of 13 October 2005, 23 September 2001.
- CJCSI 6215.01C “Policy for Department of Defense (DoD) Voice Networks with Real Time Services (RTS),” 9 November 2007.
- CJCSI 6215.02A “Policy, Responsibilities, Processes, and Administration for the Department of Defense Global Information Grid Networks,” 31 July 2004.
- CJCSI 6510.01E “Information Assurance (IA) and Computer Network Defense (CND),” 15 June 2004.
- CJCSM 6510.01 “Defense in Depth: Information Assurance (IA) and Computer Network Defense (CND),” 25 March 2003, Change 1, 10 August 2004, and Change 2, 26 January 2006.

A4.3 DEFENSE INFORMATION SYSTEMS AGENCY

Defense Information Systems Agency “Global Information Grid (GIG) Convergence Master Plan,” Version 5.25b, 29 March 2006.

Defense Information Systems Agency, “Defense Information Systems Network (DISN), Department of Defense Voice Networks Generic Switching Center Requirements (GSCR),” 8 September 2003, Errata Change 2, 14 December 2006, Revised 27 March 2007.

Defense Information Systems Agency, “Defense Switched Network (DSN) Generic Switching Center Requirements (GSCR),” Change 2, September 2007.

Defense Information Systems Agency, “Department of Defense Voice Networks Generic Switching Center Requirements (GSCR),” 8 September 2003, ERRATA Change 2, 14 December 2006, Revised 27 March 2007.

Defense Information Systems Agency, “Department of Defense Voice Networks Generic Switching Center Requirements (GSCR),” 8 September 2003, with change 1 dated 1 March 2005.

Defense Information Systems Agency, “DISN Real Time Services Generic System Requirements,” Draft, 28 February 2007.

FOR OFFICIAL USE ONLY

Appendix A1 – Definitions, Abbreviations and Acronyms, and References

Section A4 – References

Defense Information Systems Agency, “DISN Real Time Services Generic System Requirements,” Appendix B, “Assured Real Time Services (ARTS) Generic System Requirements (GSR),” Draft, 28 February 2007.

Defense Information Systems Agency, “DISN Real Time Services Generic System Requirements,” Appendix D, “Real-Time Services (RTS) Information Assurance (IA) Generic System Requirements (GSR),” Draft, 28 February 2007.

Defense Information Systems Agency, “GSCR Appendix 3, DSN VoIP Services Requirements: Phase 1,” NS533, 18 December 2003. ERRATA Change 2, 14 Dec 2006, Revised 27 March 2007.

Defense Information Systems Agency, DISAC 300-115-7, “Communications Security: Defense Red Switch Network (DRSN) Security Guidance,” 19 February 2002.

Defense Information Systems Agency, DISAC 310-255-1, “DSN Worldwide Numbering and Dialing Plan.”

DISA Field Security Operations, “DoD Secure Telecommunications and Defense Red Switch Network Security Technical Implementation Guide,” Version 1, Release 1, 28 March 2006.

DISA Field Security Operations, “DoD Telecommunications and Defense Switched Network Security Technical Implementation Guide,” Version 2, Release 2, 30 June 2005.

DISA Field Security Operations, “Network Infrastructure Security Technical Implementation Guide,” Version 6, Release 4, 16 December 2005.

DISA Field Security Operations, “Voice over Internet Protocol (VoIP) Security Technical Implementation Guide,” Version 2, Release 1, 29 August 2005.

A4.3 DEPARTMENT OF DEFENSE DOCUMENTS

“Department of Defense (DoD) Class 3 Public Key Infrastructure (PKI) Public Key-Enabled Application Requirements,” Version 1.0, 13 July 2000.

DoD CIO, “Department of Defense Global Information Grid Architectural Vision: Vision for a Net-Centric, Service-Oriented DoD Enterprise,” Version 1, June 2007.

“Department of Defense Joint Technical Architecture (JTA),” Version 6.0, 3 October 2003.

“DoD Architecture Framework Version 1.0,” February 8, 2004.

“The Global Information Grid (GIG) Net-Centric Implementation Document (NCID) V2.0: T300, Quality of Service,” December 2005.

Center for DISN Services, “DISN Service Level Agreement for the Defense Information Systems Agency and its customers.”

Common Criteria Evaluation and Validation Scheme, 6 August 2004.

Department of Defense Assured Service Session Initiation Protocol (AS-SIP) Generic System Requirement (GSR), Defense Information Systems Agency, Version 1.2.1, 12 May 2006.

Department of Defense Real Time Services (RTS) Information Assurance (IA) Generic System Requirement (GSR), Defense Information Systems Agency, Revision 1.4, 8 September 2006.

Department of Defense Real-Time Services (RTS) Generic System Requirements (GSR) and Generic System Specifications (GSS) Appendices Overview, Revision 0.2, 16 August 2006.

Department of Defense Voice Networks Generic Switching Center Requirements (GSCR), 8 September 2003, ERATA Change 1, 1 March 2005.

Department of Defense Wide Area Network (WAN) Generic System Requirement (GSR), Defense Information Systems Agency, Revision 1.3, 18 May 2006.

Deputy Assistant Secretary of Defense (Deputy CIO), “DSN Generic Switching Center Specification (GSCR),” signed by the Deputy Assistant Secretary of Defense (Deputy CIO), September 8, 2003.

Deputy Secretary of Defense, “Smart Card Adoption and Implementation,” 10 November 1999.

DoD 8910.1-M, “DoD Procedures for Management of Information Requirements,” 30 June 1998.

“DoD Architecture Framework,” Version 1.0, 8 February 2004.

DoD CIO Memorandum, “Internet Protocol Version 6 (IPv6) Interim Transition Guidance,” 29 September 2003.

DoD CIO Memorandum, “Internet Protocol Version 6 (IPv6),” 9 June 2003.

FOR OFFICIAL USE ONLY

Appendix A1 – Definitions, Abbreviations and Acronyms, and References

Section A4 – References

DoD Information Technology Standards Registry (DISR) IPv6 Standards Technical Working Group (TWG), “DoD IPv6 Standard Profiles for IPv6 Capable Products,” Version 1.0, 1 June 2006.

DoD Real Time Services Working Group, “DoD RTS IA Countermeasures,” 29 March 2006.

DoD RTS IA Working Group, “Analysis of Information Assurance Requirements and Threats for the DoD Real-Time Services Environment Version 3.4,” 23 May 2006.

“DoD Voice Networks Generic Switching Center Requirements (GSCR),” 8 September 2003, Errata Change 1, 1 March 2005.

DSN Systems Design, Implementation, and Transition Branch, “Defense Switched Network (DSN) IPv6 Transition Plan,” Version 1.1, 28 June 2006.

Interim Department of Defense (DoD) Certification and Accreditation (C&A) Process Guidance, “DoD Information Assurance Certification and Accreditation Process (DIACAP),” July 6, 2006.

Office of DoD CIO, “DoD Internet Protocol Version 6 (IPv6) Transition Plan,” Version 1.0, November 2003.

United States Strategic Command (STRATCOM), “Joint Concept of Operations for Global Information Grid Network Operations (NetOps),” 20 April 2004.

Director of Central Intelligence Directive (DCID) 6/3, “Protecting Sensitive Compartmented Information within Information Systems,” 5 June 1999.

A4.4 DOD DIRECTIVES

DoDD 4630.05 “Interoperability and Supportability of Information Technology (IT) and National Security Systems (NSS),” 11 January 2002, Certified current as of 23 April 2007.

DoDD 5000.01 “The Defense Acquisition System,” 12 May 2003, Certified current as of 20 November 2007.

DoDD 5200.28 “Security Requirements for Automated Information Systems (AISs),” 21 March 1988.

DoDD 8100.1 “Global Information Grid (GIG) Overarching Policy,” 19 September 2002, Certified Current 21 November 2003.

- DoDD 8100.3 “DoD Voice Networks,” 16 January 2004.
- DoDD 8115.01 “Information Technology Portfolio Management,” 10 October 2005.
- DoDD 8500.01E “Information Assurance (IA),” 23 April 2007.
- DoDD 8530.1 “Computer Network Defense,” 8 January 2001.

A4.5 DOD INSTRUCTIONS

- DoDI 4630.8 “Procedures for Interoperability and Supportability of Information Technology (IT) and National Security Systems (NSS),” 30 June 2004.
- DoDI 5200.40 “DoD Information Technology Security Certification and Accreditation Process (DITSCAP),” 30 December 1997.
- DoDI 8100.3 “Department of Defense (DoD) Voice Networks,” 16 January 2004.
- DoDI 8500.2 “Information Assurance (IA) Implementation,” 6 February 2003.
- DoDI 8510.01 “DoD Information Assurance Certification and Accreditation Process (DIACAP),” 28 November 2007.
- DoDI 8551.1 “Ports, Protocols, and Services Management (PPSM),” 13 August 2004.

A4.6 ETSI DOCUMENTS

- TS 102 165-1 “Telecommunications and Internet Converged Services and Protocols for Advanced Networking (TISPAN) – Methods and protocols; Part 1: Method and proforma for Threat, Risk, Vulnerability Analysis,” Version 4.2.1, December 2006.
- TS 102 165-2 “Telecommunications and Internet Protocol Harmonization over Networks (TIPHON) Release 4; Protocol Framework Definition; Methods and Protocols for Security; Part 2: Counter Measures,” Version 4.1.1, February 2003.

A4.7 FEDERAL INFORMATION PROCESSING STANDARDS PUBLICATIONS

- FIPS PUB 140-2 U.S. Department of Commerce/National Institute of Standards and Technology, “Security Requirements for Cryptographic Modules,” 25 May 2001.
- FIPS PUB 186-2 U.S. Department of Commerce/National Institute of Standards and Technology, “Digital Signature Standard (DSS),” 27 January 2000.
- FIPS 197 Federal Information Processing Standards Publication 197, “Advanced Encryption Standard (AES),” 26 November 2001.

A4.8 INSTITUTE OF ELECTRICAL AND ELECTRONICS ENGINEERS, INC.

- IEEE 743 IEEE Standard for Standard Methods and Equipment for Measuring the Transmission Characteristics of Analog Voice Frequency Circuits, 1984.
- IEEE 802.1D™-2004 IEEE Standard for Local and Metropolitan Area Networks: Media Access Control (MAC) Bridges, June 2004.
- IEEE 802.1Q™-2003 IEEE Standards for Local and Metropolitan Area Networks: Virtual Bridged Local Area Networks, 2003.
- IEEE 802.1s IEEE Standard for Local and Metropolitan Area Networks: Multiple Spanning Trees, 2003. (Merged into 802.1Q-2003).
- IEEE 802.1w IEEE Standard for Local and Metropolitan Area Networks: Rapid Reconfiguration of Spanning Tree, 2003. (Merged into 802.1D-2004).
- IEEE 802.1X™-2001 IEEE Standard for Local and Metropolitan Area Networks: Port Based Network Access Control, 2001.
- IEEE 802.3™-2005 IEEE Standard for information technology—Telecommunications and information exchange between systems—Local and metropolitan area networks—Part 3: Carrier sense multiple access with collision detection (CSMA/CD) access method and physical layer specifications, December 2005.

-
- IEEE 802.3i IEEE Standard for information technology—Telecommunications and information exchange between systems—Local and metropolitan area networks—Part 3: Carrier sense multiple access with collision detection (CSMA/CD) access method and physical layer specifications: 10BASE-T 10 Mbit/s (1.25 MB/s) over twisted pair, 1990.
- IEEE 802.3u-1995 IEEE Standard for information technology—Telecommunications and information exchange between systems—Local and metropolitan area networks—Part 3: Carrier sense multiple access with collision detection (CSMA/CD) access method and physical layer specifications: 100BASE-TX, 100BASE-T4, 100BASE-FX Fast Ethernet at 100 Mbit/s (12.5 MB/s) w/autonegotiation, 1995.
- IEEE 802.3x-1997 IEEE Standard for information technology—Telecommunications and information exchange between systems—Local and metropolitan area networks—Part 3: Carrier sense multiple access with collision detection (CSMA/CD) access method and physical layer specifications: Full Duplex and flow control, 1997.
- IEEE 802.3z-1998 IEEE Standard for information technology—Telecommunications and information exchange between systems—Local and metropolitan area networks—Part 3: Carrier sense multiple access with collision detection (CSMA/CD) access method and physical layer specifications: 1000BASE-X Gbit/s Ethernet over Fiber-Optic at 1 Gbit/s (125 MB/s), 1998.
- IEEE 802.3ab-1999 IEEE Standard for information technology—Telecommunications and information exchange between systems—Local and metropolitan area networks—Part 3: Carrier sense multiple access with collision detection (CSMA/CD) access method and physical layer specifications: 1000BASE-T Gbit/s Ethernet over twisted pair at 1 Gbit/s (125 MB/s), 1999.
- IEEE 802.3ad-2000 IEEE Standard for information technology—Telecommunications and information exchange between systems—Local and metropolitan area networks—Part 3: Carrier sense multiple access with collision detection (CSMA/CD) access method and physical layer specifications: Link aggregation for parallel links, 2000.

FOR OFFICIAL USE ONLY

Appendix A1 – Definitions, Abbreviations and Acronyms, and References

Section A4 – References

- IEEE 802.3ae-2003 IEEE Standard for information technology—Telecommunications and information exchange between systems—Local and metropolitan area networks—Part 3: Carrier sense multiple access with collision detection (CSMA/CD) access method and physical layer specifications: 10 Gbit/s (1,250 MB/s) Ether over fiber; 10GBASE-SR, 10GBASE-LR, 10GBASE-ER, 10GBASE-SW, 10GBASE-LW, 10GBASE-EW, 2003.
- IEEE 802.11™-2007 IEEE Standard for Information technology—Telecommunications and information exchange between systems—Local and metropolitan area networks—Specific requirements—Part 11: Wireless LAN Medium Access Control (MAC) and Physical Layer (PHY) Specifications, June 2007.
- IEEE 802.11a Supplement to IEEE Standard for Information technology—Telecommunications and information exchange between systems—Local and metropolitan area networks—Specific requirements—Part 11: Wireless LAN Medium Access Control (MAC) and Physical Layer (PHY) specifications: High-speed Physical Layer in the 5 GHz Band, June 2003.
- IEEE 802.11b Supplement to IEEE Standard for Information technology—Telecommunications and information exchange between systems—Local and metropolitan area networks—Specific requirements—Part 11: Wireless LAN Medium Access Control (MAC) and Physical Layer (PHY) specifications: Higher-Speed Physical Layer Extension in the 2.4 GHz Band, June 2003.
- IEEE 802.11e Supplement to IEEE Standard for Information technology—Telecommunications and information exchange between systems—Local and metropolitan area networks—Specific requirements—Part 11: Wireless LAN Medium Access Control (MAC) and Physical Layer (PHY) specifications: Wireless LAN for Quality of Service, June 2003.
- IEEE 802.11g Supplement to IEEE Standard for Information technology—Telecommunications and information exchange between systems—Local and metropolitan area networks—Specific requirements—Part 11: Wireless LAN Medium Access Control (MAC) and Physical Layer (PHY) specifications: Amendment 4: Further Higher Data Rate Extension in the 2.4 GHz Band, June 2003.

- IEEE 802.16TM-2004 IEEE Standard for Local and metropolitan area networks—Part 16: Air Interface for Fixed Broadband Wireless Access Systems, 1 October 2004.
- IEEE 802.16eTM IEEE Standard for Local and metropolitan area networks— 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, 28 February 2006.

A4.9 INTERNATIONAL TELECOMMUNICATION UNION

- E.164 ITU-T Recommendation E.164, “The International Public Telecommunication Numbering Plan,” Geneva, Switzerland, 2005.
- E.721 ITU-T Recommendation E.721, “Network grade of service parameters and target values for circuit-switched services in the evolving ISDN,” Geneva, Switzerland, May 1999.
- G.165 ITU-T Recommendation G.165, “Echo cancellers,” Geneva, Switzerland, November 1988.
- G.168 ITU-T Recommendation G.168, “Digital network echo cancellers,” Geneva, Switzerland, January 2007.
- G.703 ITU-T Recommendation G.703, “Physical/Electrical Characteristics of Hierarchical Digital Interfaces at 1544, 2048, 8448, and 44736 kbit/s Hierarchical Levels,” 2001.
- G.704 ITU-T Recommendation G.704, “Series G: Transmission Systems and Media, Digital Systems and Networks—Digital transmission systems – Terminal equipments – General Synchronous frame structures used at 1544, 6312, 2048, 8448 and 44 736 kbit/s hierarchical levels,” October 1998.
- G.711 ITU-T Recommendation G.711, “General Aspects of Digital Transmission Systems, Terminal Equipments, Pulse code modulation (PCM) of voice frequencies,” Geneva, Switzerland, November 1988.

Appendix I, “A high quality low complexity algorithm for packet loss concealment with G.711,” Geneva, Switzerland, September 1999.

FOR OFFICIAL USE ONLY

Appendix A1 – Definitions, Abbreviations and Acronyms, and References

Section A4 – References

Appendix II, “A comfort noise payload definition for ITU-T G.711 use in packet-based multimedia communication systems,” Geneva, Switzerland, February 2000.

G.722 ITU-T Recommendation G.722, “7 kHz audio-coding within 64 kbit/s,” Geneva, Switzerland, November 1988.

G.723.1 ITU-T Recommendation G.723.1, “Dual rate speech coder for multimedia communications transmitting at 5.3 and 6.3 kbit/s,” Geneva, Switzerland, May 2006.

G.726 ITU-T Recommendation G.726, “32 kbps Adaptive Differential Pulse Code Modulation (ADPCM),” Geneva, Switzerland, December 1990.

G.728 ITU-T Recommendation G.728, “Coding of speech at 16 kbit/s using low-delay code excited linear prediction,” Geneva, Switzerland, September 1992.

G.729 ITU-T Recommendation G.729, “Coding of speech at 8 kbit/s conjugate-structure algebraic-code-excited linear prediction (CS-ACELP),” Geneva, Switzerland, March 1996, plus Erratum 1, April 2006, and Annexes A through J, and Appendices I, II, and III.

G.729.1 ITU Recommendation G.729.1 (2006) Amendment 1, “New Annex A on G.729.1 usage in H.245, plus corrections to the main body and updated test vectors,” Geneva, Switzerland, January 2007.

This corrigendum was never published, its content having been included in the published ITU-T Recommendation G.729.1 (2006)

G.729.1 ITU Recommendation G.729.1 (2006), “G.729 based Embedded Variable bit-rate codor: An 8-32 kbit/s scalable wideband coder bitstream interoperable with G.729,” Geneva, Switzerland, May 2006.

This edition includes the modifications introduced by G.729.1 (2006) Amd. 1 approved on 13 January 2007, and G.729.1 (2006) Amd. 2 approved on 13 February 2007.

G.732 ITU-T Recommendation G.732, “Characteristics of primary PCM multiplex equipment operating at 2048 kbit/s,” Geneva, Switzerland, November 1988.

G.772 ITU-T Recommendation G.772 (REV), “Protected monitoring points on digital transmission systems,” Geneva, Switzerland, March 2003.

- H.244 ITU Recommendation H.244, “Synchronized aggregation of multiple 64 or 56 kbit/s channels,” Geneva, Switzerland, July 1995.
- H.248.1 ITU-T Recommendation H.248.1, “Gateway control protocol: Version 3,” Geneva Switzerland, September 2005.
- H.248.24 ITU-T Recommendation H.248.24, “Gateway control protocol: Multi-frequency tone generation and detection packages,” Geneva, Switzerland, July 2003.
- H.248.25 ITU-T Recommendation H.248.24, “Gateway control protocol: Basic CAS packages,” Geneva, Switzerland, January 2007.
- H.248.28 ITU-T Recommendation H.248.28, “Gateway control protocol: International CAS packages,” Geneva, Switzerland, January 2007.
- H.261 ITU-T Recommendation H.261, “Video codec for audiovisual services at p x 64 kbit/s,” Recommendation H.261, Geneva, Switzerland, March 1993.
- H.263 ITU-T Recommendation H.263, “Video coding for low bit rate communication,” Geneva, Switzerland, January 2005. (H.263a, H.323+, H.263 (1999)).
- H.264 ITU-T Recommendation H.264, “Advanced video coding for generic audiovisual services,” Geneva, Switzerland, March 2005. (Also, known as H.264/AVC)
- H.323 ITU-T Recommendation H.323, “Packet-based multimedia communications systems,” Geneva, Switzerland, June 2006.
- I.431 ITU-T Recommendation I.431, “Primary rate user-network interface – Layer 1 specification,” Geneva, Switzerland, March 1993.
- M.3100 ITU-T Recommendation M.3100, “Generic network information model,” Geneva, Switzerland, April 2005.
- P.561 ITU-T Recommendation P.561, “In-service non-intrusive measurement device – Voice service measurements,” Geneva, Switzerland, July 2002.
- P.562 ITU-T Recommendation P.562, “Analysis and interpretation of INMD voice-service measurements,” Geneva, Switzerland, May 2004.

FOR OFFICIAL USE ONLY

Appendix A1 – Definitions, Abbreviations and Acronyms, and References

Section A4 – References

- P.862 ITU-T Recommendation P.862, “Perceptual evaluation of speech quality (PESQ): An objective method for end-to-end speech quality assessment of narrow-band telephone networks and speech codecs,” Geneva, Switzerland, February 2001.
- Q.735.3 ITU-T Recommendation Q.735.3, “Stage 3 description for community of interest supplementary services using Signalling System No. 7: Multi-level precedence and preemption,” Geneva, Switzerland, March 1993.
- Q.850 ITU-T Recommendation Q.850, “Usage of cause and location in the Digital Subscriber Signalling System No. 1 and the Signalling System No. 7 ISDN User Part,” Geneva, Switzerland, May 1998.
- Q.921 ITU-T Recommendation Q.921, “ISDN user-network interface – Data link layer specification,” Geneva, Switzerland, September 1997.
- NOTE: This Recommendation is published with the double number Q.921 and I.441.
- Q.931 ITU-T Recommendation Q.931, “ISDN user-network interface layer 3 specification for basic call control,” Geneva, Switzerland, May 1998.
- NOTE: This Recommendation is also included but not published in I series under alias number I.451.
- Q.955.3 ITU-T Recommendation Q.955.3, “Stage 3 description for community of interest supplementary services using DSS 1 – Multi-level precedence and preemption (MLPP),” Geneva, Switzerland, March 1993.
- Q.1912.5 ITU-T Recommendation Q.1912.5, “Interworking between Session Initiation Protocol (SIP) and Bearer Independent Call Control Protocol or ISDN User Part,” Geneva, Switzerland, March 2004.
- T.4 ITU-T Recommendation T.4, “Standardization of Group 3 facsimile terminals for document transmission,” Geneva, Switzerland, July 2003.
- T.38 ITU-T Recommendation T.38, “Procedures for real-time Group 3 facsimile communication over IP networks,” Geneva, Switzerland, April 2007.
- V.35 ITU-T Recommendation V.35, “Data transmission at 48 kilobits per second using 60-108 kHz group band circuits,” Geneva, Switzerland, October 1984.

- V.54 ITU-T Recommendation V.54, “Loop test devices for modems,” Geneva, Switzerland, November 1988.
- V.90 ITU-T Recommendation V.90, “A digital modem and analogue modem pair for use on the Public Switched Telephone Network (PSTN) at data signalling rates of up to 56 000 bit/s downstream and up to 33 600 bit/s upstream,” Geneva, Switzerland, September 1998.
- V.92 ITU-T Recommendation V.92, “Enhancements to Recommendation V.90,” November 2000.
- V.150.1 ITU-T Recommendation V.150.1, “Modem-over-IP networks: Procedures for the end-to-end connection of V-series DCEs,” Geneva, Switzerland, January 2003.
- ITU-T Recommendation V.150.1, Amendment 1, Geneva, Switzerland, January 2005.
- X.731 ITU-T Recommendation X.731, “Information technology – Open Systems Interconnection – Systems management: State management function,” Geneva, Switzerland, January 1992.
- X.805 ITU-T Recommendation X.805, “Security architecture for systems providing end-to-end communications,” Geneva, Switzerland, October 2003.
- Y.1541 ITU-T Recommendation Y.1541, “Network performance objectives for IP-based services,” Geneva, Switzerland, February 2006.

A4.10 INTERNET ENGINEERING TASK FORCE REQUESTS FOR COMMENT

- RFC 768 Postel, J., “User Datagram Protocol,” August 1980.
- RFC 791 Information Services Institute, “Internet Protocol,” September 1981.
- RFC 793 Information Services Institute, “Transmission Control Protocol,” September 1981.
- RFC 1046 Prue, W. and J. Postel, “A Queuing Algorithm to Provide Type-of-Service for IP Links,” February 1988.
- RFC 1157 Case, J., M. Fedor, M. Schoffstall, and J. Davin, “A Simple Network Management Protocol (SNMP),” May 1990.

FOR OFFICIAL USE ONLY

Appendix A1 – Definitions, Abbreviations and Acronyms, and References

Section A4 – References

- RFC 1215 Rose, M., Ed., “A Convention for Defining Traps for use with SNMP,” March 1991.
- RFC 1772 Rekhter, Y., P. Gross, “Application of the Border Gateway Protocol in the Internet,” March 1995.
- RFC 1812 Baker, F., Ed., “Requirements for IP Version 4 Routers,” June 1995.
- RFC 1981 McCann, J., S. Deering, and J. Mogul, “Path MTU Discovery for IP Version 6,” August 1996.
- RFC 2119 Bradner, S., “Key words for use in RFCs to Indicate Requirement Levels,” March 1997.
- RFC 2205 Braden, R., Ed., L. Zhang, S. Berson, S. Herzog, and S. Jamin, “ReSerVation Protocol (RSVP)– Version 1 Functional Specification,” September 1997.
- RFC 2206 Baker, F., J. Krawczyk, and A. Sastry, “RSVP Management Information Base using SMIV2,” September 1997.
- RFC 2327 Handley, M. and V. Jacobson, “SDP: Session Description Protocol,” April 1998.
- RFC 2407 Piper, D., “The Internet IP Security Domain of Interpretation for ISAKMP,” November 1998.
- RFC 2408 Maughan, D., M. Schertler, M. Schneider and J. Turner, “Internet Security Association and Key Management Protocol (ISAKMP),” November 1998.
- RFC 2409 Harkins, J. and D. Carrel, “The Internet Key Exchange (IKE),” November 1998.
- RFC 2460 Deering S. and R. Hinden, “Internet Protocol Version 6 (IPv6) Specification,” December 1998.
- RFC 2461 Narten, T., E. Nordmark, and W. Simpson, “Neighbor Discovery for IP Version 6 (IPv6),” December 1998.
- RFC 2462 Thomson, S. and T. Narten, “IPv6 Stateless Address Autoconfiguration,” December 1998.
- RFC 2464 Crawford, M., “Transmission of IPv6 Packets over Ethernet Networks,” December 1998.

- RFC 2473 Conta, A. and S. Deering, “Generic Packet Tunneling in IPv6 Specification,” December 1998.
- RFC 2474 Nichols, K., S. Blake, F. Baker, and D. Black, “Definition of the Differentiated Services Field (DS Field) in the IPv4 and IPv6 Headers,” December 1998.
- RFC 2475 Blake, S., D. Black, M. Carlson, E. Davies, Z. Wang, and W. Weiss, “An Architecture for Differentiated Services,” December 1998.
- RFC 2494 Fowler, D., Ed., “Definitions of Managed Objects for the DS0 and DS0 Bundle Interface Type,” January 1999.
- RFC 2545 Marques, P. and F. Dupont, “Use of BGP-4 Multiprotocol Extensions for IPv6 Inter-Domain Routing,” March 1999.
- RFC 2597 Heinanen, J., F. Baker, W. Weiss, and J. Wroclawski, “Assured Forwarding PHB Group,” June 1999.
- RFC 2598 Jacobson, V., K. Nichols, and K. Poduri, “An Expedited Forwarding PHB,” June 1999.
- RFC 2660 Rescorla, E., and A. Schiffman, “The Secure HyperText Transfer Protocol,” August 1999.
- RFC 2702 Awduche, D., J. Malcolm, J. Agogbua, M. O’Dell, and J. McManus, “Requirements for Traffic Engineering Over MPLS,” September 1999.
- RFC 2710 Deering S., W. Feener, and B. Haberman, “Multicast Listener Discovery (MLD) for IPv6,” October 1999.
- RFC 2740 Coltun, R., D. Ferguson, and J. Moy, “OSPF for IPv6,” December 1999.
- RFC 2805 Greene, N., M. Ramalho, and B. Rosen, “Media Gateway Control Protocol Architecture and Requirements,” RFC 2805, April 2000.
- RFC 2806 Vaha-Sipila, A., “URLs for Telephone Calls,” April 2000.
- RFC 2818 Rescorla, E., “HTTP over TLS, May 2000.

FOR OFFICIAL USE ONLY

Appendix A1 – Definitions, Abbreviations and Acronyms, and References

Section A4 – References

- RFC 2819 Waldbusser, S., “Remote Network Monitoring Management Information Base,” May 2000.
- RFC 2833 Schulzrinne, H. and S. Petrack, “RTP Payload for DTMF Digits, Telephony Tones and Telephony Signals,” May 2000.
- RFC 2858 Bates, T., Y. Rekhter, R. Chandra, and D. Katz, “Multiprotocol Extensions for BGP-4,” June 2000.
- RFC 2960 Stewart, R., Q. Xie, K. Morneault, C. Sharp, H. Schwarzbauer, T. Taylor, I. Rytina, M. Kalla, L. Zhang, and V. Paxson, “Stream Control Transmission Protocol,” October 2000.
- RFC 2976 Donovan, S., “The SIP INFO Method,” October 2000.
- RFC 3041 Narten, T. and R. Draves, “Privacy Extensions for Stateless Address Autoconfiguration in IPv6,” January 2001.
- RFC 3118 Droms, R., Ed., W. Arbaugh, “Authentication for DHCP Messages,” June 2001.
- RFC 3204 Zimmerer, E., J. Peterson, A. Vemuri, L. Ong, F. Audet, M., Watson, and M. Zonoun, “MIME media types for ISUP and QSIG Objects,” December 2001.
- RFC 3246 Davie, B., A. Charny, J.C.R. Bennett, K. Benson, J.Y. Le Boudec, W. Courtney, S. Davari, V. Firoiu, and D. Stiliadis, “An Expedited Forwarding PHB (Per-Hop Behavior),” March 2002.
- RFC 3261 Rosenberg, J., H. Schulzrinne, G. Camarillo, A. Johnston, J. Peterson, R. Sparks, M. Handley, and R. Schooler, “SIP: Session Initiation Protocol,” June 2002.
- RFC 3262 Rosenberg, J. and H. Schulzrinne, “Reliability of Provisional Responses in Session Initiation Protocol (SIP),” June 2002.
- RFC 3264 Rosenberg, J. and H. Schulzrinne, “An Offer/Answer Model with the Session Description Protocol (SDP),” June 2002.
- RFC 3265 Roach, A. B., “Session Initiation Protocol (SIP)-Specific Event Notification,” June 2002.
- RFC 3266 Olson, S., G. Camarillo, and A. B. Roach, “Support for IPv6 in Session,” June 2002.

- RFC 3267 Sjoberg, J., M. Westerlund, A. Lakaniemi, and Q. Xie, “Real-Time Transport Protocol (RTP) Payload Format and File Storage Format for the Adaptive Multi-Rate (AMR) and Adaptive Multi-Rate Wideband (AMR-WB) Audio Codecs,” June 2002.
- RFC 3309 Stone, J., R. Stewart, and D. Otis, “Stream Control Transmission Protocol (SCTP) Checksum Change,” September 2002.
- RFC 3311 Rosenberg, J., “The Session Initiation Protocol (SIP) UPDATE Method,” September 2002.
- RFC 3312 Camarillo, G., W. Marshall, and J. Rosenberg, “Integration of Resource Management and Session Initiation Protocol (SIP),” October 2002.
- RFC 3315 Droms, E., J. Bound, B. Volz, T. Lemon, C. Perkins, and M. Carney, “Dynamic Host Configuration Protocol for IPv6 (DHCPv6),” July 2003.
- RFC 3323 Peterson, J., “A Privacy Mechanism for the Session Initiation Protocol (SIP),” November 2002.
- RFC 3325 Jennings, C., J. Peterson, and M. Watson, “Private Extensions to the Session Initiation Protocol (SIP) for Asserted Identity within Trusted Networks,” November 2002.
- RFC 3326 Schulzrinne, H., D. Oran, and G. Camarillo, “The Reason Header Field for the Session Initiation Protocol (SIP),” December 2002.
- RFC 3331 Morneault, K., R. Dantu, G. Sidebottom, B. Bidulock, and J. Heitz, “Signaling System 7 (SS7) Message Transfer Part 2 (MTP2) – User Adaptation Layer,” September 2002.
- RFC 3366 Fairhurst, G., and L. Wood, “Advice to link designers on link Automatic Repeat reQuest (ARQ),” August 2002.
- RFC 3372 Vemuri, A., and J. Peterson, “Session Initiation Protocol for Telephones (SIP-T): Context and Architecture,” September 2002.
- RFC 3398 Camarillo, G., A. B. Roach, J. Peterson, and L. Ong, “Integrated Services Digital Network (ISDN) User Part (ISUP) to Session Initiation Protocol (SIP) Mapping,” December 2002.

FOR OFFICIAL USE ONLY

Appendix A1 – Definitions, Abbreviations and Acronyms, and References

Section A4 – References

- RFC 3410 Case, J., R. Mundy, D. Partain, and B. Stewart, “Introduction and Applicability Statements for Internet Standard Management Framework,” December 2002.
- RFC 3411 Harrington, D., R. Presuhn, and B. Wijnen, “An Architecture for Describing Simple Network Management Protocol (SNMP) Management Frameworks,” December 2002.
- RFC 3412 Case, J., D. Harrington, R. Presuhn, and B. Wijnen, “Message Processing and Dispatching for the Simple Network Management Protocol (SNMP),” December 2002.
- RFC 3413 Levi, D., P. Meyer, and B. Stewart, “Simple Network Management Protocol (SNMP) Applications,” December 2002.
- RFC 3414 Blumenthal, U., and B. Wijnen, “User-based Security Model (USM) for version 3 of the Simple Network Management Protocol (SNMPv3), December 2002.
- RFC 3459 Burger, E., “Critical Content Multi-Purpose Internet Mail Extensions (MIME) Parameter,” January 2003.
- RFC 3484 Draves, R., “Default Address Selection for Internet Protocol Version 6 (IPv6),” February 2003.
- RFC 3513 Hinden, R., and S. Deering, “Internet Protocol Version 6 (IPv6) Addressing Architecture,” April 2003.
- RFC 3515 Sparks, R., “The Session Initiation Protocol (SIP) Refer Method,” April 2003.
- RFC 3550 Schulzrinne, H., S. Casner, R. Frederick, and V. Jacobson, “RTP: A Transport Protocol for Real-Time Applications,” July 2003.
- RFC 3584 Frye, R., D. Levi, S. Routhier, and B. Wijnen, “Coexistence between Version 1, Version 2, and Version 3 of the Internet-standard Network Management Framework,” August 2003.
- RFC 3596 Thomson, S., C. Huitema, V. Ksinant, and M. Souissi, “DNS Extensions to Support IPv6,” October 2003.
- RFC 3608 Willis, D., and B. Hoeneisen, “Session Initiation Protocol (SIP) Extension Header Field for Service Route Discovery During Registration,” October 2003.

- RFC 3662 Bless, R., K. Nichols, and K. Wehrle, “A Lower Effort Per-Domain Behavior (PDB) for Differentiated Services,” December 2003.
- RFC 3670 Moore, B., D. Durham, J. Strassner, A. Westerinen, and W. Weiss, “Information Model for Describing Network Device QoS Datapath Mechanism,” January 2004.
- RFC 3711 Baugher, M., D. McGrew, M. Naslund, E. Carrara, and K. Norrman, “The Secure Real-time Transport Protocol (SRTP),” March 2004.
- RFC 3775 Johnson, D., C., Perkins, and J. Arkko, “Mobility Support in IPv6,” June 2004.
- RFC 3776 Arkko, J., V. Devarapalli, and F. Dupont, “Using IPSec to Protect Mobile IPv6 Signaling Between Mobile Nodes and Home Agents,” June 2004.
- RFC 3826 Blumenthal, U., F. Maino, and K. McCloghrie, “The Advanced Encryption Standard (AES) Cipher Algorithm in the SNMP User-based Security Model,” June 2004.
- RFC 3840 Rosenberg, J., H. Schulzrinne, and P. Kyzivat, “Indicating User Agent Capabilities in the Session Initiation Protocol (SIP),” August 2004.
- RFC 3853 Peterson, J., “S/MIME Advanced Encryption Standard (AES) Requirements for the Session Initiation Protocol (SIP),” July 2004.
- RFC 3868 Loughney, J., Ed., G. Sidebottom, L. Coene, G. Verwimp, J. Keller, and B. Bidulock, “Signalling Connection Control Part User Adaptation Layer (SUA),” October 2004.
- RFC 3890 Westerlund, M., “A Transport Independent Bandwidth Modifier for the Session Description Protocol (SDP),” September 2004.
- RFC 3891 Mahy, R., B. Biggs, and R. Dean, “The Session Initiation Protocol (SIP) “Replaces” Header,” September 2004.
- RFC 3892 Sparks, R., “The Session Initiation Protocol (SIP) Referred-By Mechanism,” September 2004.
- RFC 3960 Camarillo, G., and H. Schulzrinne, “Early Media and Ringing Tone Generation in the Session Initiation Protocol (SIP),” December 2004

FOR OFFICIAL USE ONLY

Appendix A1 – Definitions, Abbreviations and Acronyms, and References

Section A4 – References

- RFC 3963 Devarapalli, V., R. Wakikawa, A. Petrescu, and P. Thurbert, “Network Mobility (NEMO) Basic Support Protocol,” January 2005.
- RFC 3966 Schulzrinne, H., “The tel URI for Telephone Numbers,” December 2004.
- RFC 3968 Camarillo, G., “The Internet Assigned Number Authority (IANA) Header Field Parameter Registry for the Session Initiation Protocol (SIP),” December 2004.
- RFC 3971 Arkko, E., B. Zill, J. Kempf, and P. Nikander, “Secure Neighbor Discovery (SEND),” March 2005.
- RFC 3984 Wenger, S., M. M. Hannuksela, T., Stockhammer, M. Westerlund, and D. Singer, “RTP Payload Format for H.264 Video,” February 2005.
- RFC 3986 Berners-Lee, T., R. Fielding, and L. Masinter, “Uniform Resource Identifier (URI): Generic Syntax,” January 2005.
- RFC 4007 Deering, S., B. Haberman, T. Jinmei, E. Nordmark, and B. Zill, “IPv6 Scoped Address Architecture,” March 2005.
- RFC 4022 Raghunathan, R., “Management Information Base for the Transmission Control Protocol (TCP),” March 2005.
- RFC 4028 Donovan, B., and J. Rosenberg, “Session Timers in the Session Initiation Protocol (SIP),” April 2005.
- RFC 4040 Kreuter, R., “RTP Payload Format for a 64 kbit/s Transparent Call,” April 2005.
- RFC 4091 Camarillo, G. and J. Rosenberg, “The Alternative Network Address Types (ANAT) Semantics for the Session Description Protocol (SDP) Grouping Framework,” June 2005.
- RFC 4092 Camarillo, G. and J. Rosenberg, “Usage of the Session Description Protocol (SDP) Alternative Network Address Types (ANAT) Semantics in the Session Initiation Protocol (SIP),” June 2005.
- RFC 4109 Hoffman, P., “Algorithms for Internet Key Exchange version 1 (IKEv1),” May 2005.
- RFC 4113 Fenner, B. and J. Flick, “Management Information Base for the User Datagram Protocol (UDP),” June 2005.

- RFC 4165 George, T., B. Bidulock, R. Dantu, H. Schwarzbauer, and K. Morneault, “Signaling System 7 (SS7) Message Transfer Part 2 (MTP2) – User Peer-to-Peer Adaptation Layer (M2PA),” September 2005.
- RFC 4191 Draves, R. and D. Thaler, “Default Router Preferences and More-Specific Routes,” November 2005.
- RFC 4193 Hinden, R. and B. Haberman, “Unique Local IPv6 Unicast Addresses,” October 2005.
- RFC 4213 Nordmark, E. and R. Gilligan, “Basic Transition Mechanisms for IPv6 Hosts and Routers,” October 2005.
- RFC 4233 Morneault, K., S. Rengasami, M. Kalla, and G. Sidebottom, “Integrated Services Digital Network (ISDN) Q.921-User Adaptation Layer, January 2006.
- RFC 4251 Ylonen, T., and C. Lonvick, Ed., “The Secure Shell (SSH) Protocol Architecture,” January 2006.
- RFC 4252 Ylonen, T., and C. Lonvick, Ed., “The Secure Shell (SSH) Authentication Protocol,” January 2006.
- RFC 4253 Ylonen, T., and C. Lonvick, Ed., “The Secure Shell (SSH) Transport Layer Protocol,” January 2006.
- RFC 4254 Ylonen, T., and C. Lonvick, Ed., “The Secure Shell (SSH) Connection Protocol,” January 2006.
- RFC 4271 Rekhter, Y., T. Li, and S. Hares, “A Border Gateway Protocol 4 (BGP-4),” January 2006.
- RFC 4291 Hinden, R. and S. Deering, “IP Version 6 Addressing Architecture,” February 2006.
- RFC 4293 Routhier, S., “Management Information Base for the Internet Protocol (IP),” April 2006.
- RFC 4294 Loughney, E., “IPv6 Node Requirements,” April 2006.
- RFC 4301 Kent, S. and K. Seo, “Security Architecture for the Internet Protocol,” December 2005.

FOR OFFICIAL USE ONLY

Appendix A1 – Definitions, Abbreviations and Acronyms, and References

Section A4 – References

- RFC 4302 Kent, S., “IP Authentication Header,” December 2005.
- RFC 4303 Kent, S., “IP Encapsulating Security Payload (ESP),” December 2005.
- RFC 4304 Kent, S., “Extended Sequence Number (ESN) Addendum to IPSec Domain of Interpretation (DOI) for Internet Security Association and Key Management Protocol (ISAKMP),” December 2005.
- RFC 4305 Eastlake, D., “Cryptographic Algorithm Implementation Requirements for the Encapsulating Security Payload (ESP) and Authentication Header (AH),” December 2005.
- RFC 4306 Kaufman, E., “Internet Key Exchange (IKEv2) Protocol,” December 2005.
- RFC 4307 Schiller, J., “Cryptographic Algorithms for Use in the Internet Key Exchange Version 2 (IKEv2),” December 2005.
- RFC 4308 Hoffman, P., “Cryptographic Suites for IPSec,” December 2005.
- RFC 4320 Sparks, R., “Action Addressing Identified Issues with the Session Initiation
- RFC 4330 Mills, D., “Simple Network Time Protocol (SNTP) version 4 for IPv4, IPv6, and OSI,” January 2006.
- RFC 4346 Dierks, T., and E. Rescorla, “The Transport Layer Security (TLS) Protocol, Version 1.1,” April 2006.
- RFC 4411 Polk, J., “Extending the Session Initiation Protocol (SIP) Reason Header for Preemption Events,” February 2006.
- RFC 4412 Schulzrinne, H. and J. Polk, “Communications Resource Priority for the Session Initiation Protocol (SIP),” February 2006.
- RFC 4443 Conta, A., S. Deering, and M. Gupta, “Internet Control Message Protocol (ICMPv6) for the Internet Protocol Version 6 (IPv6) Specification,” March 2006.
- RFC 4566 Handley, M., V. Jacobson, and C. Perkins, “SDP: Session Description Protocol,” July 2006.
- RFC 4666 Morneault, K., Ed., and J. Pastor-Balbas, Ed., “Signaling System 7 (SS7) Message Transfer Part 3 (MTP3) – User Adaptation Layer (M3UA),” September 2006.

- RFC 4904 Gurbani, V. and C. Jennings, “Representing Trunk Groups in tel/sip Uniform Resource Identifiers (URIs),” June 2007.
- RFC draft Camarillo, G., K. El Malki, V. Gurbani, Ed., “IPv6 Transition in the Session Initiation Protocol (SIP),” draft-ietf-sipping-v6-transition-02.txt, IETF Internet-Draft, I-D Exists, 7 February 2006.
- RFC draft Johnston, A., R. Sparks, S. Cunningham, S. Donovan, and K. Summers, “SIP Service Examples,” draft-ietf-sipping-service-examples-10.txt, IETF Internet-Draft, I-D Expired, 6 September 2006.

A4.11 JOINT REQUIREMENTS OVERSIGHT COUNCIL DOCUMENTS

- JROCM 048-96 Memorandum for the Under Secretary of Defense for Acquisition and Technology, Subject: Validation of Defense Information Systems Network (DISN) Capstone Requirements Document (CRD), 15 April 1996.
- JROCM 134-01 “Global Information Grid (GIG) Capabilities Requirement Document (CRD),” 30 August 2001.
- JROCM 202-02 “Global Information Grid (GIG), Mission Area Initial Capabilities Document (MA ICD),” 22 November 2002.

A4.12 NATIONAL SECURITY AGENCY DOCUMENTS

- National Security Agency, “Common Criteria for Information Technology Evaluation, Protection Profile for Switches and Routers,” Draft 2.1, 22 February 2001.
- National Security Agency, “DoD Class 3 Public Key Infrastructure Interface Specification,” Version 1.2, 10 August 2000.

A4.13 NATIONAL SECURITY TELECOMMUNICATIONS AND INFORMATION SYSTEMS SECURITY DOCUMENTS

- NSTISSI No. 4009 National Security Telecommunications and Information Systems Security Instruction, “National Information Systems Security (INFOSEC) Glossary,” 5 June 1992.
- National Security Telecommunications and Information Systems Security Authority Manual (NSTISSAM), “TEMPEST/2-95, RED/Black Installation Guidance,” 12 December 1995.

Section A4 – References

National Security Telecommunications and Information Systems Security Committee (NSTISSC), “National Security Telecommunications and Information Systems Security Policy (NSTISSP) No. 11, Subject: National Policy Governing the Acquisition of Information Assurance (IA) and IA-Enabled Information Technology (IT) Products,” January 2000 and revised June 2003.

A4.14 U. S. SECURE COMMUNICATION INTEROPERABILITY PROTOCOL

SCIP-215 U.S. Secure Communication Interoperability Protocol (SCIP) over IP Implementation Standard and Minimum Essential Requirements (MER) Publication, Revision 2.0, 3 October 2007.

SCIP-216 Minimum Essential Requirements (MER) for V.150.1 Gateways Publication, Revision 2.0, 2 November 2007.

A4.15 TELCORDIA TECHNOLOGIES DOCUMENTS

Feature Service Description (FSD) 30-33-0000, *Release to Pivot Network Capability*.

FR-E911-1 *Requirements to Support E9-1-1 Service*, Issue 5, January 2007.

GR-63-CORE *NEBS™ Requirements: Physical Protection*, 2002.

GR-217-CORE *CLASSSM Feature: Selective Call Forwarding*, Issue 1, June 2000.

GR-218-CORE *CLASSSM Feature: Selective Call Rejection*, Issue 1, June 2000.

GR-246-CORE *Specification of Signalling System Number 7*, 2005/12/30.

GR-253-CORE *Synchronous Optical Network (SONET) Transport Systems: Common Generic Criteria*, December 2005.

GR-303-CORE *Integrated Digital Loop Carrier System Generic Requirements, Objectives, and Interface*, Issue 4, December 2000.

GR-436-CORE *Digital Network Synchronization Plan*, Issue 1 with Revision 1, June 1996.

GR-472-CORE *Network Element Configuration Management*, Revision 2, February 1999.

FOR OFFICIAL USE ONLY

Appendix A1 – Definitions, Abbreviations and Acronyms, and References

Section A4 – References

GR-474-CORE	<i>OTGR Section 4: Network Maintenance: Alarm and Control for Network Elements</i> , December 1997.
GR-477-CORE	<i>Network Traffic Management</i> , February 2000.
GR-478-CORE	Issue 4, February 2000.
GR-505-CORE	<i>Call Processing</i> , December 1997.
GR-506-CORE	<i>LSSGR: Signaling for Analog Interfaces</i> , December 2006.
GR-510-CORE	<i>System Interfaces</i> , Issue 1, June 2000.
GR-512-CORE	<i>LSSGR: Reliability</i> , Section 12, January 1998.
GR-513-CORE	<i>Module of the LSSGR, FR-64</i> , Issue 1, September 1995.
GR-517-CORE	<i>LSSGR: Traffic Capacity and Environment</i> , December 1997.
GR-518-CORE	<i>LSSGR: Synchronization Section 18</i> , Issue 1, May 1994.
GR-520-CORE	<i>Features Common to Residence and Business</i> , Issue 1, June 2000.
GR-524-CORE	<i>LSSGR: Attendant and Customer Switching System Features and Customer Interfaces, PBX Line</i> , Issue 1, FSD 04-01-0000, June 2000.
GR-529-CORE	<i>LSSGR: Public Safety</i> , June 2000.
GR-533-CORE	<i>LSSGR: Database Services – Service Switching Points, Toll-Free Service</i> , (FSD 31-01-000), June 2001.
GR-540-CORE	, <i>LSSGR: Tandem Supplement</i> , Issue 2, March 1999.
GR-562-CORE	<i>Manual Line Features</i> , Issue 1, June 2000.
GR-569-CORE	<i>Multiline Hunt Service</i> , Issue 1, June 2000.
GR-571-CORE	<i>LSSGR: Call Waiting, FSD 01-02-1201</i> , June 2000.
GR-572-CORE	<i>LSSGR: Cancel Call Waiting, FSD 01-02-1204</i> , June 2000.

FOR OFFICIAL USE ONLY

Appendix A1 – Definitions, Abbreviations and Acronyms, and References

Section A4 – References

- GR-577-CORE *Three-Way Calling*, Issue 1, June 2000.
- GR-579-CORE *Add-on Transfer and Conference Calling Features*, Issue 1, June 2000.
- GR-580-CORE *LSSGR: Call Forwarding Variable*, FSD 01-02-1401, June 2000.
- GR-586-CORE *LSSGR: Call Forwarding Subfeatures*, FSD 01-02-1450, April 2002.
- GR-590-CORE *LSSGR: Call Pickup Features*, Issue 1, June 2000.
- GR-606-CORE *LSSGR: Common Channel Signaling, Section 6.5*, Component of FR-64, December 2004.
- GR-690-CORE *LSSGR: Exchange Access Interconnection*, FSD 20-24-0000, November 1996.
- GR-741-CORE *LSSGR: Network Administration Center (NAC) Input/Output (I/O) Channel*, FSD 45-10-0000, June 2000.
- GR-747-CORE *LSSGR: An Alternative Implementation of an SPCS to NTM OS Interface via an NDC OS*, FSD 45-18-0450, June 2000.
- GR-782-CORE *SONET Digital Switch Trunk Interface Criteria*, A Module of TSGR, FR-440, Issue 1, June 2000 (Formerly TR-TSY-000782, Issue 2, September 1989).
- GR-815-CORE *Generic Requirements for Network Element/Network System (NE/NS) Security: A Module of LSSGR*, Component of FR-64, Issue 2, March 2002.
- GR-820-CORE *OTGR Section 5.1: Generic Digital Transmission Surveillance*, December 1997.
- GR-822-CORE *OTGR Section 6.3: Network Maintenance: Access and Testing-Switched Circuits, Pots Loops and Public Packet Switched Network (PPSN)*, December 1995.
- GR-844-CORE *Network Maintenance: Access and Testing TSC/RTU Generic Requirements for Metallic Loop Testing*, November 1995.

FOR OFFICIAL USE ONLY

Appendix A1 – Definitions, Abbreviations and Acronyms, and References

Section A4 – References

GR-874-CORE	<i>An Introduction to the Reliability and Quality Generic Requirements (RQGR), Issue 3, April 1997.</i>
GR-1100-CORE	<i>Billing Automatic Message Accounting Format (BAF) Generic Requirements, December 2007.</i>
GR-2932-CORE	<i>Database Functionalities, May 1997.</i>
GR-3051-CORE	<i>Voice Over Packet: NGN Call Connection Agent Generic Requirements, Issue 2, January 2001.</i>
GR-3053-CORE	<i>Voice Over Packet (VOP): Next Generation Network (NGN) Signaling Gateway Generic Requirements, February 2000.</i>
GR-3054-CORE	<i>Voice Over Packet: NGN Trunk Gateway Generic Requirements, Issue 1, March 2000.</i>
GR-3055-CORE	<i>Voice Over Packet: NGN Access Gateway Generic Requirements, Issue 1, March 2000.</i>
GR-3058-CORE	<i>Voice over Packet (VoP): Next Generation Networks (NGN) Accounting Management Generic Requirements, December 2005.</i>
SR-2275	<i>Telcordia Notes on the Networks, Issue 4, Section 6, Signaling, October 2000.</i>
SR-3476	<i>National ISDN 1995 and 1996, Issue 1, June 1995.</i>
SR-4994	<i>2000 Version of National ISDN Primary Rate Interface (PRI) Customer Premises Equipment Generic Guidelines, Issue 1, December 1999.</i>
SR-NWT-002120	<i>National ISDN-2, Issue 1, May 1992 with revision 1, June 1993.</i>
SR-NWT-002343	<i>ISDN Primary Rate Interface Generic Guidelines for Customer Premises Equipment, Issue 1, June 1993.</i>
TR-NWT-000057	<i>Functional Criteria for Digital Loop Carrier Systems, Issue 2, January 1993.</i>
TR-NWT-001244	<i>Clocks for the Synchronized Network: Common Generic Criteria, Issue 1, June 1993.</i>

FOR OFFICIAL USE ONLY

Appendix A1 – Definitions, Abbreviations and Acronyms, and References

Section A4 – References

TR-NWT-001268 *ISDN Primary Rate Interface Call Control Switching and Signaling Generic Requirements for Class II Equipment*, Issue 1, December 1991.

TR-NWT-000284 *Reliability and Quality Switching Systems Generic Requirements (RQSSGR)*, Issue 2, October 1990.

Telcordia and Computer Sciences Corporation, *Call Connection Agent (CCA) Chapter, Assured Real Time Service (ARTS) Generic System Requirement (GRS)*, Draft October 2006.

Telcordia and Computer Sciences Corporation, *Media Gateway Chapter, Assured Real Time Service (ARTS) Generic System Requirement (GRS)*, Draft October 2006.

Telcordia and Computer Sciences Corporation, *Signaling Gateway Chapter, Assured Real Time Service (ARTS) Generic System Requirement (GRS)*, Draft October 2006.

A4.16 UNITED STATES CODE

Title 10 Section 2224, “Defense Information Assurance Program.”

Title 40 Section 11331.

Title 44 “Federal Information Security Management Act (FISMA) of 2002.”

A4.17 OTHER DOCUMENTS

ATIS-PP-1000012.2006, *Signaling Systems No. 7 (SS7) – SS7 – Network and NNI Interconnection Security Requirements and Guidelines*, November 2006.

DCID 6/3, Series, “Protecting Sensitive Compartmented Information within Information Systems.”

EIA-366-A, “Interface Between Data Terminal Equipment and Automatic Calling Equipment for Data Communication.”

EIA-449-1, “General Purpose 37-Position and 9-Position Interface for Data Terminal Equipment and Data Circuit-Terminating Equipment Employing Serial Binary Data Interchange.”

Federal Telecommunications Recommendation 1080B-2002, “*Video Teleconferencing Services*,” August 15, 2002.

Global Information Grid (GIG) Mission Area Initial Capabilities Document, (MA ICD), 6 January 2003.

House Report 107-436, “Bob Stump National Defense Authorization Act for Fiscal Year 2003”: Report of the Committee on Armed Services, House of Representatives on H.R. 4546, 3 May 2002.

Joint Interoperability Test Center, “Internet Protocol Version 6 Generic Test Plan,” Version 2, June 2006.

Joint Staff, Command, Control, Communications, and Computer Systems Directorate (J-6), “Joint Net-Centric Operations Campaign Plan,” October 2006.

National Communications System, NCS Directive 3-10, “Telecommunications Operations, Government Emergency Telecommunications Service (GETS),” 2000.

Net-Centric I Document (NCID) Version 3 QoS (T300).

Office of Management and Budget (OMB) Circular A-130, Appendix III.

Public Law 107-314, Section 353, “Bob Stump National Defense Authorization Act for Fiscal Year 2003,” 2 December 2002.

Real-Time Services Information Assurance Working Group, “Analysis of IA Requirements and Threats for the DoD RTS Environment,” Version 2.2, July 2005.

Real-Time Services Working Group, “Real Time Services (RTS) Information Assurance (IA) Generic System Requirements (GSR),” Version 1.3, 6 July 2006.

TIA-232-F, “Interface Between Data Terminal Equipment and Data Circuit-Terminating Equipment Employing Serial Binary Data Interchange.”

TIA-530-A, “High Speed 25-Position Interface for Data Terminal Equipment and Data Circuit-Terminating Equipment, Including Alternative 26-Position Connector.”

TIA/EIA-470-B, “Telecommunications - Telephone Terminal Equipment - Performance and Compatibility Requirements for Telephone Sets with Loop Signaling,” 1997.

TIA TSB-116, “Telecommunications – IP Telephony Equipment – Voice Quality Recommendations for IP Telephony,” March 2001.

TIA TSB-116-A, “Telecommunications System Bulletin – Telecommunications – IP Telephony Equipment – Voice Quality Recommendations for IP Telephony,” March 2006.

THIS PAGE INTENTIONALLY LEFT BLANK