Department of Defense

Unified Capabilities Requirements 2013 (UCR 2013) Errata-1

July 2013

The Office of the DoD Chief Information Officer

DEPARTMENT OF DEFENSE
UNIFIED CAPABILITIES REQUIREMENTS 2013(UCR 2013) ERRATA-1

This document specifies the functional requirements, performance objectives, and technical specifications for DoD networks that support UC, and shall be used to support test, certification, acquisition, connection, and operation of UC devices.

It fulfills the requirements specified in DoD Instruction (DoDI) 8100.04 for the development of a UC requirements document.

UCR 2013, Errata Table

SECTION	ERRATA #	REQ-ID	CORRECTION	EFFECTIVE DATE
2	1	SCM-000190	Requirement deleted – redundant to SCM-000210.	Immediate
2	1	SCM-000990.a	In Section 2.6.1.1, corrected requirement identifier to SCM-001180.a	Immediate
2	1	SCM-00180.a	In Section 2.6.1.1, corrected requirement identifier to SCM-001180.b	Immediate
2	1	SCM-001660	Changed "SC" in requirement text to "SS sending the OPTIONS request."	Immediate
2	1	SCM-001780	Removed PEI and AEI from requirement marking and added new requirement similar to SCM-001780 applicable to PEI and AEI to clarify that 1000-T Mbps Ethernet physical interfaces are not required for PEI and AEI.	Immediate
2	1	SCM-000190	Requirement deleted – redundant to SCM-000210.	Immediate
2	1	SCM-00178x	New requirement. Please see Correction entry for SCM-001780.	Immediate
2	1	SCM-001890, SCM-001900	Changed (10/100 Ethernet) to (10/100/1000 Ethernet).	Immediate
2	1	SCM-001940-SCM-001970	Changed [Required: Voice EI] to [Required: PEI, AEI].	Immediate
2	1	SCM-001980	Requirement deleted – EI multiple line appearance requirements appears in Section 2. 9.7	Immediate
2	1	SCM-002040	Made changes to clarify required vs. optional announcements. Changes include revisions to Table 2.9-3, Required Announcements, a new Conditional requirement applicable to optional announcements, the addition of Table 2.9-4, Optional Announcements, and the deletion of requirement SCM-002050.	Immediate
2	1	SCM-00204x	New requirement. Please see Correction entry for SCM-002040.	Immediate
2	1	SCM-002050	Requirement deleted. See Correction entry for SCM-002040.	Immediate
2	1	SCM-002560	Changed requirement for SC to support AS-SIP voice EI from Required to Optional. Changed [SC, SS] to [SC].	Immediate
2	1	SCM-002590	Requirement for SC to track and limit number of simultaneous calls at an AS-SIP voice EI deleted, to be consistent with AS-SIP 2013 requirements.	Immediate
2	1	SCM-002600	Requirement was deleted. Please see Correction entry for SCM-002590.	Immediate
2	1	SCM-002610	Changed requirement for SC to support AS-SIP secure voice EI from Required to Optional. Changed [SC, SS] to [SC].	Immediate

SECTION	ERRATA #	REQ-ID	CORRECTION	EFFECTIVE DATE
2	1	SCM-002750	Changed requirement for SC to support AS-SIP video EI from Required to Optional. Changed [SC, SS] to [SC].	Immediate
2	1	SCM-002810	Requirement for SC to track and limit number of simultaneous calls at an AS-SIP video EI was deleted, in order to be consistent with AS-SIP 2013 requirements.	Immediate
2	1	SCM-003220 through SCM-003290	Revisions made to introductory text in Section 2.9, End Instruments, and Section 2.9.10, ROUTINE-Only EIs, to clarify that ROUTINE-only EIs can use either AS-SIP or proprietary signaling.	Immediate
2	1	SCM-003230	Requirement deleted. Explanatory note added to SCM-003220 to clarify that an SC that supports ROUTINE-only video EIs is not required to support video EIs that fully support precedence and preemption.	Immediate
2	1	SCM-003250	Requirement that a precedence call to a ROUTINE-only EI be immediately diverted by the SC to an attendant has been qualified to apply to calls to ROEIs that use proprietary signaling.	Immediate
2	1	SCM-003255	Optional SC requirement added to immediately divert precedence call to a ROUTINE-only EI that uses AS-SIP signaling.	Immediate
3	1	AUX-006390	Changed from Required to Conditional.	Immediate
3	1	AUX-006400	Changed from Required to Conditional.	Immediate
3	1	AUX-006410	Changed from Required to Conditional.	Immediate
3	1	AUX-006440	Changed from Required to Conditional.	Immediate
3	1	AUX-006450	Changed from Required to Conditional.	Immediate
3	1	AUX-006460	Changed from Required to Conditional.	Immediate
3	1	AUX-006510	Changed CP MG and CP SBC from Required to Conditional.	Immediate
3	1	AUX-006540	Changed CP MG and CP SBC from Required to Conditional.	Immediate
3	1	AUX-006550	Changed CP MG and CP SBC from Required to Conditional.	Immediate
3	1	AUX-006560	Changed CP MG and CP SBC from Required to Conditional.	Immediate
3	1	AUX-006570	Changed CP MG and CP SBC from Required to Conditional.	Immediate
3	1	AUX-006580	Changed CP MG and CP SBC from Required to Conditional.	Immediate
3	1	AUX-006590	Changed CP MG and CP SBC from Required to Conditional.	Immediate
3	1	AUX-006710	Changed Requirement from Optional to Conditional	Immediate
3	1	AUX-006720	Changed Requirement from Optional to Conditional	Immediate
3	1	AUX-006730	Changed Requirement from Optional to Conditional	Immediate
3	1	AUX-006740	Changed Requirement from Optional to Conditional	Immediate
3	1	AUX-006750	Changed Requirement from Optional to Conditional	Immediate

SECTION	ERRATA #	REQ-ID	CORRECTION	EFFECTIVE DATE
3	1	AUX-006760	Changed Requirement from Optional to Conditional / Optional	Immediate
3	1	AUX-006770	Changed Requirement from Optional to Conditional	Immediate
3	1	AUX-006780	Changed Requirement from Optional to Conditional	Immediate
3	1	AUX-006790	Changed Requirement from Optional to Conditional	Immediate
3	1	AUX-006800	Changed Requirement from Optional to Conditional	Immediate
3	1	AUX-006810	Changed Requirement from Optional to Conditional	Immediate
3	1	AUX-006820	Changed Requirement from Optional to Conditional	Immediate
3	1	AUX-006830	Changed Requirement from Optional to Conditional	Immediate
3	1	AUX-006840	Changed Requirement from Optional to Conditional	Immediate
3	1	AUX-006870	Changed Requirement from Optional to Conditional	Immediate
3	1	AUX-006880	Changed Requirement from Optional to Conditional; Removed CP MG.	Immediate
3	1	AUX-006890	Changed Requirement from Optional to Conditional; Removed CP MG.	Immediate
3	1	AUX-006900	Changed Requirement from Optional to Conditional	Immediate
3	1	AUX-006910	Changed Requirement from Optional to Conditional; Removed CP MG	Immediate
3	1	AUX-006920	Changed Requirement from Optional to Conditional; Removed CP MG	Immediate
	1	AUX-006930	Changed Requirement from Optional to Conditional; Removed CP MG	Immediate
3	1	AUX-006940	Changed Requirement from Optional to Conditional	Immediate
4	1	IA-005000−IA-008020	Requirement applicability statement changed to remove WIDS from the role based access control requirements. Removed the generic “Security Device” or “SD” from the applicability statement and added FW, VPN, IPS, and NAC.	Immediate
4	1	IA-016000	Changed requirement to reflect that the minimum version of NTP for which interoperability must be maintained is NTPv3, even if higher versions of NTP are supported.	Immediate
4	1	IA-065000	Added clarification to the requirement as follows: (Reference Appendix A of RFC 2409 for the definition of 'Class Value 2').	Immediate
4	1	IA-067000	Requirement IA-067000 was removed.	Immediate
4	1	IA-071020	Requirement IA-071020 was removed.	Immediate
4	1	IA-071080	Requirement IA-071080 was removed.	Immediate
4	1	IA-074080	Requirement IA-074080 was removed.	Immediate
4	1	IA-074090	Requirement IA-074090 was removed.	Immediate
5	1	IP6-000050	Added note to bound the feature parity to the functionality tested by the distributed test lab test procedures for the product category.	Immediate
7	1	EDG-000020	Reduced Core interface requirements from 100 and 1000 Mbps to 1000 mbps.	Immediate

SECTION	ERRATA #	REQ-ID	CORRECTION	EFFECTIVE DATE
7	1	EDG-000080	Clarified auto-negotiation.	Immediate
7	1	EDG-000150	Added plus or minus 10 percent to variation	Immediate
7	1	EDG-000170	Clarified which MIBs need to be supported.	Immediate
7	1	EDG-000600	Clarified auto-negotiation.	Immediate
7	1	EDG-000630	Clarified which MIBs need to be supported.	Immediate
7	1	EDG-000650	Changed Link Layer Discover – Media Endpoint Discovery Optional: PON.	Immediate
7	1	EDG-001030	Clarified IPv6 requirements for PON.	Immediate
7	1	EDG-001020	Changed PON faiover to 5 seconds to match rest of LAN	Immediate
7	1	EDG-001160	Increased CER latency for T1/E1 to match UCR 2008.	Immediate
8	1	N/A	Mobile Device Manager was redefined to be Mobile Device Manangment for consistency with DISA MDM SRG.	N/A
9	1	VDS-000540	Changed "Move, Add and Change (MAC) address" to “MAC Address” as the acronym is reflective of the hardware interface.	Immediate
9	1	VDS-000550	Changed from Required to Optional since most signal extenders are designed to not modify signaling.	Immediate
9	1	VDS-000560	Removed the descriptive text from the requirement in order to specify a required feature and not dictate how the feature should be implemented.	N/A
9	1	VDS-000570	Requirement reworded in order to specify a required feature and not dictate how the feature should be implemented.	Immediate
10	1	NI-001065	Added requirement for transponders to support OC-758/STM-256 or OTU.3.	18-Month
10	1	NI-001465	Added requirement for framed wavelength services supported for 40 (ITU-T Recommendation G.709) and 100 Gbps (OTU4 (ITU-T Recommendation G.709 standard) signals.	18-Month
10	1	NI-010590	Changed RFC 5925 to 2385.	Immediate
13	1	SEC-000020	Requirement changed to say interoperability with NTP3 is necessary.	Immediate
13	1	SEC-000080	Requirement only applicable to FW. Removed requirement for IPS and WIDS.	Immediate
13	1	SEC-000240 SEC-000250	Requirements only applicable to FW. Removed requirement for IPS and VPN.	Immediate
Appendix A	1	TAC-001510	Clarified language.	Immediate

TABLE OF CONTENTS

LIST OF FIGURES

LIST OF TABLES

SECTION 1
INTRODUCTION

1.1 PURPOSE

The Department of Defense (DoD) Unified Capabilities Requirements (UCR) 2013 specifies the technical requirements for certification of approved products to be used in DoD networks to provide end-to-end Unified Capabilities (UC).

This document supersedes UCR 2008, Change 3.

The UCR specifies the functional requirements, performance objectives, and technical specifications for DoD networks that support UC, and shall be used to support test, certification, acquisition, connection, and operation of these devices. It may also be used for UC product assessments and/or operational tests for emerging UC technology. The Defense Information Systems Agency (DISA) translates DoD Component functional requirements into engineering specifications for inclusion into the UCR that identify the minimum requirements and features for UC applicable to the overall DoD community. The UCR also defines interoperability, Information Assurance, and interface requirements among products that provide UC. It provides a common language and reference for DoD Components' implementation of UC technology, supports implementation of DoD Component solutions, and directs adherence to common standards and specifications to support the Department's Joint Information Environment goal of establishing effective, secure, and common UC.

The UCR is based on commercial off-the-shelf (COTS) products' features, standards listed in the DoD Information Technology Standards Registry (DISR), and unique requirements needed to support DoD mission-critical needs.

1.2 APPLICABILITY

Per DoD Instruction (DoDI) 8100.04, the UCR applies to the following:

1. The Office of the Secretary of Defense (OSD), the Military Departments (MILDEPs), the Office of the Chairman of the Joint Chiefs of Staff (CJCS) and the Joint Staff (JS), the Combatant Commands (COCOMs), the Office of the Inspector General of the DoD, the Defense Agencies, the DoD Field Activities, and all other organizational entities within the DoD (hereafter referred to collectively as the "DoD Components").
2. DoD Component planning, investment, development, acquisition, operations, and management of DoD networks to support UC, independent of the mix of technologies (e.g., circuit-switched and/or Internet Protocol [IP]), and whether converged or non-converged, including all equipment or software (hereafter referred to as "UC products" or "products") and services that provide or support UC, during each phase of those products' life cycles, from acquisition to operations.
3. Acquisition of services is described in DoD Directive (DoDD) 5000.01 and DoDI 5000.02.

1.3 UC DEFINITION

Unified Capabilities are the integration of voice, video, and/or data services delivered ubiquitously across a secure and highly available network infrastructure, independent of technology, to provide increased mission effectiveness to the warfighter and business communities.

1.4 SCOPE OF DOCUMENT

The UCR consists of the following 15 sections and three appendices:

- Section 1, Introduction, addresses the purpose, applicability, and overview of the UCR.
- Section 2, Session Control Products, addresses UC products that perform Session Control functions for Defense Information Systems Network (DISN) Voice over IP (VoIP) and Video over IP services.
- Section 3, Auxiliary Services, addresses the required functionality, performance, capabilities, and associated technical parameters for Auxiliary Services and Systems.
- Section 4, Information Assurance, defines the interoperability focused Information Assurance requirements for UC products.
- Section 5, IPv6, describes the IPv6 requirements for Sensitive but Unclassified (SBU) UC subsets provided by all products and technologies used to send and receive or to support voice, video, or data across DoD networks that provide UC services.
- Section 6, Network Infrastructure End-to-End (E2E) Performance, focuses on the wide area network (WAN) performance characteristics for Layer 3 routers and switches used in the E2E UC network infrastructure. It defines the Differentiated Services Code Point (DSCP) Plan, Per-Hop Behavior (PHB) policy and priority as applied to packets based on the granular service class when traversing a DISN network hop, and traffic conditioning treatment requirements that are to be given to network queues.
- Section 7, Network Edge Infrastructure, defines technical requirements for the products used in configuring the network edge infrastructure.
- Section 8, Multifunction Mobile Devices, addresses the requirements for an array of mobile devices and their associated supporting infrastructure elements. These devices provide network access through primarily wireless means, though wired connectivity may also be a feature of these products. A Multifunction Mobile Device (MMD) can assume any number of form factors including, but not limited to, a smartphone, Personal Digital Assistant (PDA), or small form factor wireless tablet.
- Section 9, Video Distribution System, defines requirements for a complement of audio and video equipment designed for interfacing, switching/bridging, and distributing digital and/or analog audio and video signals sourced from multiple devices and destined to multiple devices.

- Section 10, Network Infrastructure Products, defines requirements for products used in the DISN backbone network infrastructure.
- Section 11, Network Elements, defines requirements that must be met by DISN Fixed network element (F-NE) and Deployed network element (D-NE) devices.
- Section 12, Generic Security Devices, defines high-level requirements for encryption products.
- Section 13, Security Devices, defines requirements for security devices including firewalls, Intrusion Protection Systems (IPSs), Network Access Control, and Virtual Private Network (VPN) devices.
- Section 14, Online Storage Controller, defines requirements for Data Storage Controller (DSC) systems.
- Section 15, Enterprise and Network Management Systems, defines general requirements for enterprise and network management systems.
- Appendix A, Unique Deployed (Tactical), contains requirements unique to tactical (deployed) systems.
- Appendix B, Unique Classified Unified Capability, contains requirements unique to Classified systems.
- Appendix C, Glossary of Abbreviations and Acronyms, contains the acronyms applicable to the UCR.

1.5 UCR 2013 DOCUMENT SUITE

This specification is one of several DoD documents that specify requirements for Assured Services networks and requirements for products to achieve DoD UC Approved Products List (APL) certification. The UC requirements documents that are included in the UCR scope are shown in Figure 1.5-1 and include the following.

- UCR 2013: specifies the functional requirements, performance objectives and technical specifications.
- Assured Services – Session Initiation Protocol (AS-SIP) 2013: contains the requirements for the IP-based UC Signaling system.
- UC XMPP 2013: contains the requirements for multivendor interoperability as required to exploit the full potential of Instant Messaging (IM), Chat, and Presence across DoD.
- UC Framework 2013: specifies the descriptive text and design associated with each of the UCR 2013 sections.

The reference documents used are cited in UC Framework 2013, Appendix C, Definitions, Abbreviations and Acronyms, and References.

Figure 1.5-1. UCR 2013 Document Suite

1.6 APPLICABLE STANDARDS

The standards used in this section are provided in UC Framework 2013, Appendix C, Definitions, Abbreviations and Acronyms, and References.

1.7 GENERAL REQUIREMENT LANGUAGE

The words "REQUIRED," "MUST," or "SHALL" mean that the definition is an absolute requirement of the product.

The word "CONDITIONAL" means a requirement is dependent on a condition. The text of a CONDITIONAL requirement may use the "If <condition>, then <requirement>" format. An example of a CONDITIONAL requirement is "If the system provides authentication via the SIP digest method, then the SIP digest implementation shall be in accordance with RFC 3261."

The phrases "MUST NOT" or "SHALL NOT" mean that the definition is an absolute prohibition of the item.

The word "RECOMMENDED" means that the reference is given as guidance and is not required to be tested. (This word is applicable to the AS-SIP and XMPP protocol requirements only.)

The word "OPTIONAL" means that the item or feature may or may not be used by a product when installed in the field. Optional requirements are features and capabilities that are not considered critical for DoD mission support based on DoD policies. Nevertheless, it is recognized that such features do have utility for some users or for specific operations. To ensure interoperability and consistency of the Assured Services across all platforms, these features and capabilities are specified with set parameters. If these features and capabilities are provided, then the UC product shall perform and meet the requirements as identified in the UCR.

1.7.1 Product Applicability

This document identifies the minimum functional and performance requirements for products to be placed on the UC APL.

1.8 DEFINITIONS

Definitions are found in UC Framework 2013, Appendix C, Definitions, Abbreviations and Acronyms, and References.

SECTION 2
SESSION CONTROL PRODUCTS

2.1 INTRODUCTION

This section addresses Assured Services (AS) products that perform Session Control functions for Defense Information Systems Network (DISN) Voice over Internet Protocol (IP) (VoIP) and Video over IP services. UC product requirements include not just the Session Control requirements described in this section, but also Information Assurance (IA), various protocol requirements (e.g., AS Session Initiation Protocol [SIP] [AS-SIP], IP version 6 [IPv6]), and requirements tailored to unique deployment situations; those requirements are described in separate sections of the Unified Capabilities Requirements (UCR) or other UC-related documents as described in Section 1. The primary products that involve Session Control include Session Controllers (SCs), Softswitches (SSs), and End Instruments (EIs).

An AS-SIP End Instrument (AEI) is an EI that interfaces with a Session Controller using AS-SIP. A Proprietary End Instrument (PEI) interfaces with a Session Controller using proprietary Voice and Video over IP (VVoIP) signaling.

Although not considered primary Session Control products, AS-SIP Gateways, Session Border Controllers (SBCs), and the UC Stateful Firewall also have requirements in support of Session Control and session quality.

Session Control requirements are described in terms of appliance functions associated with the Session Control products; these include the Call Connection Agent (CCA), Media Gateway (MG), Network Management (NM), and Assured Services Admission Control (ASAC).

How the various UC products are deployed within the network is described in the companion document entitled UC Framework 2013.

2.2 VOICE FEATURES AND CAPABILITIES

This section describes Assured Services capabilities and characteristics together with the design and performance metrics associated with each capability or characteristic. For brevity, the rationale behind the selected metrics is not provided in this section, but references to other sections and documents are provided where available. The Government retains the right to change, modify, or alter any of the specified capabilities or characteristics and performance metrics as requirements and technology mature. Table 2.2-1, Assured Services Product Features and Capabilities, summarizes the product features and capabilities.

Table 2.2-1. Assured Services Product Features and Capabilities

	FEATURE AND CAPABILITY	UCR SECTION	REFERENCE DOCUMENT
1	Precedence Call (Session) Waiting	2.2.3	Telcordia Technologies GR-571-CORE Telcordia Technologies GR-572-CORE
2	Call (Session) Forwarding	2.2.1	Telcordia Technologies GR-217-CORE Telcordia Technologies GR-580-CORE Telcordia Technologies GR-586-CORE
3	Call (Session) Transfer	2.2.4	
4	Call (Session) Hold	2.2.5	
5	UC Conferencing	3.4	
6	Three-Way Calling	2.2.6	
7	Hotline Service	2.2.7	
8	Calling Number Delivery	2.2.8	Telcordia Technologies GR-317-CORE
9	Call Pick-Up	2.2.9	Telcordia Technologies GR-590-CORE

It is expected that all Assured Services products, such as SCs and SSs, will support vendor-proprietary VVoIP features and capabilities, in addition to supporting the required VVoIP features and capabilities that are listed in Table 2.2-1, Assured Services Product Features and Capabilities.

SCM-000010 [**Required: PEI, SC, SS**] The Assured Services product's support for these vendor-proprietary VVoIP features and capabilities shall not adversely affect the required operation of the MLPP or ASAC features on that product. The required operation of the MLPP and ASAC features is specified in Section 2.25.1, Multilevel Precedence and Preemption; this section; and AS-SIP 2013.

In addition, vendor-proprietary VVoIP features and capabilities on Assured Services products shall work with and interact with these MLPP and ASAC features, so that all the UCR requirements for MLPP and ASAC are still met. A vendor-proprietary VVoIP feature or capability shall not cause the MLPP feature to fail, and it shall not cause the ASAC feature to fail.

2.2.1 Call Forwarding

Call Forwarding (CF) allows for incoming calls to a given line—or Directory Number (DN)—to be redirected to another DN, contingent upon feature activation and possibly other conditions. The forwarded-to DN may be any telephone number, subject to the CoS restrictions of the DN activating the feature. Calls forwarded to DNs that have a call forwarding feature already activated may be forwarded again.

Four types of Call Forwarding features are considered for UC:

- Call Forwarding Variable (CFV).
- Call Forwarding Busy Line (CFBL).
- Call Forwarding – Don't Answer – All Calls (CFDA).
- Selective Call Forwarding (SCF).

Call forwarding interaction with Multilevel Precedence and Preemption (MLPP) is Optional.

SCM-000020 [**Conditional: PEI, AEI, SC, SS**] If a call forwarding feature that does not support interaction with MLPP is activated or configured for a given DN, incoming calls to that DN at PRIORITY or above precedence shall not be forwarded, and shall be processed as if the call forwarding feature is not active or configured.

SCM-000030 [**Optional: PEI, AEI, SC, SS**] Reminder Ring for all call forwarding features, as specified in accordance with (IAW) Telcordia Technologies GR-217-CORE, GR-580-CORE, and GR-586-CORE, shall be supported. The UC requirements for Reminder Ring are optional.

2.2.1.1 Call Forwarding Variable

When the CFV feature is active for a given user's DN, calls intended for that DN are redirected to a user-specified DN (Defense Switched Network [DSN] Number or commercial). A user can activate and deactivate CFV for his DN, and specifies the desired terminating DN during each activation. Users cannot answer calls at a DN for which CFV is active, but can originate calls at that DN.

SCM-000040 [**Required: PEI, AEI, SC, SS**] CFV shall be supported IAW Telcordia Technologies GR-580-CORE.

SCM-000050 [**Optional: PEI, AEI, SC, SS**] CFV shall interact with MLPP IAW Section 2.2.2.1, Call Forwarding at a Busy Station.

2.2.1.2 Call Forwarding Busy Line

When Call Forwarding Busy Line (CFBL) is configured for a given DN, calls intended for that DN are redirected to a configured DN when the former DN is busy.

SCM-000060 [**Required: PEI, AEI, SC, SS**] CFBL shall be supported IAW Telcordia Technologies GR-586-CORE.

SCM-000070 [**Optional: PEI, AEI, SC, SS**] CFBL shall interact with MLPP IAW Section 2.2.2.1, Call Forwarding at a Busy Station.

2.2.1.3 Call Forwarding – Don't Answer – All Calls

Calls to DNs configured with CFDA that are not answered after a user-specified number of ringing cycles are redirected to a configured DN.

NOTE: If the DN to which unanswered calls are forwarded is busy, the original DN continues to ring until the originator of the call abandons it or the call is answered.

SCM-000080 [**Required: PEI, AEI, SC, SS**] CFDA shall be supported IAW Telcordia Technologies GR-586-CORE.

SCM-000090 [**Optional: PEI, AEI, SC, SS**] CFDA shall interact with MLPP IAW Section 2.2.2.1, Call Forwarding at a Busy Station, and Section 2.2.2.2, Call Forwarding – No Reply at Called Station.

2.2.1.4 Selective Call Forwarding

SCF allows users to forward calls from selected, user-specified calling parties identified by DNs on a screening list. Support for SCF is optional.

SCM-000100 [**Conditional: PEI, AEI, SC, SS**] If SCF is supported, it shall be provided IAW Telcordia Technologies GR-217-CORE.

SCM-000110 [**Optional: PEI, AEI, SC, SS**] SCF shall interact with MLPP IAW Section 2.2.2.1, Call Forwarding at a Busy Station, and Section 2.2.2.2, Call Forwarding – No Reply at Called Station.

2.2.2 MLPP Interactions With Call Forwarding

SCM-000120 [**Conditional: PEI, AEI, SC, SS**] If a call is forwarded by a CF feature that supports MLPP, the precedence level of the call shall be preserved during the forwarding process.

2.2.2.1 Call Forwarding at a Busy Station

SCM-000130 [**Conditional: PEI, AEI, SC, SS**] If a called DN has a CF feature active or configured that supports MLPP:

a. If the incoming call is of a higher precedence level than the established call (or calls, if Three-Way Calling (TWC) is established) at the busy DN being called, then all calls to the busy DN shall be preempted and the incoming call shall be established, i.e., the CF feature shall not be invoked.

b. If the incoming call is of an equal or lower precedence level than the established call (or calls, if TWC is established) at a busy DN being called, then the CF feature shall be invoked.

c. If the called IMMEDIATE/PRIORITY (I/P) user, FLASH/FLASH OVERRIDE (F/FO) user, or other UC user is non-preemptable (i.e., is not classmarked for preemption), then the CF feature shall be invoked regardless of the precedence levels of incoming calls and established calls.

d. The precedence level of calls shall be preserved during the forwarding process.

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

2.2.2.2 Call Forwarding – No Reply at Called Station

SCM-000140 [**Conditional: PEI, AEI, SC, SS**] If a called DN has a CF feature active or configured that supports MLPP, then the precedence level of calls shall be preserved during the forwarding process, and the forwarded-to user may be preempted.

SCM-000150 [**Conditional: PEI, AEI, SC, SS**] If a called DN has a CF feature active or configured that supports MLPP and if a precedence call (i.e., PRIORITY and above) is forwarded (including possible multiple forwarding) and is not responded to by any forwarded-to party (e.g., called party busy with a call of equal or higher precedence level, or called party busy and non-preemptable) within a specified period (e.g., 30 seconds), then the call shall be diverted to an attendant.

2.2.3 Precedence Call Waiting

SCM-000160 [**Required: PEI, AEI, SC, SS**] The following Precedence Call Waiting (CW) treatment shall apply to precedence levels of PRIORITY and above.

2.2.3.1 Busy With Higher Precedence Call

SCM-000170 [**Required: PEI, AEI, SC, SS**] If the precedence level of the incoming call is lower than the existing MLPP call, Precedence CW shall be invoked. If the incoming call is PRIORITY precedence or above, the Precedence CW tone (see Table 2.9-2, UC Information Signals) shall be applied to the called party.

2.2.3.2 Busy With Equal Precedence Call

SCM-000180 [**Required: PEI, AEI, SC, SS**] The End Instrument (EI) shall provide the Precedence CW tone (see Table 2.9-2, UC Information Signals) to the called user. The EI shall apply this tone regardless of other programmed features, such as CF on busy or caller ID. The called EI shall be able to place the current active call on hold, or disconnect the current active call and answer the incoming call.

2.2.3.3 Busy With Lower Precedence Call

SCM-000190 [**Removed** see SCM-000210~~**Required: PEI, AEI, SC, SS**~~] ~~The UC appliance shall preempt the active call. The active busy station EI shall receive continuous preemption tone until an "on-hook" signal is received and the other party on the preempted call shall receive a preemption tone for a minimum of 3 seconds. After going "on-hook," the EI to which the precedence call is directed shall be provided precedence ringing. The EI shall be connected to the preempting call after going "off-hook."~~

2.2.3.4 No Answer

SCM-000200 [**Required: PEI, AEI, SC, SS**] If, after receiving the Precedence CW signal, the busy called EI does not answer the incoming UC call within the maximum programmed time interval, then the SC/SS shall treat the call IAW Section 2.2.10, Precedence Call Diversion.

2.2.3.5 Line Active With a Lower Precedence Call

SCM-000210 [**Required: PEI, AEI, SC, SS**] Precedence calls arriving at a busy EI that is classmarked as preemptable shall preempt the active lower precedence call. The active busy EI shall receive a continuous preemption tone until an "on-hook" signal is received and the other party shall receive a preemption tone for a minimum of 3 seconds (see Table 2.9-2, UC Information Signals). After going "on-hook," the station to which the precedence call is directed shall be provided precedence ringing (see Table 2.9.1, UC Ringing Tones and Cadences). The station shall be connected to the preempting call after going "off-hook."

If CW is ~~invoked~~ enabled on the terminating DN, it shall ~~be ignored~~not be invoked and the existing lower precedence call shall be preempted.

2.2.3.6 Call Waiting for Single Call Appearance VoIP Phones

The Precedence CW feature is for single-call-appearance VoIP phones, Analog Terminal Adapters (ATAs), and Integrated Access Devices (IADs) only. It is not a feature for multiple-call-appearance VoIP phones. Multiple-call-appearance phones already support the Precedence CW functionality since there is an active call on Call Appearance 1 (CA 1) and a "waiting call" on CA 2, or an active call on CA 2 and a held call on CA 1.

2.2.4 Call Transfer

SCM-000220 [**Required: PEI, AEI, SC, SS**] Two types of call transfers are normal and explicit. A normal call transfer is a transfer of an incoming call to another party. An explicit call transfer happens when both calls are originated by the same subscriber. The UC signaling appliance shall provide the interactions described in the following paragraphs, with both normal and explicit call transfers.

2.2.4.1 Call Transfer Interaction at Different Precedence Levels

SCM-000230 [**Required: PEI, AEI, SC, SS**] When a call transfer is made at different precedence levels, the SC/SS that initiates the transfer shall classmark the connection at the highest precedence level of the two segments of the transfer.

2.2.4.2 Call Transfer Interaction at Same Precedence Levels

SCM-000240 [**Required: PEI, AEI, SC, SS**] The SC/SS ~~Service (SCS)~~ that initiates a call transfer between two segments that have the same precedence level shall maintain the precedence level upon transfer.

2.2.5 Call Hold

SCM-000250 [**Required: PEI, AEI, SC, SS**] Call Hold is a function of the serving UC signaling appliance system and shall be invoked by going "on-hook," then "off-hook." Calls on hold shall retain the precedence of the originating call.

Figure 2.2-1, Call Hold Scenarios, illustrates three typical call hold scenarios. In each scenario, caller #3 is on hold with caller #1, and caller #1 is talking to caller #2.

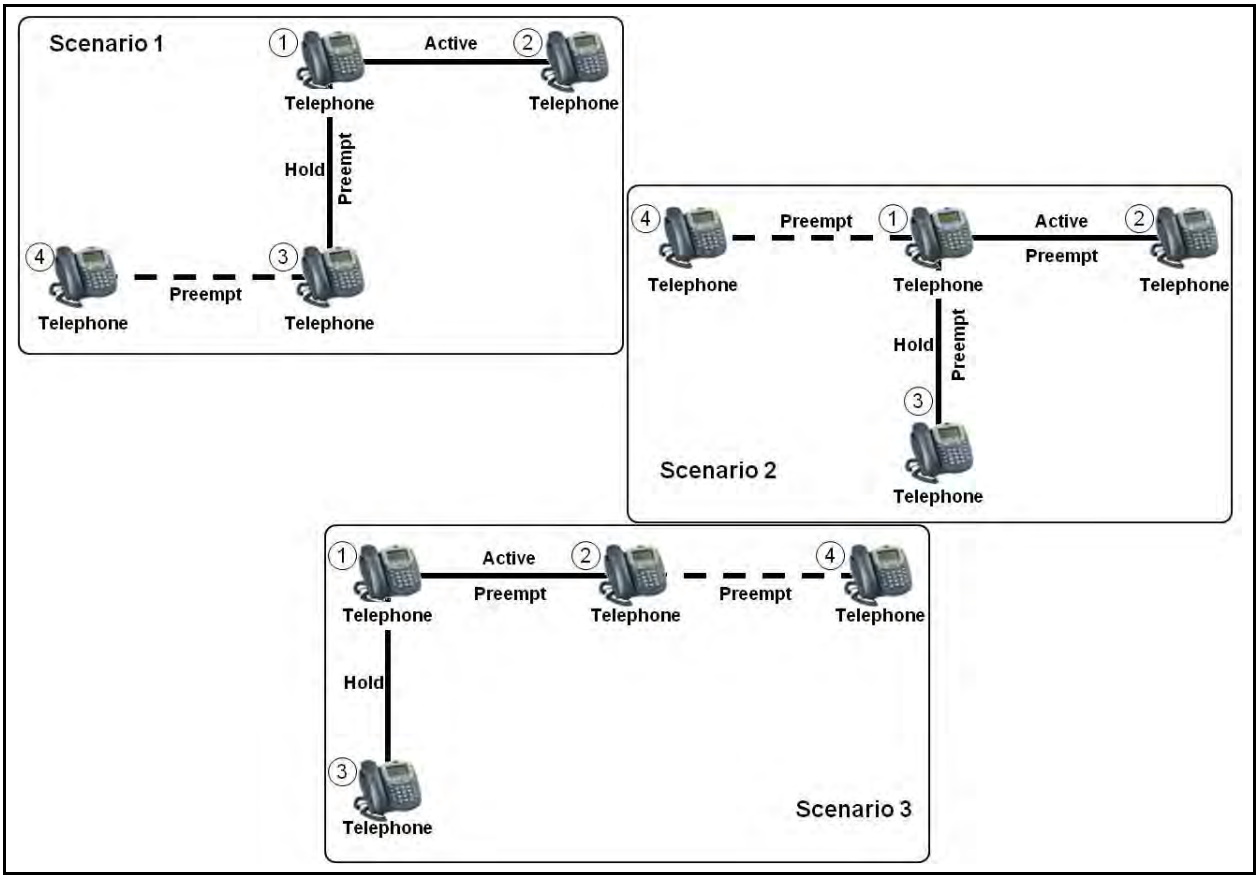


Figure 2.2-1. Call Hold Scenarios

In scenario 1, caller #3 receives an incoming, higher precedence call from caller #4. Caller #3 receives a preemption tone. After caller #3 acknowledges the preemption tone by going "on hook," the call between caller #4 and caller #3 is established when caller #3 answers caller #4. Caller #1 will receive a preemption tone also only if caller #1 attempts to retrieve caller #3 while the preemption tone is being sent to caller #3.

(NOTE: The preemption tone shall not be sent to caller #1 while active with caller #2. This would give caller #1 the false indication that the active call with caller #2 is being preempted.)

Caller #2 remains connected to caller #1, and caller #1 does not receive any preemption notification.

In scenario 2, caller #1 receives an incoming, higher precedence call from caller #4. Caller #1, caller #2, and caller #3 receive a preemption tone (see Table 2.9-2, UC Information Signals). After caller #1 acknowledges the preemption and then goes "on hook," the higher precedence call from caller #4 is offered. Callers #2 and #3 are disconnected and the call between caller #4 and caller #1 is established.

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

2.2.6 Three-Way Calling

SCM-000260 [**Required: PEI, AEI, SC, S**S] In TWC, each call shall have its own precedence level. When a three-way conversation is established, each connection shall maintain its assigned precedence level. Each connection of a call resulting from a split operation shall maintain the precedence level that it was assigned upon being added to the three-way conversation.

SCM-000270 [**Required: PEI, AEI, SC, S**S] The SC/SS shall classmark the originator of the three-way call at the highest precedence level of the two segments of the call. Incoming calls to lines participating in TWC that have a higher precedence than the higher of the two segments shall preempt unless the call is marked non-preemptable.

SCM-000280 [**Required: PEI, AEI, SC, S**S] When a higher precedence call is placed to any one of the three-way call participants (including the originator), that participant shall receive the preemption tone (see Table 2.9-2, UC Information Signals). The other two parties shall receive a conference disconnect tone as described in Table 2.9-2. This tone indicates to the other parties that one of the other three-way call participants is being preempted.

SCM-000290 [**Required: AEI, SC, SS**] When the originator of the three-way call is on an AEI and is being preempted, the other two parties shall be disconnected from the three-way call.

SCM-000300 [**Conditional: PEI, SC, SS**] When the originator of the three-way call is on a PEI and is being preempted, if the TWC bridge is provided by the PEI, the other two parties shall be disconnected from the three-way call.

SCM-000310 [**Conditional, Optional: PEI, SC, SS**] When the originator of the three-way call is on a PEI and is being preempted, if the TWC bridge is provided by the SC or a Media Server, then the other two parties shall remain connected.

2.2.6.1 Three-Way Calling for AEIs and PEIs

SCM-000320 [**Required: AEI**] Three-Way Calling shall be supported by AEIs consistent with AS-SIP 2013, for TWC and the following sections of Request for Comment (RFC) 5359:

> **SCM-000320.a** [**Required: AEI**] Section 2.10, Three-Way Conference – Third Party is Added.
>
> **SCM-000320.b** [**Required: AEI**] Section 2.11, Three-Way Conference – Third Party Joins.

SCM-000330 [**Required: AEI**] The TWC mixer/bridge shall be located in the AEI.

For PEIs, the mixer/bridge can be provided by the PEI, SC, or a Media Server.

2.2.7 Hotline Service

SCM-000340 [**Optional: PEI, TA, IAD, SC – Required: SS**] The Hotline Service shall allow an analog subscriber or user to initiate a voice or data call to a predetermined party automatically by going off hook. The PEI or SC/SS shall dial hotline calls automatically when an "off-hook" condition occurs and the MG outpulses the appropriate routing digit, i.e., "5" for voice and "6" for circuit mode data calls when transported on non-Integrated Services Digital Network (ISDN) circuits. In addition, the hotline information can be carried in the Information Elements on ISDN circuits. Refer to Table 2.2-2, Route Code Assignments.

Table 2.2-2. Route Code Assignments

ROUTE CODE	ROUTE CODE USE
10	Voice Call (default)
11	Circuit-Switched Data
12	Satellite Avoidance (N/A for CAS and Optional for CCS)
13	Reserved
14	Reserved
*5	Hotline (Off-Hook) Voice Grade
*6	Hotline (Off-Hook) Data Grade
17	Reserved

18	Reserved
19	Reserved
* The user does not dial these route codes. The PEI or SC/SS shall dial hotline calls automatically when an off-hook condition occurs and outpulses the appropriate route digit (i.e., hotline voice-5 or hotline data-6).	
LEGEND CAS: Channel-Associated Signaling CCS: Common Channel Signaling N/A: Not Applicable	

SCM-000350 [**Optional: PEI, TA, IAD, SC – Required: SS**] Hotline service shall be allowed for VVoIP end users (on a PEI) or Time Division Multiplexing (TDM) end users (on an analog or ISDN device behind a TA, IAD, or MG).

SCM-000360 [**Optional: PEI, SC – Required: SS**] The PEI or SC/SS shall have the ability to classmark a designated hotline user with a hotline indicator of either voice or data. The PEI or SC/SS also shall have the ability to make optional a hotline user as follows: origination only, termination only, and both origination and termination. Hotline users assigned a hotline indicator of voice shall be allowed to connect only with other hotline users assigned as voice, and hotline users assigned a hotline indicator of data shall be allowed to connect only with other hotline users assigned as data.

The role of the Master SC (MSC) and SS in the hotline requirements is to support hotline calls when they receive AS-SIP, Primary Rate Interface (PRI), or CAS signaling from another appliance that supports hotline. The MG does the interworking of AS-SIP Hotline signaling with Defense Information Systems Agency (DISA) PRI, or CAS Hotline signaling.

2.2.7.1 Protected Hotline Calling

SCM-000370 [**Optional: PEI, SC; Required: SS**] The Hotline Service Protection shall be accomplished within the same UC appliance and outside the serving UC appliance as follows:

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

   (1) Only allowing completion of calls from hotline users found in a specified screening list. (This feature is required only between hotline users on the same UC appliance.)

   (2) The MLPP interaction between hotline users shall be allowed only between hotline users classmarked with the same hotline indicator (i.e., voice or data), as described in Section 2.25.1, Multilevel Precedence and Preemption, with the exception that unanswered hotline calls above ROUTINE precedence will not divert as defined in Section 2.2.10, Precedence Call Diversion. Hotline user calls regardless of precedence level placed between hotline users with unlike hotline indicators (i.e., voice or data) shall receive a Vacant Code Announcement (VCA).

2.2.7.2 Hotline Service Protection

SCM-000380 [**Optional: PEI, SC; Required: MG, SS**] The Hotline Service Protection between a UC appliance and a circuit switch shall be accomplished between hotline users as follows:

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

b. T1 ISDN PRI ANSI T1.619a and E1 ISDN PRI ANSI Q.955.3 Interfaces. The Hotline Service Protection via this interface shall be accomplished by the use of the Optional Off-Hook Indicator parameter in the Setup message. This indicator shall be assigned in Code Set 5 with an element identifier of 01100101 binary (i.e., 65 hexadecimal). The data value within this identifier shall be one of two values: 00000001 (1) for hotline voice or 00000010 (2) for hotline data in Octet 3 as shown in Table 2.2-3. These parameters will correlate directly to Route Digit 5 (voice) or Route Digit 6 (data), respectively. Interaction between Hotline Voice and Hotline Data Indicator parameters via this interface, and voice and data hotline users shall be the same as described in Section 2.2.7.1, Protected Hotline Calling.

Table 2.2-3. Code Set 5 Optional Off-Hook Parameters

8	7	6	5	4	3	2	1	Octet
OPTIONAL OFF-HOOK INFORMATION								**1**
0	1	1	0	0	1	0	1	
ELEMENT IDENTIFIER								
FORMAT DESCRIPTOR								**2**
0	0	0	0	0	0	0	1	
VALUE								**3**
SEE NOTE 1 FOR VALUES.								
NOTE 1. VALUES FOR OCTET 3								
0	0	0	0	0	0	0	1	Voice
0	0	0	0	0	0	1	0	Data

c. E1 ISDN PRI ANSI Q.955.3. The Hotline Service Protection via this interface shall be accomplished by the use of the Optional Off-Hook Indicator parameter in the Setup

message. This indicator shall be assigned in Code Set 5 with an element identifier of 01100101 binary (i.e., 65 hexadecimal). The data value within this identifier shall be one of two values: 00000001 (1) for hotline voice or 00000010 (2) for hotline data. These parameters will correlate directly to Route Digit 5 (voice) or Route Digit 6 (data), respectively. Interaction between Hotline Voice and Hotline Data Indicator parameters via this interface, and voice and data hotline users shall be the same as described in Section 2.2.7.1, Protected Hotline Calling.

SCM-000390 [**Optional: PEI, SC – Required: MG, SS**] Hotline Service Protection interaction between hotline user indicators shall be as depicted in Table 2.2-4, UC Hotline Service Protection Matrix.

Table 2.2-4. UC Hotline Service Protection Matrix

CALLED FROM	CALLED TO	PROTECTION	TREATMENT
Hotline Data User	Hotline Voice User	Denied	VCA
Hotline Data User	Hotline Data User	Allowed	
Hotline Voice User	Hotline Data User	Denied	VCA
Hotline Voice User	Hotline Voice User	Allowed	
Non-Hotline Data User	Hotline Voice User	Denied	VCA
Non-Hotline Voice User	Hotline Voice User	Denied	VCA
Non-Hotline Data User	Hotline Data User	Denied	VCA
Non-Hotline Voice	Hotline Data User	Denied	VCA
LEGEND VCA: Vacant Code Announcement			

SCM-000400 [**Optional: PEI, SC – Required: MG, SS**] The UC Hotline service shall not be allowed to interact with the following services (This restriction shall be applied manually in software or by default when a user is classmarked as a hotline user):

SCM-000400.a [**Optional: PEI, SC – Required: MG, SS**]Hold (EI denied to put call on "HOLD").

SCM-000400.b [**Optional: PEI, SC – Required: MG, SS**]Three way calling.

SCM-000400.c [**Optional: PEI, SC – Required: MG, SS**]Normal call transfer.

SCM-000400.d [**Optional: PEI, SC – Required: MG, SS**]Electronic Key Telephone System (EKTS).

SCM-000400.e [**Optional: PEI, SC – Required: MG, SS**]UC conferencing.

2.2.7.3 Non-Pair Protected Hotline Calling

SCM-000410 [**Optional: PEI, SC – Required: SS**] A Non-Pair Protected Hotline user shall be able to receive calls from any other hotline user with the same hotline indicator (i.e., voice or data) as described in Section 2.2.7.1, Protected Hotline Calling. The Non-Pair Protected Hotline user shall originate calls to a specified destination only, called the Designated Called Party (DCP).

2.2.7.4 Pair Protected Hotline Calling

SCM-000420 [**Optional: PEI, SC – Required: SS**] Pair Protected Hotline users shall be able to call only each other and shall not be allowed to receive calls from a third party. This protection shall be required for intra-UC appliance hotlines. It may be allowed for hotlines between a UC appliance and a circuit switch when end-to-end ISDN is supported between hotline users.

2.2.8 Calling Number Delivery

SCM-000430 [**Required: PEI, AEI, SC, SS**] The calling number provided to the called party shall be determined by the dialing plan used by the calling instrument, IAW Telcordia Technologies GR-31-CORE.

SCM-000440 [**Required: PEI, AEI, SC, SS**] If the incoming call is from another DSN user, the calling number shall be delivered to the called party in 10-digit DSN number format.

SCM-000450 [**Required: PEI, AEI, SC, SS**] If the incoming call is from a commercial user, the calling number shall be delivered to the called party in national or international calling number format.

2.2.8.1 Calling Name Delivery

SCM-000460 [**Optional: PEI, AEI, TA, IAD, SC, SS**] The UC products shall support delivery of Calling Name information to SC end users on incoming UC calls.

2.2.8.2 Calling Party Organization and Location Delivery

SCM-000470 [**Optional: PEI, AEI, TA, IAD, SC**] The UC products shall support delivery of Calling Party Org and Location information (e.g., the caller's military unit and location identity) to SC end users.

2.2.9 Call Pick-Up

SCM-000480 [**Optional: PEI, AEI, SC, SS**] A user EI shall be equipped to answer any calls directed to other EI within the user's own preset pick-up group, as established by an administrative facility, by dialing the appropriate feature code.

Three types of Call Pick-Up features are considered for UC:

a. Basic Call Pick-Up. An EI may answer a call that has been offered to another EI in its common call pick up group in a business group. This is accomplished by dialing a pick-up access code while the called EI is ringing. If more than one EI in the group is ringing, then the EI that has been ringing longer shall be picked up first.

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

c. Directed Call Pick-Up Without Barge-In. This feature is identical to the Directed Call Pick-Up feature, except that if the destination number being picked up has already answered, the party dialing the pick-up code shall be routed to reorder rather than be permitted to barge in on the established connection to create a TWC.

SCM-000490 [**Conditional: PEI, AEI, SC, SS**] If a Call Pick-Up feature is provided, it shall be IAW Telcordia Technologies GR-590-CORE.

SCM-000500 [**Conditional: PEI, AEI, SC, SS**] If a Call Pick-Up feature is provided, it shall interact with MLPP IAW the following:

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

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

2.2.10 Precedence Call Diversion

SCM-000510 [**Required: PEI, AEI, SC**] Precedence Call Diversion shall be supported on calls from one UC EI to another UC EI on the same SC.

SCM-000520 [**Required: PEI, AEI, SC, SS**] Precedence Call Diversion shall be supported on calls from a UC EI on one SC to a UC EI on another SC.

SCM-000530 [**Required: PEI, AEI, SC, SS**] Precedence Call Diversion shall be supported on calls from a UC EI on an SC to a DSN EI (on an End Office [EO], SMEO, Private Branch Exchange [PBX] 1, or PBX 2).

SCM-000540 [**Required: PEI, AEI, SC, SS**] Precedence Call Diversion shall be supported on calls from a DSN EI (on an EO, SMEO, PBX 1, or PBX 2) to a UC EI on an SC.

SCM-000550 [**Required: SC, SS**] The AS-SIP signaling appliance shall divert ALL unanswered UC VoIP calls above the ROUTINE level to a designated DN for PCD (e.g., the number of an attendant console or group of attendant consoles). This diversion shall occur after a specified PCD time period, selectable from 15–45 seconds, and configurable at the per-appliance level

SCM-000560 [**Required: SC, SS**] Unanswered UC VoIP calls above the ROUTINE precedence level shall not be forwarded to voicemail, and shall not be forwarded to ACD systems. Instead, they shall divert to the PCD DN when the PCD time period expires.

SCM-000570 [**Required: SC, SS**] Unanswered UC VoIP ROUTINE calls to DNs that are configured with voicemail or an ACD system shall be forwarded to voicemail or to the ACD system.

SCM-000580 [**Required: SC, SS**] Calls above the ROUTINE precedence level that are directly dialed to DNs assigned to voicemail or ACD systems shall divert to the PCD DN as specified above (i.e., when they are unanswered at the voicemail or ACD system, and the PCD time period expires).

SCM-000590 [**Required: SC, SS**] The AS-SIP signaling appliance shall support a per-appliance configuration option that, when activated, diverts ROUTINE calls directly dialed to DNs assigned to voicemail or ACD systems to the PCD DN, if they go unanswered and the PCD time period expires. These calls shall keep their ROUTINE precedence level after they are diverted by PCD. When this configuration option is not used, unanswered ROUTINE calls shall continue to be offered to the voicemail or ACD system, and shall not be diverted by PCD.

SCM-000600 [**Optional: SC, SS**] During configurable time periods, an announcement that identifies the DSN number of a continuously manned attendant station or console shall be provided to the calling party of a call that would otherwise be diverted to the designated PCD DN. The purpose of this optional requirement is to provide an alternative treatment if there are time periods during which calls to the PCD DN are not expected to be answered.

2.2.11 Public Safety Voice Features

2.2.11.1 Basic Emergency Service (911)

SCM-000610 [**Required: SC, SS**] The Basic 911 Emergency Service feature provides a three-digit universal telephone number (e.g., 911) that gives the public direct access to an emergency service bureau. The emergency service is one way only, terminating to the service bureau. A given local switching system shall serve no more than one emergency service bureau. When the originating line and the emergency service bureau are served by the same switching system, the bureau can hold and disconnect the connection, monitor the supervisory state, and ring the

originating station back. When the local switching system is in an area with enhanced emergency service (E911) served through a tandem switch, the emergency call is advanced to the tandem switch with calling line Automatic Number Identification (ANI) or Calling Number Delivery (CND).

The SC and SS may support 911 services for VoIP and TDM end users. Within the United States, 911 calls from VoIP and TDM lines may be routed either to a DoD Emergency Response Center, or to a PSTN 911 Short Reach (SR) and Public Safety Answering Point (PSAP), depending on the SC or SS configuration. The emergency services network that handles DoD and PSTN 911 calls may be TDM based or IP based. Outside of the United States, 911 calls from VoIP and TDM lines may be routed to a DoD Emergency Response Center (if one exists within the DoD location), depending on the SC or SS configuration.

Calling 911 from an SC or SS shall not require the use of access codes such as 99. Dialing 911 only shall connect to the public emergency service bureau. If this feature is provided, it shall be IAW Telcordia Technologies GR-529-CORE (Functional Specifications Document [FSDs] 15-01-0000, 15-03-0000, 15-07-0000), as interpreted for VoIP calls. This feature does not apply to video calls or sessions.

In the continental United States (CONUS), calls from UC users to 911 are not subject to Multilevel Precedence and Preemption, i.e., 911 calls shall not be preempted. This requirement also applies to 911 calls outside CONUS (OCONUS) from UC users in Hawaii, Alaska, and the U.S. overseas territories (e.g., Guam).

In Europe (EUR), calls from UC users to 112 (the European equivalent of 911) shall not be preempted.

The SC/SS shall allow an administrator to configure a set of phone numbers that when dialed, cannot be preempted.

NOTE: This permits the configuration of an emergency number that cannot be preempted. This set of phone numbers can include 911 (for CONUS locations, and OCONUS U.S. locations), 112 (for EUR locations), and other emergency numbers that are used in an individual Base/Post/Camp/Station (B/P/C/S) or enclave.

See Section 3.6, E911 Management System, for requirements for E911 Management Systems.

2.2.11.2 Tracing of Terminating Calls

SCM-000620 [**Required: SC, SS**] The Tracing of Terminating Calls feature identifies the calling number on intraoffice and interoffice calls terminating to a specified DN. When this feature is activated, the originating DN, the terminating DN, and the time and date are recorded for each call to the specified line.

Requirements for this feature shall be IAW Telcordia Technologies GR 529 CORE, FSD 15-03-0000, as interpreted for VoIP calls.

2.2.11.3 Outgoing Call Tracing

SCM-000630 [**Required: SC, SS**] The Outgoing Call Tracing feature allows the tracing of nuisance calls to a specified DN suspected of originating from a given local office. The tracing is activated when the specified DN is entered. A record of the originating DN, and the time and date, are generated for every call to the specified DN.

Requirements for this feature shall be IAW Telcordia Technologies GR 529 CORE, FSD 15-03-0000, as interpreted for VoIP calls.

2.2.11.4 Tracing of a Call in Progress

SCM-000640 [**Required: SC, SS**] The Tracing of a Call in Progress feature identifies the originating DN for a call in progress. Authorized personnel entering a request that includes the specific terminating DN involved in the call activate the feature.

Requirements for this feature shall be IAW Telcordia Technologies GR 529 CORE, FSD 15-03-0000, as interpreted for VoIP calls.

2.2.11.5 Tandem Call Trace

SCM-000650 [**Optional: SC – Required: SS**] The Tandem Call Trace feature identifies the calling party of a tandem call to a specified office DN. The feature is activated by entering the specified distant office DN for a tandem call trace. When Tandem Call Trace is enabled, a record of the calling party number and terminating DN, and the time and date, shall be generated for every call to the specified DN.

SCM-000660 [**Optional: SC, Required: SS**]The calling party number recorded by the Tandem Call Trace shall be taken from the P-Asserted-Identity, From, or Contact header in the incoming AS-SIP INVITE message for this call. The P-Asserted-Identity header is preferred over the From and Contact headers because the value in the P-Asserted-Identity header is UC-network-validated.

For incoming IP calls that reach the SC/SS enclave via the SBC, the P-Asserted-Identity header should be in the AS-SIP INVITE message. For incoming TDM calls that reach the SC/SS enclave via the MG, if AS-SIP is used between the SC/SS and the MG, the P-Asserted-Identity header should be in the AS-SIP INVITE message.

2.3 ASAC

This section presents the ASAC requirements for the SC and the SS. In the execution of ASAC, certain procedures need to be followed, such as (a) actions to be taken if a precedence session request cannot be completed because existing sessions are at equal or higher precedence, or (b) tones to be generated when a session is preempted. Section 2.25.1, Multilevel Precedence and

Preemption, addresses these issues. AS-SIP 2013 provides a more detailed description of the session control signaling requirements of the SC and the SS.

2.3.1 ASAC Requirements Related to Voice

2.3.1.1 Voice Session Budget Unit

SCM-000670 [**Required: SC, SS**] One voice session budget unit shall be equivalent to 110 kilobits per second (kbps) of access circuit bandwidth independent of the PEI or AEI codec used. This bandwidth equivalent is based on International Telecommunications Union – Telecommunication (ITU-T) Standardization Sector Recommendation G.711 encoding rate plus IPv6 packet overhead plus Assured Services (AS) Local Area Network (ASLAN) Ethernet overhead. IPv6 overhead, not IPv4 overhead, is used to determine bandwidth equivalents here.

2.3.1.2 ASAC States

The terms "inbound" and "outbound" in the context of ASAC requirements are always relative to an SC. An inbound session is one that has been initiated by a PEI or AEI outside a given SC's domain, whereas an outbound session is one that is initiated by a PEI or AEI within a given SC's domain. ASAC requirements involving directionalization are Optional.

SCM-000680 [**Required: SC, SS**] The states that shall be maintained for ASAC purposes are as follows:

SCM-000680.a [**Required: SC**] Line Side States. The SC shall maintain the session state of each local PEI and AEI in its domain as follows:

(1) Busy/Not Busy. The Busy State includes the session setup phase and the active session phase.

(2) Session Precedence. If the PEI or AEI is busy, the state shall include the precedence level of the session (FO, F, I, P, R).

(3) The Line Side States also apply to multi-appearance EIs, but at this time, no more than two line appearances are dealt with, and the procedures are the same as for ISDN Basic Rate Interface (BRI) instruments.

SCM-000680.b Trunk Side States.

SCM-000680.b.1 [**Required: SC, SS**] The SC and its associated SS shall be configurable with the following VoIP Session Budgets:

SCM-000680.b.1.a [**Required: SC, SS**] IP Budget (IPB). The total budget of VoIP sessions plus session attempts in the session setup phase that are allowed on the Customer Edge (CE) Router (CE-R) to Wide Area Network (WAN) IP access link.

SCM-000680.b.1.b [**Optional: SC, SS**] IPBo. The budget for outbound VoIP sessions plus session attempts in the session setup phase that are allowed on the IP access link.

i. IPBo shall take any value in the range (0, IPB) or "null."

ii. Null implies that there are no outbound directionalization restrictions.

SCM-000680.b.1.c [**Optional: SC, SS**] IPBi. The budget for inbound VoIP sessions plus session attempts in the session setup phase that are allowed on the IP access link.

IPBi shall take any value in the range (0, IPB) or "null."

i. Null implies that there are no inbound directionalization restrictions.

ii. Note the relationship among IPB, IPBo, and IPBi:

iii. IPBi plus IPBo equals IPB, if there is directionalization.

iv. IPBi equals null if, and only if, IPBo equals null.

SCM-000680.b.2 [**Required: SC, SS**] The SC and its associated SS shall maintain the following VoIP Session Counts:

SCM-000680.b.2.a [**Required: SC, SS**] IP Count (IPC). The total number of interbase IP sessions in progress plus the number of session attempts in the session setup phase.

SCM-000680.b.2.b [**Optional: SC, SS**] IPCo. The number of outbound IP sessions in progress plus the number of outbound session attempts in the session setup phase.

SCM-000680.b.2.c [**Optional: SC, SS**] IPCi. The number of inbound IP sessions in progress plus the number of inbound session attempts in the session setup phase.

SCM-000680.b.3 [**Required: SC**] A TDM Session Budget (TDMB) shall be configurable on an SC. This amount is the budget for the overall number of TDM sessions plus sessions in the session setup phase on the SC's TDM links. This budget equals the number of digital signal level 0s (DS0s) on the trunk between the SC MG and the EO/SMEO/PBX1/PBX2.

SCM-000680.b.4 [**Required: SC**] The SC shall maintain a TDM Session Count that is the total number of sessions in progress between the TDM switch and the SC's MG, plus the total number of session attempts in the session setup phase.

2.3.1.3 Session Control Processing With No Directionalization

This section considers the functions carried out by the SC and the SS when the Optional directionalization of ASAC budgets is not implemented.

1. SC Processing for an Outbound Session.

SCM-000690 [**Required: SC**] The SC shall take the following actions when an outbound session request is initiated by a local PEI or AEI:

SCM-000690.a [**Required: SC**] Users and/or PEIs and/or AEIs that place sessions shall be authenticated as per Section 4, Information Assurance Requirement, before processing the outbound session.

SCM-000690.a.1 [**Required: SC**] If IPC is less than IPB, the session request shall be forwarded to the SS for forwarding to the sessioned SC for processing (see item 2, SC Processing for an Inbound Session).

SCM-000690.a.2 [**Required: SC**] If IPC equals IPB and all existing sessions are at precedence equal to or greater than the new session request, then the SC shall not place the session, and the caller shall receive a Blocked Precedence Announcement (BPA). If it is a ROUTINE call, the caller shall receive an All Circuits Busy indication as per Table 2.9-2, UC Information Signals.

SCM-000690.a.3 [**Required: SC**] If IPC equals IPB and at least one existing session is of lower precedence than the new session, the SC shall preempt one of the lowest precedence sessions and shall forward the session INVITE (via the SS) to the sessioned SC for processing. The algorithm for selecting the session to preempt shall be deterministic.

SCM-000690.a.4 [**Required: SC**] IPC is greater than IPB is not an allowed state. If this occurs, the SC shall either:

(a) Deterministically preempt sessions starting with those of lowest precedence until IPC equals IPB, and then proceed as specified in items (3) and (4) previously.

(b) Allow the sessions to terminate naturally until IPC equals IPB.

The SC shall notify the Element Management System (EMS) of this fault state.

SCM-000690.a.5 [**Required: SC**] The SC shall increment and decrement its IPC as follows:

(a) The SC increments its IPC upon forwarding a session request to the SS, that it received from its local PEI or AEI.

(b) The SC decrements its IPC upon determining that a session request is completely terminated or an established session is completely terminated.

2. SC Processing for an Inbound Session.

SCM-000700 [**Required: SC**] The SC shall take the following actions when a new inbound session INVITE is received from a remote SC:

SCM-000700.a [**Required: SC**] If IPC is less than IPB and the local PEI or AEI is not busy, then the SC shall place the session.

SCM-000700.b [**Required: SC**] If IPC is less than IPB and the local PEI or AEI is busy with a session that is of lower precedence level than the one being placed, the SC shall preempt the existing session and place the new session.

SCM-000700.c [**Required: SC**] When IPC is less than IPB and the local PEI or AEI is busy with a session that is of an equal or higher precedence level than the session being placed, and the call attempt is at a precedence level above ROUTINE, then if the called EI is a single-call-appearance EI (or ATA or IAD), and Precedence Call Waiting is not assigned to that EI, and Precedence Call Diversion is not activated, then the new session is not placed. The call attempt shall receive a BPA.

SCM-000700.d [**Required: SC**] When IPC is less than IPB and the local PEI or AEI is busy with a session that is of an equal or higher precedence level than the session being placed, and the call attempt is at a precedence level above ROUTINE, then if the called EI is a single-call-appearance EI (or ATA or IAD), and Precedence Call Waiting is not assigned to that EI, but Precedence Call Diversion is activated, then the requirements in Section 2.2.10, Precedence Call Diversion, apply.

SCM-000700.e [**Required: SC**] When IPC is less than IPB and the local PEI or AEI is busy with a session that is of an equal or higher precedence level than the session being placed, and the call attempt is at a precedence level above ROUTINE, then if the called EI is a single-call-appearance EI (or ATA or IAD), and Precedence Call Waiting is assigned to that EI, then the requirements in Section 2.2.3.1, Busy with Higher Precedence Call, apply.

SCM-000700.f [**Required: SC**] When IPC is less than IPB and the local PEI or AEI is busy with a session that is of an equal or higher precedence level than the session being placed, and the call attempt is at a precedence level above ROUTINE, then if the called EI is a multiple-call-appearance EI, then the requirements in Section 2.9.7.3, Multiple Call Appearances – Interactions with Precedence Calls, apply.

SCM-000700.g [**Required: SC**] When IPC is less than IPB, and the new inbound session INVITE is for a ROUTINE call, and the local PEI or AEI is busy, the new session is not placed. The caller shall receive an All Circuits Busy indication as per Table 2.9-2, UC Information Signals.

SCM-000700.h [**Required: SC**] If IPC equals IPB and the local PEI or AEI is not busy, and all existing sessions on the access link are at a precedence level equal to or greater than the new session, the SC shall not place the new session. The caller shall receive a BPA, and if it is a ROUTINE call, the caller shall receive an All Circuits Busy indication as per Table 2.9-2, UC Information Signals.

SCM-000700.i [**Required: SC**] If IPC equals IPB and the local PEI or AEI is not busy, and at least one existing session on the access link is of a lower precedence level than the new session, the SC shall deterministically preempt one of the lowest precedence sessions. Then it shall forward the session INVITE to the sessioned SC via the SS for processing.

SCM-000700.j [**Required: SC**] If IPC equals IPB and the local PEI or AEI is busy with a session that is of a lower precedence level than the new session, then the SC shall preempt the session and forward the session INVITE to the local PEI or AEI.

SCM-000700.k [**Required: SC**] If IPC equals IPB and the local PEI or AEI is busy with a session that is of an equal to or higher precedence level than the new session, the SC shall not place the session. The caller shall receive a BPA, and if it is a ROUTINE call, the caller shall receive an All Circuits Busy indication as per Table 2.9-2, UC Information Signals.

SCM-000700.l [**Required: SC**] The IPC is greater than IPB is not an allowed state. If this occurs, the SC shall deterministically preempt sessions starting with those of the lowest precedence level until IPC equals IPB, and then proceed as specified in items d, e, f, and g. The SC shall notify the EMS of this fault state.

SCM-000710 [**Required: SC**] The SC shall increment and decrement its IPC as specified in, AS-SIP 2013.

3. SC Processing for a Local Session.

A local session is one that is initiated by a local PEI or AEI intended for another local PEI or AEI.

SCM-000720 [**Required: SC**] If the sessioned PEI or AEI is not busy, the SC shall complete the session.

SCM-000730 [**Required: SC**] If the sessioned PEI or AEI is busy with a session that is of a lower precedence level than the new session, the SC shall preempt the session, and then complete the new session.

SCM-000740 [**Required: SC**] When the call attempt is at a precedence level above ROUTINE and the local PEI or AEI is busy with a session that is equal to or higher than the precedence level of the new session, then if the called EI is a single-call-appearance EI (or ATA or IAD), the

Precedence Call Waiting is not assigned to that EI, and Precedence Call Diversion is not activated, then the SC shall not complete it. The caller shall receive a BPA.

SCM-000750 [**Required: SC**] When the call attempt is at a precedence level above ROUTINE and the local PEI or AEI is busy with a session that is equal to or higher than the precedence level of the new session, then if the called EI is a single-call-appearance EI (or ATA or IAD), and Precedence Call Waiting is not assigned to that EI, but Precedence Call Diversion is activated, then the requirements in Section 2.2.10, Precedence Call Diversion, apply.

SCM-000760 [**Required: SC**] When the call attempt is at a precedence level above ROUTINE and the local PEI or AEI is busy with a session that is equal to or higher than the precedence level of the new session, then if the called EI is a single-call-appearance EI (or ATA or IAD), and Precedence Call Waiting is assigned to that EI, then the requirements in Section 2.2.3.1, Busy with Higher Precedence Call, apply.

SCM-000770 [**Required: SC**] When the call attempt is at a precedence level above ROUTINE and the local PEI or AEI is busy with a session that is equal to or higher than the precedence level of the new session, then if the called EI is a multiple-call-appearance EI, then the requirements in Section 2.9.7.3, Multiple Call Appearances – Interactions with Precedence Calls, apply.

SCM-000780 [**Required: SC**] When the call attempt is a ROUTINE call and the local PEI or AEI is busy with a session, the caller shall receive Station Busy tone as per Section 2.9.1.2.1, UC Ringing Tones, Cadences, and Information Signals.

SCM-000790 [**Required: SC**] The SC shall not modify its IPC when local sessions are connected or disconnected because they do not affect traffic in the access link to the WAN.

SCM-000800 [**Optional: SC**] An intrabase session count shall be maintained separately, independent of precedence, and when this ~~valve~~ value is reached no more ROUTINE precedence level session requests shall be processed for intrabase connection. PRIORITY, IMMEDIATE, FLASH, and FLASH OVERRIDE session requests shall be processed in accordance with requirements SCM-000720 through SCM-000780 above.~~as specified in items a, b, and c.~~

2.3.1.4 SC Session Control Processing With Directionalization

The requirements for ASAC directionalization are optional.

The SC directionalization requirements are applicable to VoIP sessions transmitted over an IP access link. They are not applicable to TDM sessions.

SCM-000810 [**Optional: SC**] When ASAC directionalization is implemented and applied, directionalized session budgets (IPBo and IPBi) shall be set and the SC shall keep a running count of IPCo and IPCi to ensure that these counts do not exceed their respective budgets. The IPCo processing is carried out independently from that of IPCi. Each process is identical to that carried for IPC for non-directionalization, as specified earlier. Since the IPCo and IPCi control

processes are independent, a FLASH OVERRIDE inbound session will not be able to preempt a ROUTINE outbound session.

2.3.2 ASAC Requirements for the SS Related to Voice

The signaling for the TDM voice sessions is processed by the MG in conjunction with the EO/SMEO/PBX1/PBX2. The SS is not involved with intrabase signaling. Consequently, this section considers only those VoIP sessions that are transmitted over the IP access link.

2.3.2.1 Voice Session Budget Unit

SCM-000820 [**Required: SS**] The SS shall be configurable with the IPB VoIP Session Budget for each SC in its domain, consistent with the requirements in Section 2.3.1.2, ASAC States.

SCM-000830 [**Optional: SS**] The SS shall be configurable with separate IPBi and IPBo VoIP Session Budgets for each SC in its domain, consistent with the requirements in Section 2.3.1.2, ASAC States.

SCM-000840 [**Required: SS**] The SS shall maintain a running count of IPC for each SC in its domain. It shall do this by monitoring the AS-SIP messages associated with each of its subordinate SCs as specified in AS-SIP 2013.

SCM-000850 [**Optional: SS**] The SS shall maintain a running count of separate IPCo and IPCi counts for each SC in its domain. It shall do this by monitoring the AS-SIP messages associated with each of its subordinate SCs as specified in AS-SIP 2013.

SCM-000860 [**Required: SS**] Initially, the IPC for each SC is set to zero. The SS shall increment and decrement the IPC as follows:

SCM-000860.a For outbound sessions:

SCM-000860.a.1 [**Required: SS**] After having received a session request (i.e., INVITE) from its local SC, the SS shall increment the corresponding IPC upon forwarding that session request to the far-end SC.

SCM-000860.a.2 [**Required: SS**] The SS shall decrement its IPC when it determines that a session request is completely terminated or an established session is completely terminated.

SCM-000860.b For inbound sessions:

SCM-000860.b.1 [**Required: SS**] The SS shall increment its IPC upon transmitting to the far-end SC a "session accepted" (i.e., 1XX or 2XX) response to an INVITE request that it received from the far-end SC. (The IPC is not incremented for INVITE requests.)

SCM-000860.b.2 [**Required: SS**] The SS decrements its IPC when it determines that a session request is completely terminated or an established session is completely terminated.

SCM-000870 [**Required: SS**] The SS shall police each SC in its domain to ensure that the IPC does not exceed IPB.

SCM-000870.a [**Required: SS**] If IPC equals IPB, and an SC attempts to place another session by forwarding a session INVITE to its SS, the SS shall not forward the session INVITE and shall send an error message to the EMS. The caller shall receive a busy announcement as per Section 2.9.1.2.2, Announcements.

SCM-000870.b [**Required: SS**] If IPC equals IPB at an SC, and its SS receives a session INVITE intended for that SC (either from another SC or another SS), the SS shall forward the session INVITE to the SC. If the SC accepts the session (without preempting another session so that IPC would be greater than IPB), the SS shall not forward the "session accepted" to the sessioning SC/SS, and shall send an error message to the EMS. The caller shall receive a busy announcement as per Section 2.9.1.2.2, Announcements.

SCM-000880 [**Required: SS**] If the SS's count of an IPC is greater than or equal to the corresponding IPB, and it receives an INVITE request for a precedence session, the SS shall preempt a lower priority session (if such a session exists), and then proceed with processing the higher precedence session connect request.

SCM-000890 [**Required: SS**] If the SS receives a CCA-ID for which there is no entry in ASAC budget table, the SS shall reject the session and generate an alarm for the EMS.

SCM-000900 [**Conditional: SS**] If directionalization is implemented and applied, then the SS shall police IPCi and IPCo to ensure that they do not exceed their respective budgets. The IPCi processing is independent of that for IPCo, and the process for each is identical to that carried out for IPC in the non-directionalization case.

2.3.3 ASAC Requirements for the SC and the SS Related to Video Services

The SC and the SS will process only AS-SIP video. H.323 video will be processed by a gatekeeper appliance, and H.320 video will be processed by TDM appliances. This section considers ASAC requirements for SC and SS in processing AS-SIP video.

SCM-000910 [**Required: SC, SS**] Since the bandwidth of a video session can vary, video sessions shall be budgeted and counted in terms of Video Session Units (VSUs). One VSU equals 500 Kbps, and bandwidth for video sessions will be allocated in multiples of VSUs. For example, the bandwidth allocated to video sessions may be 500 Kbps, 1000 Kbps, 2500 Kbps, and 4000 Kbps. Thus, a video session that requires 2500 Kbps will be allocated five VSUs, and a video session that requires 4000 Kbps will be allocated eight VSUs.

SCM-000920 [**Required: SC, SS**] The SC and its corresponding SS shall be configurable with the following VSU budget (VDB): the total number of inbound and outbound VSUs plus the in-progress VSU connection attempts that an SC is allowed to have over the IP access link.

SCM-000930 [**Optional: SC, SS**] The SC and its corresponding SS shall be configurable with separate outbound (VDBo) and inbound (VDBi) VSU budgets that include respective in-progress connection attempts.

NOTE: VDB=VDBo + VDBi

SCM-000940 [**Required: SC, SS**] Since video and voice services are separately allocated bandwidth, preemption of low-precedence video sessions by high-precedence voice sessions (and vice versa) shall not be implemented. Voice sessions shall strictly preempt within their allocated bandwidth, and video sessions likewise.

SCM-000950 [**Required: SC**] The SC shall manage VSU count (VDC) of active video sessions to ensure that it does not exceed VDB. The preemption rules for video sessions are the same as for voice sessions as specified in Section 2.25.1, Multilevel Precedence and Preemption.

SCM-000960 [**Optional: SC**] The SC will manage VDCo and VDCi independently to ensure that neither one exceeds its corresponding budget.

SCM-000970 [**Optional: SC**] The SC shall preempt sessions in the process of signaling setup (progress) before preempting active sessions.

SCM-000980 [**Optional: SC**] The SC shall preempt the minimum number of sessions to accumulate the amount of VSU budget needed to satisfy the video session request.

SCM-000990 [**Required: SC**] The SC shall accumulate the needed number of VSUs by preempting all sessions of a lower precedence level (starting at the ROUTINE level) before proceeding to preempt from sessions of the next higher precedence level for the remaining required budgets.

SCM-001000 [**Required: SC**] When the total VSU counts for the sessions selected for preemption exceed the VSU budget required to satisfy the new priority video session request, the SC shall return the resulting excess VSU budget to the ASAC pool.

SCM-001010 [**Required: SS**] The SS processing requirements of video sessions shall be similar to its processing of VoIP sessions. The SS shall manage the VDC to ensure that it does not exceed VDB.

SCM-001020 [**Optional: SS**] The SS shall manage VDCo and VDCi independently to ensure that neither one exceeds its corresponding budget.

SCM-001030 [**Required: SS**] If necessary, the SS shall preempt for a session request that is at precedence level FLASH OVERRIDE or FLASH and the counts equal the budgets.

2.4 SIGNALING PROTOCOLS

SCM-001040 [**Required: PEI, SC, SS**] The control/management protocol between the PEI and the SC is, in general, proprietary.

SCM-001050 [**Required: AEI, SC, SS**] The control/management protocol between the AEI and the SC is AS-SIP as specified in AS-SIP 2013.

SCM-001060 [**Required: SC, SS**] The signaling protocol used on UC IP trunks is AS-SIP as specified in AS-SIP 2013.

SCM-001070 [**Required: SS**] The TDM-side of an SS uses DSN CCS7 signaling on CCS7-like trunks.

SCM-001080 [**Required: SC, MG within the SS**] The SC and the MG within the SS use DSN T1-619a PRI signaling on DSN PRI trunks.

SCM-001090 [**Optional: SC, MG within the SS**] The SC and the MG within the SS shall support CAS trunks. CAS signaling is used on CAS trunks.

2.4.1 Signaling Performance Guidelines

Call setup times should adhere to the following guidelines:

- For intra-enclave calls, the average delay should be no more than 1 second. For 95 percent of calls, the delay should not exceed 1.5 seconds during normal traffic conditions.
- For inter-enclave and worldwide calls within the IP environment, average delay should not exceed 6 seconds, with 95 percent of calls not to exceed 8 seconds during normal traffic conditions.

Call tear-down times should adhere to the following guidelines:

- For intra-enclave calls, the average call tear-down delay should be no more than 1 second. For 95 percent of calls, the delay should not exceed 1.5 seconds during normal traffic conditions.
- For inter-enclave and worldwide calls within the IP environment, average call tear-down delay should not exceed 3 seconds, with 95 percent of calls not to exceed 5 seconds during normal traffic conditions.

2.5 REGISTRATION AND AUTHENTICATION

SCM-001100 [Required: PEI AEI, SC, SS] Registration and authentication between Network Elements (NEs) shall follow the requirements set forth in Section 4, Information Assurance.

SCM-001110 [**Conditional**] If a Session Control appliance uses Network Time Protocol (NTP), then NTP version 3 shall be used and authentication shall be performed.

SCM-001120 [**Conditional**] If a Session Control appliance uses NTP and the NTPv3 implementation supports authentication using Public Key Infrastructure (PKI), then PKI-based authentication shall be performed.

SCM-001130 [**Conditional**] If a Session Control appliance uses NTP and the NTPv3 implementation does not support PKI, then authentication shall be performed using SHA-1 or MD5. MD5 shall be used only when SHA-1 is not supported by either the NTP client or NTP server.

2.6 SC AND SS FAILOVER AND RECOVERY

SCM-001140 [Required: SS] For failover purposes SSs shall be deployed in pairs whereby when one SS is designated as the primary SS for a given SC then the paired SS is designated as the secondary (backup) SS for the SC.

SCM-001150 [**Required: SS**] Each SS shall be provisioned with the identity of its paired SS.

SCM-001160 [**Optional: SC]** An SC MAY be provisioned with direct links to any number of other SCs (i.e. direct tertiary routes) and provisioned with the set of addresses or record served by each SC with which it has a direct tertiary route.

SCM-001170 [**Required: SC, SBC]** Each SC and SBC pairing shall support OPTIONS-based failover by at least one of the following methods:

- Alternative A: The SC-Generated OPTIONS Method (sec. Section 2.6.1 below), or
- Alternative B: The SBC-Generated OPTIONS Method (sec Section 2.6.2 below).

2.6.1 SC Failover: Alternative A: The SC-Generated OPTIONS Method

NOTE 1: The SC is not required to comply with the SC requirements set forth in Alternative A as long as the SC complies with the SC requirements set forth in alternative B.

NOTE 2: The SC that operates in accordance with alternative A MUST NOT be deployed in conjunction with a SBC that only supports alternative B.

2.6.1.1 SC-Generated OPTIONS

SCM-001180 [**Required: SC**] The SC shall send periodic OPTIONS requests to its primary SS.

SCM-001180.a [**Required: SC**] The OPTIONS request shall have 2 Route header field values whereby the first Route header field value identifies the SBC fronting the SC and the second Route header field value identifies the SBC fronting the primary SS.

SCM-001180.b [**Required: SC**] The interval between sending OPTIONS requests shall be configurable with a minimum interval of 30 seconds and a default interval of 45 seconds.

SCM-001190 [**Required: SC**] The SC shall send periodic OPTIONS requests to its secondary SS.

SCM-001190.a [**Required: SC**] The OPTIONS request shall have 2 Route header field values whereby the first Route header field value identifies the SBC fronting the SC and the second Route header field value identifies the SBC fronting the secondary SS.

SCM-001190.b [**Required: SC**] The interval between sending OPTIONS requests shall be configurable with a minimum interval of 30 seconds and a default interval of 45 seconds.

2.6.1.2 SC OPTIONS-based Failover

SCM-001200 [**Required: SC**] The SC shall designate the primary SS to be unreachable when the SC sends a configurable number of consecutive OPTIONS requests to the primary SS to which it either receives no response or receives a response code 408 (Request Time-Out), 500 (Server Internal Error), 503 (Service Unavailable) or 504 (Server Time-Out).

SCM-001200.a [**Required: SC**] The default number of consecutive failed OPTIONS requests is 2.

SCM-001210 [**Required: SC**] The SC shall designate the secondary SS to be unreachable when the SC sends a configurable number of consecutive OPTIONS requests to the secondary SS to which it either receives no response or receives a response code 408 (Request Time-Out), 500 (Server Internal Error), 503 (Service Unavailable) or 504 (Server Time-Out).

SCM-001210.a [**Required: SC**] The default number of consecutive failed OPTIONS requests is 2.

SCM-001220 [**Required: SC**] When the SC designates the primary SS to be unreachable then:

SCM-001220.a [**Required: SC**] If the SC has not also designated the secondary SS to be unreachable:

SCM-001220.a.1 [**Required: SC**] The SC sends all outbound dialog initiating requests intended for destinations reached via a SS to the secondary SS (with the exception of OPTIONS requests intended for the primary SS (see SC-based Failback).

SCM-001220.a.2 [**Required: SC**] The dialog initiating requests sent by the SC to the secondary SS shall include 2 Route header field values whereby the first Route header field value identifies the SBC fronting the SC and the second Route header field value identifies the SBC fronting the secondary SS.

SCM-001220.a.3 [**Required: SC**] The SC shall send all subsequent outbound in-dialog requests and responses associated with dialogs established over the secondary SS to the secondary SS.

SCM-001220.a.4 [**Required: SC**] The SC shall continue to send periodic OPTIONS requests to the secondary SS.

SCM-001220.b [**Required: SC**] If the SC has also designated the secondary SS to be unreachable then:

SCM-001220.b.1 [**Required: SC**] When the SC receives an outbound dialog initiating request intended for a destination outside the enclave and the SC does NOT have a direct tertiary route to the destination SC that serves the target endpoint then from a signaling perspective the SC is isolated from the UC WAN and the SC SHOULD arrange to play the isolated code announcement to the user at the originating EI.

SCM-001220.b.2 [**Optional: SC**] When the SC receives an outbound dialog initiating request intended for a destination outside the enclave and the SC has a direct tertiary route to the destination SC that serves the target endpoint then the SC forwards the INVITE over the direct tertiary route.

2.6.1.3 SC-based Failback

SCM-001230 [**Required: SC**] The SC shall send periodic OPTIONS requests to the failed primary SS.

SCM-001230.a [**Required: SC**] The OPTIONS request shall have 2 Route header field values whereby the first Route header field value identifies the SBC fronting the SC and the second Route header field value identifies the SBC fronting the primary SS.

SCM-001230.b [**Required: SC**] The interval between sending OPTIONS requests shall be configurable with a minimum interval of 30 seconds and a default interval of 60 seconds.

SCM-001240 [**Required: SC**] When the primary SS responds with 200 (OK) to a configurable number of consecutive OPTIONS requests then the SC waits a configurable wait time interval and then designates the primary SS to be reachable once again.

SCM-001240.a [**Required: SC**] The default number of consecutive successful OPTIONS requests is 2.

SCM-001240.b [**Required: SC**] The minimum wait time interval is 1 second and the default wait time interval is 60 seconds.

SCM-001250 [**Required: SC**] The SC shall again send all outbound dialog initiating requests intended for destinations reached via a SS to the primary SS.

SCM-001260 [**Required: SC**] The SC shall send all subsequent outbound in-dialog requests and responses associated with dialogs established over the primary SS to the primary SS.

SCM-001270 [**Required: SC**] The SC shall send all outbound in-dialog requests and responses associated with dialogs established over the secondary SS to the secondary SS.

SCM-001280 [**Required: SC**] The SC shall send periodic OPTIONS requests to its primary SS. The interval between sending OPTIONS requests shall be configurable with a minimum interval of 30 seconds and a default interval of 45 seconds.

SCM-001290 [**Required: SC**] The SC shall continue to send periodic OPTIONS requests to the secondary SS.

SCM-001300 [**Required: SC**] When the SC designates the secondary SS to be unreachable the SC shall send periodic OPTIONS requests to the failed secondary SS.

> **SCM-001300.a** [**Required: SC**] The OPTIONS request shall have 2 Route header field values whereby the first Route header field value identifies the SBC fronting the SC and the second Route header field value identifies the SBC fronting the secondary SS.
>
> **SCM-001300.b** [**Required: SC**] The interval between sending OPTIONS requests shall be configurable with a minimum interval of 30 seconds and a default interval of 60 seconds.

SCM-001310 [**Required: SC**] When the secondary SS responds with 200 (OK) to a configurable number of consecutive OPTIONS requests then the SC waits a configurable wait time interval and then designates the secondary SS to be reachable once again.

> **SCM-001310.a** [**Required: SC**] The default number of consecutive successful OPTIONS requests is 2.
>
> **SCM-001310.b** [**Required: SC**] The minimum wait time interval is 1 second and the default wait time interval is 60 seconds.

SCM-001320 [**Optional: SC**] If the SC established calls over direct tertiary routes when the secondary SS was unreachable then the SC shall continue to send the outbound in-dialog requests and responses associated with those calls over the respective direct tertiary routes.

SCM-001330 [**Required: SC**] The SC shall send periodic OPTIONS requests to its secondary SS. The interval between sending OPTIONS requests shall be configurable with a minimum interval of 30 seconds and a default interval of 45 seconds.

2.6.1.4 Failure Handling for Outbound Dialog-initiating INVITE

SCM-001340 [**Required: SC**] When the SC sends an outbound dialog initiating INVITE by way of its primary SS and receives either no response or receives a 408 (Request Time-Out), 500 (Server Internal Error), 503 (Service Unavailable), or 504 (Server Time-Out) then:

> **SCM-001340.a** [**Required: SC**] If the SC has not designated the secondary SS as unreachable, the SC SHALL resend the INVITE by way of the secondary SS.

SCM-001340.a.1 [**Required: SC**] If the SC receives either no response or receives a 408 (Request Time-Out), 500 (Server Internal Error), 503 (Service Unavailable), or 504 (Server Time-Out) then:

SCM-001340.a.1.a [**Required: SC**] If the SC does NOT have a direct tertiary route to the destination SC that serves the target endpoint then from a signaling perspective the SC is isolated from the UC WAN and the SC SHOULD arrange to play the isolated code announcement to the user at the originating EI.

SCM-001340.a.1.b [**Optional: SC**] If the SC has a direct tertiary route to the destination SC that serves the target endpoint then the SC forwards the INVITE over the direct tertiary route.

SCM-001340.b [**Required: SC**] If the SC has designated the secondary SS as unreachable then:

SCM-001340.b.1 [**Required: SC**] If the SC does NOT have a direct tertiary route to the destination SC that serves the target endpoint then from a signaling perspective the SC is isolated from the UC WAN and the SC SHOULD arrange to play the isolated code announcement to the user at the originating EI.

SCM-001340.b.2 [**Optional: SC**] If the SC has a direct tertiary route to the destination SC that serves the target endpoint then the SC forwards the INVITE over the direct tertiary route.

2.6.2 SC Failover: Alternative B: The SBC-Generated OPTIONS Method

NOTE 1: The SBC is not required to comply with the SBC requirements set forth in Alternative B as long as the SBC complies with the requirements set forth in alternative A.

NOTE 2: The SBC that only supports Alternative B MUST be deployed in conjunction with a SC that supports Alternative B.

2.6.2.1 SBC-Generated OPTIONS

SCM-001350 [**Required: SBC**] The SBC fronting the SC shall send periodic OPTIONS requests to the SBC fronting the primary SS.

SCM-001350.a [**Required: SBC**] The interval between sending OPTIONS requests shall be configurable with a minimum interval of 35 seconds and a default interval of 60 seconds.

SCM-001360 [**Required: SBC**] The SBC fronting the SC shall send periodic OPTIONS requests to the SBC fronting the secondary SS.

SCM-001360.a [**Required: SBC**] The interval between sending OPTIONS requests shall be configurable with a minimum interval of 35 seconds and a default interval of 60 seconds.

SCM-001370 [**Required: SBC**] The SBC fronting the primary SS shall send periodic OPTIONS requests to the primary SS.

SCM-001370.a [**Required: SBC**] The interval between sending OPTIONS requests shall be configurable with a minimum interval of 35 seconds and a default interval of 60 seconds.

SCM-001380 [**Required: SBC**] The SBC fronting the secondary SS shall send periodic OPTIONS requests to the secondary SS.

SCM-001380.a [**Required: SBC**] The interval between sending OPTIONS requests shall be configurable with a minimum interval of 35 seconds and a default interval of 60 seconds.

2.6.2.2 SBC-based Failover

SCM-001390 [**Required: SBC**] The SBC fronting the SC shall mark the path to the primary SS as unavailable when the SBC fronting the SC sends a configurable number of consecutive OPTIONS requests to the SBC fronting the primary SS to which it either receives no response or receives a response code of 408 (Request Time-Out), 500 (Server Internal Error), 503 (Service Unavailable) or 504 (Server Time-Out).

SCM-001390.a [**Required: SBC**] The default number of consecutive failed OPTIONS requests is 2.

SCM-001400 [**Required: SBC**] The SBC fronting the primary SS shall mark the path to the primary SS as unavailable when the SBC fronting the primary SS sends a configurable number of consecutive OPTIONS requests to the primary SS to which it either receives no response or receives a response code of 408 (Request Time-Out), 500 (Server Internal Error), 503 (Service Unavailable) or 504 (Server Time-Out).

SCM-001400.a [**Required: SBC**] The default number of consecutive failed OPTIONS requests is 2.

SCM-001410 [**Required: SBC**] The SBC fronting the SC shall mark the path to the secondary SS as unavailable when the SBC fronting the SC sends a configurable number of consecutive OPTIONS requests to the SBC fronting the secondary SS to which it either receives no response or receives a 408 (Request Time-Out), 500 (Server Internal Error), 503 (Service Unavailable) or 504 (Server Time-Out).

SCM-001410.a [**Required: SBC**] The default number of consecutive failed OPTIONS requests is 2.

SCM-001420 [**Required: SBC**] The SBC fronting the secondary SS shall mark the path to the secondary SS as unavailable when the SBC fronting the secondary SS sends a configurable number of consecutive OPTIONS requests to the secondary SS to which it either receives no response or receives a 408 (Request Time-Out), 500 (Server Internal Error), 503 (Service Unavailable) or 504 (Server Time-Out).

> **SCM-001420.a** [**Required: SBC**] The default number of consecutive failed OPTIONS requests is 2.

SCM-001430 [**Required: SBC**] When the SBC fronting the SC marks the path to the primary SS as unavailable AND the SBC fronting the SC receives an outbound request from the SC whose Route header(s) identify the next hop to be the SBC serving the primary SS, then the SBC serving the SC shall respond with either a 500 (Server Internal Error), 503 (Service Unavailable) or 504 (Server Time-Out).

SCM-001440 [**Required: SBC**] When the SBC fronting the primary SS marks the path to the primary SS as unavailable AND the SBC fronting the primary SS receives an outbound request from the SBC serving the SC then the SBC serving the primary SS shall respond with either a 500 (Server Internal Error), 503 (Service Unavailable) or 504 (Server Time-Out).

SCM-001450 [**Required: SBC**] When the SBC fronting the SC marks the path to the secondary SS as unavailable AND the SBC fronting the SC receives an outbound request from the SC whose Route header(s) identify the next hop to be the SBC serving the secondary SS, then the SBC serving the SC shall respond with either a 500 (Server Internal Error), 503 (Service Unavailable) or 504 (Server Time-Out).

SCM-001460 [**Required: SBC**] When the SBC fronting the secondary SS marks the path to the secondary SS as unavailable AND the SBC fronting the secondary SS receives an outbound request from the SBC serving the SC then the SBC serving the secondary SS shall respond with either a 500 (Server Internal Error), 503 (Service Unavailable) or 504 (Server Time-Out).

2.6.2.3 SBC-based Fail Back

SCM-001470 [**Required: SBC**] When the SBC fronting the SC has marked the path to the primary SS as unavailable then the SBC fronting the SC shall send periodic OPTIONS requests to the SBC fronting the primary SS.

SCM-001480 [**Required: SBC**] The interval between sending OPTIONS requests shall be configurable with a minimum interval of 35 seconds and a default interval of 60 seconds.

SCM-001490 [**Required: SBC**] When the SBC fronting the primary SS responds with 200 (OK) to a configurable number of consecutive OPTIONS requests sent by the SBC fronting the SC then the SBC fronting the SC marks the path to the primary SS as available once again.

> **SCM-001490.a** [**Required: SBC**] The default number of successful OPTIONS requests is 2.

SCM-001500 [**Required: SBC**] Upon failback, the SBC fronting the SC shall send periodic OPTIONS requests to the SBC fronting its primary SS whereby the interval between sending OPTIONS requests shall be configurable with a minimum interval of 35 seconds and a default interval of 60 seconds.

SCM-001510 [**Required: SBC**] When the SBC fronting the primary SS has marked the path to the primary SS as unavailable then the SBC fronting the primary SS shall send periodic OPTIONS requests to the primary SS.

> **SCM-001510.a** [**Required: SBC**] The interval between sending OPTIONS requests shall be configurable with a minimum interval of 35 seconds and a default interval of 60 seconds.

SCM-001520 [**Required: SBC**] When the primary SS responds with 200 (OK) to a configurable number of consecutive OPTIONS requests sent by the SBC fronting the primary SS then the SBC fronting the primary SS marks the path to the primary SS as available once again.

> **SCM-001520.a** [**Required: SBC**] The default number of successful OPTIONS requests is 2.

SCM-001530 [**Required: SBC**] Upon failback, the SBC fronting the primary SS shall send periodic OPTIONS requests to the primary SS whereby the interval between sending OPTIONS requests shall be configurable with a minimum interval of 35 seconds and a default interval of 60 seconds.

SCM-001540 [**Required: SC**] For any calls established via the secondary SS when the primary SS was unavailable, the SC shall continue to send the outbound in-dialog requests and responses via the secondary SS.

SCM-001550 [**Required: SBC**] When the SBC fronting the SC has marked the path to the secondary SS as unavailable then the SBC fronting the SC shall send periodic OPTIONS requests to the SBC fronting the secondary SS.

> **SCM-001550.a** [**Required: SBC**] The interval between sending OPTIONS requests shall be configurable with a minimum interval of 35 seconds and a default interval of 60 seconds.

SCM-001560 [**Required: SBC**] When the SBC fronting the secondary SS responds with 200 (OK) to a configurable number of consecutive OPTIONS requests sent by the SBC fronting the SC then the SBC fronting the SC marks the path to the secondary SS as available once again.

> **SCM-001560.a** [**Required: SBC**] The default number of successful OPTIONS requests is 2.

SCM-001570 [**Required: SBC**] Upon failback, the SBC fronting the SC shall send periodic OPTIONS requests to the SBC fronting its secondary SS whereby the interval between sending

OPTIONS requests shall be configurable with a minimum interval of 35 seconds and a default interval of 60 seconds.

SCM-001580 [**Required: SBC**] When the SBC fronting the secondary SS has marked the path to the secondary SS as unavailable then the SBC fronting the secondary SS shall send periodic OPTIONS requests to the secondary SS.

> **SCM-001580.a** [**Required: SBC**] The interval between sending OPTIONS requests shall be configurable with a minimum interval of 35 seconds and a default interval of 60 seconds.

SCM-001590 [**Required: SBC**] When the secondary SS responds with 200 (OK) to a configurable number of consecutive OPTIONS requests sent by the SBC fronting the secondary SS then the SBC fronting the secondary SS marks the path to the secondary SS as available once again.

> **SCM-001590.a** [**Required: SBC**] The default number of successful OPTIONS requests is 2.

SCM-001600 [**Required: SBC**] Upon failback, the SBC fronting the secondary SS shall send periodic OPTIONS requests to the secondary SS whereby the interval between sending OPTIONS requests shall be configurable with a minimum interval of 35 seconds and a default interval of 60 seconds.

SCM-001610 [**Optional: SC**] if the SC established calls over direct tertiary routes when the secondary SS was unavailable then the SC shall continue to send its outbound in-dialog requests and responses associated with those calls over the respective direct tertiary routes.

2.6.2.4 Failure Handling for Outbound Dialog-initiating INVITE

SCM-001620 [**Required: SC**] When the SC sends an outbound dialog initiating INVITE by way of its primary SS and receives either no response or a 408 (Request Time-Out), 500 (Server Internal Error), 503 (Service Unavailable), or 504 (Server Time-Out) then the SC shall resend the INVITE by way of its secondary SS.

SCM-001630 [**Required: SC**] If the SC resends an outbound dialog initiating INVITE by way of its secondary SS and receives either no response or a 408 (Request Time-Out), 500 (Server Internal Error), 503 (Service Unavailable), or 504 (Server Time-Out) then:

> **SCM-001630.a** [**Required: SC**] If the SC does NOT have a direct tertiary route to the destination SC that serves the target endpoint then from a signaling perspective the SC is isolated from the UC WAN and the SC SHOULD arrange to play the isolated code announcement to the user at the originating EI.

SCM-001630.b [**Optional: SC**] If the SC has a direct tertiary route to the destination SC that serves the target endpoint, the SC forwards the INVITE over the direct tertiary route to the destination SC.

2.6.3 SS Failover

SS-Generated OPTIONS.

SCM-001640 [**Required: SS**] Each SS sends periodic OPTIONS requests to its paired SS.

SCM-001640.a [**Required: SS**] The interval between sending OPTIONS requests shall be configurable with a minimum interval of 35 seconds and a default interval of 45 seconds.

SCM-001650 [**Required: SS**] Each SS sends periodic OPTIONS requests to each of the other SSs (aside from its paired SS which is covered in the previous requirement).

SCM-001650.a [**Required: SS**] The interval between sending OPTIONS requests shall be configurable with a minimum interval of 35 seconds and a default interval of 45 seconds.

SCM-001660 [**Required: SS**] The OPTIONS requests shall have 2 Route header field values whereby the first Route header field value identifies the SBC fronting the ~~SC~~ SS sending the OPTIONS request and the second Route header field value identifies the SBC fronting the target SS.

2.6.3.1 OPTIONS-based SS failover and failback of paired SS

SCM-001670 [**Required: SS**] A SS shall designate its paired SS as unreachable when the SS sends a configurable number of consecutive OPTIONS requests to its paired SS to which it either receives no response or receives a response code 408 (Request Time-Out), 500 (Server Internal Error), 503 (Service Unavailable) or 504 (Server Time-Out).

SCM-001670.a [**Required: SS**] The default number of consecutive failed OPTIONS requests is 2.

SCM-001680 [**Required: SS**] When a SS designates its paired SS as unreachable then:

SCM-001680.a [**Required: SS**] When the SS receives a dialog initiating request whose destination is a SC for which it is the secondary SS then the SS directly sends the request to the destination SC (instead of forwarding the request to the primary SS).

SCM-001680.b [**Required: SS**] The SS includes 2 Route header field values in the request whereby the first Route header field value identifies the SBC fronting the SS and the second Route header field value identifies the SBC fronting the destination SC.

SCM-001680.c [**Required: SS**] The SS shall send OPTIONS requests to its failed paired SS.

SCM-001680.d [**Required: SS**] The interval between sending OPTIONS requests shall be configurable with a minimum interval of 35 seconds and a default interval of 60 seconds.

SCM-001690 [**Required: SS**] When the paired SS responds with 200 (OK) to a configurable number of consecutive OPTIONS requests then the SS waits a configurable wait time interval and then designates the paired SS as reachable once again.

SCM-001690.a [**Required: SS**] The default number of consecutive successful OPTIONS requests is 2.

SCM-001690.b [**Required: SS**] The minimum wait time interval is 1 second and the default wait time interval is 60 seconds.

SCM-001700 [**Required: SS**] Once the paired SS is again designated as reachable then the SS, upon receiving dialog-initiating requests whose destination is a SC for which it is the secondary SS, shall forward the requests to its paired SS.

2.6.3.2 OPTIONS-based SS Failover and Failback of another SS (that is NOT its paired SS)

SCM-001710 [**Required: SS**] A SS shall designate another SS (that is not its paired SS) as unreachable when the SS sends a configurable number of consecutive OPTIONS requests to the other SS to which it either receives no response or receives a response code 408 (Request Time-Out), 500 (Server Internal Error), 503 (Service Unavailable) or 504 (Server Time-Out).

SCM-001710.a [**Required: SS**] The default number of consecutive failed OPTIONS requests is 2.

SCM-001720 [**Required: SS**] When a SS α determines another SS to be unreachable then:

SCM-001720.a [**Required: SS**] When SS α receives a dialog initiating request whose next hop is the unreachable SS then SS α forwards the request to the next SS in the route list for the destination.

SCM-001720.b [**Required: SS**] SS α includes 2 Route header field values in the request whereby the first Route header field value identifies the SBC fronting SS α and the second Route header field value identifies the SBC fronting the next SS in the route list for the destination.

SCM-001720.c [**Required: SS**] SS α shall send OPTIONS requests to the failed SS.

SCM-001720.d [**Required: SS**] The interval between sending OPTIONS requests shall be configurable with a minimum interval of 35 seconds and a default interval of 60 seconds.

SCM-001730 [**Required: SS**] When the failed SS responds with 200 (OK) to a configurable number of consecutive OPTIONS requests then SS α waits a configurable wait time interval and then designates the failed SS as reachable once again.

SCM-001730.a [**Required: SS**] The default number of consecutive successful OPTIONS requests is 2.

SCM-001730.b [**Required: SS**] The minimum wait time interval is 1 second and the default wait time interval is 60 seconds.

SCM-001740 [**Required: SS**] Once the failed SS is again designated as reachable then SS α, upon receiving dialog-initiating requests for which the recovered SS is the first entry in the route list, shall forward the requests to the recovered SS.

2.6.3.3 Failure Handling for Dialog-initiating INVITEs

SCM-001750 [**Required: SS**] When a SS receives a dialog initiating INVITE whose destination is a SC for which it is the secondary SS then:

SCM-001750.a [**Required: SS**] The SS shall forward the INVITE to its paired SS (which is the primary SS for the SC).

SCM-001750.b [**Conditional: SS**] If the SS receives either no response or receives a 408 (Request Time-Out), 500 (Server Internal Error), 503 (Service Unavailable) or 504 (Server Time-Out) from the primary SS then the SS shall forward the INVITE directly to the SC.

SCM-001760 [**Required: SS**] When a SS α receives a dialog initiating INVITE and the first entry in the route list is another SS (that is not its paired SS) then:

SCM-001760.a [**Required: SS**] SS α shall forward the INVITE to the other SS.

SCM-001760.b [**Conditional: SS**] If SS α receives either no response or receives a 408 (Request Time-Out), 500 (Server Internal Error), 503 (Service Unavailable) or 504 (Server Time-Out) then SS α shall forward the INVITE to the next SS entry in the route list for the destination.

2.7 PRODUCT INTERFACE

2.7.1 Internal Interface

SCM-001770 [**Required: PEI, AEI, SC (including the MG and Media Server), SS, SBC**] Internal interfaces are functions that operate internal to a System Under Test (SUT) or UC-

approved product (e.g., SC, SS). The interfaces between SC/SS functions within an SC (e.g., between the Call Admission Control (CAC), Interworking Function (IWF), MGC, and MG) and Signaling Gateway (SG) are considered internal to the SC regardless of the physical packaging. These interfaces are vendor-proprietary and unique, especially the protocol used over the interface. Whenever the physical interfaces use Institute of Electrical and Electronics Engineers, Inc. (IEEE) 802.3 Ethernet standards, they shall support auto-negotiation even when the IEEE 802.3 standard has it as optional. This applies to 10/100/1000-T Ethernet standards; i.e., IEEE, Ethernet Standard 802.3, 1993; or IEEE, Fast Ethernet Standard 802.3u, 1995; and IEEE, Gigabit Ethernet Standard 802.3ab, 1999.

2.7.2 External Physical Interfaces Between Network Components

External physical interfaces between components are functions that cross the demarcation point between SUTs and other external network components. The following subparagraphs provide requirements and specifications for external component physical interfaces.

SCM-001780 [**Required: SC, SS, SBC, ~~PEI, AEI~~**] The SC (and its appliances), SS and~~,~~ SBC~~, and EIs~~ shall support 10/100/1000-T Mbps Ethernet physical interfaces to ASLAN switches and routers. Whenever the physical interfaces use IEEE 802.3 Ethernet standards, they shall support auto-negotiation even when the IEEE 802.3 standard has it as optional. This applies to 10/100/1000-T Ethernet standards; i.e., IEEE, Ethernet Standard 802.3, 1993; or IEEE, Fast Ethernet Standard 802.3u, 1995; and IEEE, Gigabit Ethernet Standard 802.3ab, 1999.

NOTE: This requirement does not preclude the use of other types of physical interfaces, including those that support fiber optic cable.

SCM-001781 [**Required: PEI, AEI**] PEI and AEI shall support 10/100-T Mbps Ethernet physical interfaces to ASLAN switches and routers. Whenever the physical interfaces use IEEE 802.3 Ethernet standards, they shall support auto-negotiation even when the IEEE 802.3 standard has it as optional. This applies to 10/100-T Ethernet standards; i.e., IEEE, Ethernet Standard 802.3, 1993; or IEEE, Fast Ethernet Standard 802.3u, 1995.

NOTE: This requirement does not preclude the use of 1000-T Mbps Ethernet other types of physical interfaces, including those that support fiber optic cable.

SCM-001790 [Required: SBC] The SBC shall support an ASLAN-side 10Base-X Ethernet interface and a WAN-side 10Base-X Ethernet interface.

SCM-001800 [Optional: SBC] The SBC shall support 100Base-X Ethernet, or Gigabit Ethernet (Gbe), or 10Gigabit Ethernet (10GbE), full duplex interfaces on both the ASLAN-side and the WAN-side.

2.7.3 Interfaces to Other Networks

Interfaces to other networks are interfaces where traffic flows from one network (e.g., UC) to another network (e.g., PSTN).

2.7.3.1 Deployable Networks Interface

The Deployable interface requirements are specified in Appendix A, Unique Deployed (Tactical), and Section 6, Network Infrastructure End-to-End Performance.

2.7.3.2 DISN Teleport Site Interface

SCM-001810 [**Required**] The Assured Services subsystem shall interface the Teleport sites on both a TDM basis and an IP basis. A T1.619a MG with PRI signaling will be used for T1 trunks to the Teleport sites. If the Teleport site contains an SC, then the interface will be via the DISN WAN for both the media and signaling, with the signaling being AS-SIP (AS-SIP 2013) between the Teleport SC and the UC SS.

2.7.3.3 PSTN Interface

SCM-001820 [**Required**] The Assured Services subsystem shall interface with the PSTN and host-nation PTTs via the MG interfaces as specified in Section 2.16, Media Gateway.

2.7.3.4 Allied and Coalition Network Interface

Voice and video interfaces with allied and coalition networks have not yet been defined. Therefore, the interface will remain TDM as specified in Figure 4.4.2-1, DSN Design and Components.

2.7.4 DISA VVoIP EMS Interface

SCM-001830 [**Required: SC, SS, SBC**] SC, SS, and SBC shall support a 10/100-Mbps Ethernet physical interface to the DISA VVoIP EMS. The interface will work in either of the two following modes using auto-negotiation: IEEE, Ethernet Standard 802.3, 1993; or IEEE, Fast Ethernet Standard 802.3u, 1995.

SCM-001840 [Optional: SC, SS, SBC] Local management traffic and VVoIP EMS management traffic shall use separate physical Ethernet interfaces. Redundant VVoIP EMS physical Ethernet interfaces may be used but are not required. Redundant local management physical Ethernet interfaces may be used but are not required.

Redundant physical Ethernet interfaces are required for signaling and bearer traffic. If the primary signaling and bearer Ethernet interface fails, then traffic shall be switched to the backup signaling and bearer Ethernet interface. When the primary Ethernet interface fails, the secondary Ethernet interface has to have the same IP address. The failover from the primary to the

secondary interface shall comply with the specifications in Section 7.6.6.2, Dual Product Redundancy.

Signaling and bearer traffic may use the same physical Ethernet interface as local or VVoIP EMS management traffic, or it may use a separate physical Ethernet interface.

SCM-001850 [**Conditional: SC, SS, SBC**] If signaling and bearer traffic shares a physical Ethernet interface with local or VVoIP EMS management traffic, then the signaling and bearer traffic shall use a separate VLAN.

2.8 PRODUCT PHYSICAL, QUALITY, AND ENVIRONMENTAL FACTORS

2.8.1 Physical Characteristics

The physical characteristics of network equipment with respect to weight, dimensions, transportation, storage, durability, safety, and color are required to be those of best commercial practices, and will be specified by the acquiring DoD organization.

2.8.2 Product Quality Factors

The product quality factors associated with reliability, maintainability, and availability are based on the requirements in Telcordia Technologies GR-512-CORE. The explanation and format for these requirements are in GR-512-CORE, Sections 1 through 5. However, the types and values of the following requirements have been modified from the Generic Requirements (GR) document to reflect a judged application to VVoIP products. Equipment capabilities are still expected to meet best commercial practices as reflected in the GR, including those of "carrier grade" or, Central Office (CO) equipment. The following paragraphs outline the availability requirements for the Assured Services subsystem.

2.8.2.1 Product Availability

SCM-001860 [**Required: High Availability, SC, SS**] The Assured Services appliance shall have a hardware or software availability of 0.99999 (a nonavailability state of no more than 5 minutes per year). The vendor shall provide an availability model for the appliance showing all calculations and showing how the overall availability will be met. The subsystem(s) shall have no single point of failure that can cause an outage of more than 96 voice and/or video subscribers. To meet the availability requirements, all subsystem(s) platforms that offer service to more than 96 voice and/or video subscribers shall have a modular chassis that provides, at a minimum, the following:

a. Dual Power Supplies. The platform shall provide a minimum of two power supplies, each with a power capacity to support the entire chassis's electrical load.

b. Dual Processors/Swappable Sparing (Control Supervisors). The chassis shall support dual-active processors, or processor card automatic swappable sparing. Failure of any one processor or swappable processor cards shall not cause a loss of any ongoing functions within the chassis (e.g., no loss of active calls).

c. Termination Sparing. The chassis shall support an (N+1) sparing capability for available 10/100-Mbps Ethernet modules used to terminate an IP voice or video subscriber.

d. Redundancy Protocol. The routing equipment shall support a protocol that allows for dynamic rerouting of IP packets or Ethernet frames so that no single point of failure exists in the Assured Services subsystem.

e. No Single Failure Point. No single point shall exist in the subsystem that could cause the loss of voice and/or video service to more than 96 voice or video PEIs or AEIs.

f. Switch Fabric or Backplane Redundancy for Active Backplanes. Active switching platforms within the subsystem components shall support a redundant (1+1) switching fabric or backplane. The second fabric's backplane shall be in active standby so failure of the first backplane shall not cause the loss of any ongoing events within the platform.

g. Software Upgrades and Patches. Software upgrades and patches shall be able to be implemented without incurring any subsystem downtime.

h. Backup Power UPS Requirements. The components that compose the subsystem for F/FO users, I/P users, and R users shall meet the appropriate Section 7, Network Edge Infrastructure, switch type backup power UPS requirements (e.g., 8 hours for an SS and SC) for all devices including the PEIs and AEIs. If a base has an automatic UPS switchover 72-hour power capability that feeds all the voice and video equipment, including the PEIs and AEIs, then it naturally meets the 8-hour backup power requirement with no need to do anything special or extra at the SC or SS. Backup power is required only for as many hours as it will take the base to switch over to backup generator power, but the total combination of backup times shall not be less than 8 hours.

i. No Loss of Active Sessions. In the event of component failure in an appliance subsystem(s), all active sessions shall not be disrupted (namely, the loss of established session connections requiring user redialing to reestablish), and the media path through the network shall be restored within 5 seconds. In addition, when the state information is lost for non-disrupted active sessions, the SRTP media streams will clear when both the called and calling parties hang up their EIs. All components used to implement redundancy shall be capable of handling the entire session processing load in the event that its counterpart device fails. Signaling states during the establishment or disestablishment of a session need not be maintained or continued during the switch over to backup components. However, session establishment or disestablishment states shall be cleared to prevent anomalous conditions such as the EI continues to ring even though the session will not be established or disestablished during the device(s) switch over. When session establishment or disestablishment signaling states are lost when switching

over to backup components, it is expected that the subscriber will be required to redial the called number.

In addition, when an Appliance component fails and the backup component takes over, each media stream for each active call shall remain active during the failover, until either 1) timer expirations or lack of state information cause that call to terminate or 2) the EI subscribers on that call, naturally terminate the call.

SCM-001870 [**Required: Medium Availability SC**] The Medium Availability SC shall have a hardware or software availability of 0.9999 (a non-availability state of no more than 53 minutes per year). The vendor shall provide an availability model for the appliance showing all calculations and showing how the overall availability will be met. In support of the availability requirements, all subsystem(s) platforms that offer service to more than 96 voice and/or video subscribers shall have a modular design and chassis that provides, at a minimum, the following:

a. Dual Power Supplies. The platform shall provide a minimum of two power supplies, each with a power capacity to support the entire chassis' electrical load.

b. Software Upgrades and Patches. Software upgrades and patches shall be able to be implemented without incurring any subsystem downtime.

c. No Loss of Active Sessions. In the event of component failure in an appliance subsystem(s), all active sessions shall not be disrupted (namely, the loss of established session connections requiring user redialing to reestablish), and the media path through the network shall be restored within 5 seconds. In addition, when the state information is lost for non-disrupted active sessions, the SRTP media streams will clear when both the called and calling parties hang up their EIs. All components used to implement redundancy shall be capable of handling the entire session processing load in the event that its counterpart device fails. Signaling states during the establishment or disestablishment of a session need not be maintained or continued during the switch over to backup components. However, session establishment or disestablishment states shall be cleared to prevent anomalous conditions such as the EI continuing to ring even though the session will not be established or disestablished during the device(s) switch over. When session establishment or disestablishment signaling states are lost when switching over to backup components, it is expected that the subscriber will be required to redial the called number.

   In addition, when an Appliance component fails and the backup component takes over, each media stream for each active call shall remain active during the failover, until either 1) timer expirations or lack of state information cause that call to terminate or 2) the EI subscribers on that call naturally terminate the call.

SCM-001880 [**Optional: Medium Availability SC**] The Medium Availability SC shall have a modular design and chassis that provides, at a minimum, the following:

a. Dual Processors/Swappable Sparing (Control Supervisors). The chassis shall support dual-active processors, or processor card automatic swappable sparing. Failure of any one processor or swappable processor cards shall not cause a loss of any ongoing functions within the chassis (e.g., no loss of active calls).

b. Termination Sparing. The chassis shall support an (N+1) sparing capability for available 10/100-Mbps Ethernet modules used to terminate an IP voice or video subscriber.

c. Redundancy Protocol. The routing equipment shall support a protocol that allows for dynamic rerouting of IP packets or Ethernet frames so that no single point of failure exists in the Assured Services subsystem.

d. No Single Failure Point. No single point shall exist in the subsystem that could cause the loss of voice and/or video service to more than 96 voice or video PEIs or AEIs.

e. Switch Fabric or Backplane Redundancy for Active Backplanes. Active switching platforms within the subsystem components shall support a redundant (1+1) switching fabric or backplane. The second fabric's backplane shall be in active standby so that failure of the first backplane shall not cause the loss of any ongoing events within the platform.

f. Backup Power UPS Requirements. The backup power requirement is a minimum of 1 hour.

NOTE: The Medium Availability SCs are not designed to support Special C2 users and are not recommended for that purpose.

2.8.2.2 Maximum Downtimes

SCM-001890 [**Required: High Availability SC, SS, ASLAN**] The performance parameters associated with the ASLAN, SS, and High Availability SC, when combined, shall meet the following maximum downtime requirements:

a. IP (10/100/1000 Ethernet) network links: 35 minutes per year.

b. IP subscriber: 12 minutes per year.

SCM-001900 [**Required: Medium Availability SC, SS, ASLAN**] The performance parameters associated with the ASLAN, SS, and Medium Availability SC, when combined, shall meet the following maximum downtime requirements:

a. IP (10/100/1000 Ethernet) network links – 82 minutes per year.

b. IP subscriber – 60 minutes per year.

2.8.3 Environmental Conditions

SCM-001910 [**Required**] Environmental conditions requirements are contained in Telcordia Technologies GR-63-CORE. This document identifies the minimum generic spatial and

environmental criteria for all new telecommunications equipment systems used in a telecommunications network. Included with these equipment systems are associated cable distribution systems, distributing and interconnecting frames, power equipment, operations support systems, and cable entrance facilities. The detailed specifications of this section are those of best commercial practice and will be specified by the acquiring DoD organization.

2.8.4 Voice Service Quality

SCM-001920 [**Required: PEI, AEI, IAD, TA, MG**] For these VoIP devices, the voice quality shall have a Mean Opinion Score (MOS) of 4.0 (R-Factor equals 80) or better, as measured IAW the E-Model. Additionally, these devices shall not lose two or more consecutive packets in a minute and shall not lose more than seven voice packets (excluding signaling packets) in a 5-minute period. This applies only to devices that generate media and have a Network Interface Card (NIC).

2.9 END INSTRUMENTS

An End Instrument (EI) is the device or application through which an end user accesses UC voice, secure voice and video communication services.

UC IP EIs use either DoD Assured Services Session Initiation Protocol 2013 (AS-SIP 2013), or vendor-proprietary protocols for signaling. AEI is used to mark requirements applicable to IP EIs that use AS-SIP and PEI is used to mark requirements applicable IP EIs that use proprietary protocols. Note that ITU H.323 and Internet Engineering Task Force (IETF) SIP are considered vendor-proprietary protocols because one EI vendor's implementation of H.323 or SIP is not guaranteed to interoperate with another vendor's implementation of H.323 or SIP.

ROUTINE-only EIs (ROEIs) are UC IP EIs that support voice or video service but do not support precedence and preemption. An ROEI can use either AS-SIP or proprietary signaling.

This section also includes requirements with respect to support for analog and ISDN BRI telephones.

~~This section defines requirements for the following End Instrument (EI) types:~~

- ~~Proprietary IP voice EIs (PEIs).~~
- ~~ROUTINE-only EIs (ROEIs).~~
- ~~AS-SIP voice End Instruments.~~
- ~~AS-SIP video End Instruments.~~
- ~~AS-SIP Secure voice End Instruments.~~
- ~~Secure IP EIs (using SCIP/V.150.1 protocol).~~
- ~~Softphones.~~

2.9.1 IP Voice End Instruments

2.9.1.1 Basic

An IP voice instrument shall be designed IAW the acquiring activity requirements, but the following capabilities are required specifically as indicated.

SCM-001930 [**Optional: PEI, AEI~~Voice EI~~**] DoD Common Access Card (CAC) reader. [See Section 4.2.3.5, Authentication Practices, item 1h(1), for SC and EI requirements on PKI and CAC authentication, and SC and EI requirements on Username and Personal Identification Number (PIN) authentication.]

SCM-001940 [**Required: PEI, AEI~~Voice EI~~**] Display calling number. (See Section 2.2.8, Calling Number Delivery, for SC and EI requirements on the Calling Number Delivery feature.)

SCM-001950 [**Required: PEI, AEI~~Voice EI~~**] Display precedence level of the session.

SCM-001960 [**Required: PEI, AEI~~Voice EI~~**] Use of DSCPs in signaling and media streams.

SCM-001970 [**Required: PEI, AEI~~Voice EI~~**] Support for Dynamic Host Configuration Protocol (DHCP).

SCM-001980 [**Removed~~Required: Voice EI~~**] ~~For multiple line appearance, only two-appearance IP voice instruments are specified and they shall function as specified in Section 2.9.7, Multiple Call Appearance Requirements for AS-SIP EIs.~~

2.9.1.2 Tones and Announcements

SCM-001990 [**Required: PEI, AEI, SC, SS**] Tones and announcements, as required in Section 2.9.1.2.1, UC Ringing Tones, Cadences, and Information Signals, and Section 2.9.1.2.2, Announcements, shall be supported~~, except for the loss of the C2 announcement~~. These tones and announcements shall be generated locally by the PEI or AEI on the command of the SC, or shall be generated on the command of the SC by an internal SC Media Server or an external Media Server connected to the ASLAN and passed as a media stream to the PEI or AEI. Regardless of how implemented, the Media Server is part of the SC SUT.

2.9.1.2.1 UC Ringing Tones, Cadences, and Information Signals

SCM-002000 [**Required: PEI, AEI, TA, IAD, MG, SC, SS**] The UC EIs and signaling appliances shall provide alerting (ringing) for precedence calls (i.e., PRIORITY and above) that is distinct from the alerting for ROUTINE calls.

SCM-002010 [**Optional: PEI, AEI, TA, IAD, MG, SC, SS**] The UC EIs and signaling appliances shall implement the ringing tones and cadences shown in Table 2.9-1, UC Ringing Tones and Cadences.

Table 2.9-1. UC Ringing Tones and Cadences

SIGNAL	FREQUENCIES (HZ)	INTERRUPT RATE	TONE ON	TONE OFF
Alerting (Ring) ROUTINE Calls	20 Hz +/- 1 Hz	10 IPM (Based on an on/off cycle of 6 seconds +/- 600 ms, and 10 on/off cycles per minute)	2000 ms (from 1800 ms to 2200 ms, which is +/- 10%)	4000 ms (from 3600 ms to 4400 ms, which is +/- 10%)
Alerting (Ring) Precedence Calls	20 Hz +/- 1 Hz	30 IPM (Based on an on/off cycle of 2 seconds +/- 200 ms, and 30 on/off cycles per minute)	1640 ms, +/- 10%	360 ms, +/- 10%
LEGEND Hz: Hertz		IPM: Interruptions per Minute		

SCM-002020 [**Optional: AEI**] The AEIs shall be able to provide customized ring tones for incoming precedence calls through the use of pre-recorded audio files (e.g., MP3, AAC [.m4a and .m4r], WAV, WMA, OGG) that are stored in the AEIs. For example, an AEI may store one audio file for use with ringing on incoming PRIORITY calls, another file for use with ringing on incoming IMMEDIATE calls, another file for use with ringing on incoming FLASH calls, and so on. Different audio files can also be associated with different calling numbers when that calling number is used on a Precedence calls (e.g., "This is an IMMEDIATE call from General John Smith.").

SCM-002030 [**Required: PEI, AEI, ATA, IAD, MG, SC, SS**] The EIs and signaling appliances shall implement the UC information signals shown in Table 2.9-2, UC Information Signals.

Table 2.9-2. UC Information Signals

SIGNAL	FREQUENCIES (HZ)	SINGLE TONE LEVEL	COMPOSITE LEVEL	INTERRUPT RATE	TONE ON	TONE OFF
Audible Ringback Precedence Call	440 + 480 (Mixed); +/- 0.5 % for each frequency	-19 dBm0, +/- 1.5 dB	-16 dBm0, +/- 1.5 dB	30 IPM (Based on an on/off cycle of 2 seconds +/- 200 ms, and 30 on/off cycles per minute)	1640 ms ; +/- 10%	360 ms; +/- 10%
Preemption Tone	440 + 620 (Mixed); +/- 0.5 % for each frequency	-19 dBm0, +/- 1.5 dB	-16 dBm0, +/- 1.5 dB		Steady on	

SIGNAL	FREQUENCIES (HZ)	SINGLE TONE LEVEL	COMPOSITE LEVEL	INTERRUPT RATE	TONE ON	TONE OFF
Call Waiting (Precedence Call)	440; +/- 0.5 %	-13 dBm0, +/- 1.5 dB		Continuous at 6 IPM (300 ms +/- 60 ms of CW tone, plus 9700 ms +/- 1940 ms of no CW tone; yields a nominal 10-second cycle which occurs 6 times per minute)	100 ± 20 ms, Three Bursts	9700 ms +/- 1940 ms
Conference Connect Tone	Vendor-provided ascending tones					
Conference Disconnect Tone	852 and 1336 (Alternated at 100 ms intervals); +/- 0.5 % for each frequency	-24 dBm0 +/- 1.5 dB		Steady on	2000 ms +/- 200 ms (per occurrence)	
Override Tone	440; +/- 0.5 percent	-13 dBm0, +/- 1.5 dB		Continuous at 6 IPM (2.5 sec +/- 0.25 sec of tone on, plus 7.5 sec +/- 0.75 sec of tone off; yields a nominal 10-second cycle which occurs 6 times per minute)	2000 ms +/- 200 ms (followed by) 500 ms +/- 50 ms on, and 7500 ms +/- 750 ms off	
Station Busy	480+620			0.5 sec on, 05. sec off (60 IPM)		
All Circuits Busy	480+620			0.25 sec on, 0.25 sec off (120 IPM)		
LEGEND						
CW: Call Waiting			IPM: Interruptions per Minute			
Hz: Hertz			sec: second			

2.9.1.2.2 Announcements

SCM-002040 [**Required: PEI, AEI, SC, SS**] ~~With the exception of the Precedence Access Limitation Announcement (PALA) and the Attendant Queue Announcement (ATQA), t~~The announcements in Table 2.9-3, Required Announcements, ~~are required for all UC Appliances and EIs~~shall be supported, along with all announcements that are associated with a specific NM trunk group and/or code control implementation. Each announcement shall contain a location identification number to be provided by the Government. The appliance playing the announcement (or serving the EI that is playing the announcement) shall be identified by "Switch Name and Location." Announcements shall be capable of being recorded and changed by Government operations and maintenance (O&M) personnel. Additional local messages may

be added and optionally activated, deactivated, or modified via administrative or operational controls.

Table 2.9-3. Required Announcements

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

~~LEGEND~~

~~ATQA: Attendant Queue Announcement~~
~~BNEA: Busy Not Equipped Announcement~~
~~BPA: Blocked Precedence Announcement~~
~~C2: Command and Control~~
~~CW: Call Waiting~~
~~DSN: Defense Switched Network~~
~~ICA: Isolated Code Announcement~~
~~LOC2: Loss of C2 Features~~
~~PALA: Precedence Access Limitation Announcement~~
~~UPA: Unauthorized Precedence Level Announcement~~
~~VCA: Vacant Code Announcement~~

SCM-002045 [Conditional: PEI, AEI, SC, SS] If an announcement in Table 2.9-4, Optional Announcements, is provided, it shall contain a location identification number to be provided by

the Government. The appliance playing the announcement (or serving the EI that is playing the announcement) shall be identified by "Switch Name and Location." Announcements shall be capable of being recorded and changed by Government operations and maintenance (O&M) personnel.

Table 2.9-4. Optional Announcements

ANNOUNCEMENT CONDITION	ANNOUNCEMENT
Precedence Access Threshold (PAT) limitation	Precedence Access Limitation Announcement (PALA). "(Switch name and Location). Precedence access limitation has prevented the completion of your call. Please hang up and try again. This is a recording. (Switch name, location identification number, and Location)."
Attendant Queue Announcement	Attendant Queue Announcement (ATQA). "(Switch name and Location). All attendants are busy now. Please remain on the line until an attendant becomes available or try your call later. This is a recording. (Switch name, location identification number, and Location)."
Loss of C2 Features	Loss of C2 Features Announcement (LOC2). "This is the (Switch name, location identification number, and Location). This call is leaving the Defense Switched Network (DSN). This is a recording."

SCM-002050 [**Removed**~~**Required: PEI, AEI, SC, SS**~~] ~~The ATQA is required for an SC SS, and for PEIs and AEIs served by SCsand SCs internal to SSs.~~

2.9.1.2.3 Loss of C2 Features Announcement

SCM-002060 [**Optional: PEI, AEI, SC, SS**] The LOC2 Features announcement applies only to calls placed via an SC MG or an SS MG to a non-MLPP PRI or CAS trunk and shall be provided IAW the following:

a. Play only for calls above the ROUTINE precedence level.

b. Not required for locally originated calls to non-MLPP PRI or CAS trunks (e.g., PSTN).

c. ~~Required~~ Appropriate for VoIP calls received from the DISN WAN, or calls received from a base MLPP tie trunk via an MG, that ~~is~~ are destined to tandem via an SC MG or SS MG to a non-MLPP PRI or CAS trunk. ~~(assuming there is an available trunk to connect to). (NOTE: CAS interfaces are conditional for the SC MG and SS MG.)~~

d. Play before ringback is provided to the caller.

e. Play before cut-through to the non-MLPP trunk. This prevents ringback from interfering with the announcement.

f. The announcement shall be played into the media stream at the MG point of departure from the DISN to the non-MLPP trunk.

g. The LOC2 announcement is not signaled by AS-SIP.

2.9.1.3 Audio Codecs, Voice Instruments

SCM-002070 [**Required: PEI, AEI, MG**] EIs and MGs shall support the origination and termination of a voice session using the ITU-T Recommendation G.711 codec, including both the μ-law and A-law algorithms.

SCM-002080 [**Required: PEI, AEI, MG**] EIs and MGs shall support the origination and termination of a voice session using the ITU-T Recommendation G.729 or G.729A codec.

SCM-002090 [**Optional: PEI, AEI, MG**] EIs and MGs shall support the origination and termination of a voice session using the ITU-T Recommendation G.723.1 codec.

SCM-002100 [**Optional: PEI, AEI, MG**] EIs and MGs shall support the origination and termination of a voice session using the ITU-T Recommendation G.722.1 codec.

The product is not required to do transcoding between codec types, but shall support, via signaling during session setup, the offer/negotiation between origination and destination EIs of the codec type to be used for the session. However, support for A-law/μ-law conversion is required, as needed, by MGs within the product.

2.9.1.4 VoIP PEI or AEI Telephone Audio Performance

SCM-002110 [**Required: PEI, AEI**] Voice over IP PEIs or AEIs (i.e., handset, headset, and hands-free types) shall comply with Telecommunications Industry Association (TIA)-810-B, November 3, 2006.

2.9.1.5 Voice over IP Sampling Standard

SCM-002120 [**Required: PEI, AEI**] For Fixed-to-Fixed calls, the product shall use 20 ms as the default voice sample length, and as the basis for the voice payload packet size. For other call types, e.g., Fixed-to-Deployable calls, the product shall use different voice sample lengths and voice payload packet sizes, as negotiated during call setup via the Session Description Protocol (SDP).

2.9.1.6 Softphones

A softphone is an end-user software application on an approved operating system that enables a general-purpose computer to function as a telephony PEI/AEI. The softphone application is considered an IP PEI/AEI. It is associated with the IP telephone switch and will be tested on an approved operating system as part of the SUT.

SC and SS support for softphones is optional.

SCM-002130 [**Conditional: PEI, AEI, SC, SS**] If a softphone is supported by an SC or SS, the softphone shall be conceptually identical to a traditional IP “hard” telephone and is required to provide voice features and functionality provided by a traditional IP hard telephone, unless

explicitly stated here within this paragraph. The softphone application in conjunction with a general-purpose computer, including its mouse (point and click) interaction, shall support, as a minimum, the following requirements:

a. Section 2.2, Voice Features and Capabilities.

b. Section 2.9.1.1, Basic.

c. Section 2.9.1.2, Tones and Announcements.

d. Section 2.9.1.3, Audio Codecs, Voice Instruments.

e. Section 2.9.1.4, VoIP PEI or AEI Telephone Audio Performance.

f. Section 2.9.1.5, Voice over IP Sampling Standard.

g. Section 2.9.4, Authentication to SC.

h. Section 2.9.5, End Instrument to ASLAN Interface.

i. Section 6, Network Infrastructure End-to-End Performance. The softphone application shall be exempt from the performance (i.e., packet loss, jitter, latency) requirements specified in Section 6, Network Infrastructure End-to-End Performance; e.g., the PEI/AEI 50-ms latency for the G.711 codec.

j. Section 6.3.2, VVoIP Differentiated Services Code Point.

k. Section 4, Information Assurance.

SCM-002140 [**Conditional: PEI, AEI**] If an EI is a softphone, then it shall inhibit any screen saver or lock screen capability whenever the softphone application is active (i.e., user is on a call). This is to avoid the situation where the user needs to interact with the softphone application via the mouse or keyboard expeditiously (e.g., respond to a new call) but first needs to re-login.

2.9.1.7 DSCP Packet Marking

SCM-002150 [**Required: PEI, AEI, SC, SS**] As part of the session setup process, the SC controls what Differentiated Service Code Point (DSCP) to use in the subsequent session media stream packets. For inter-SC media sessions (across the WAN), and intra-SC media sessions (internal to the enclave), one of the following occurs:

a. The PEI shall be commanded by the SC about which DSCP to insert in the session media stream packets.

b. The PEI shall populate the DSCP marking on its own.

c. The AEI shall populate the DSCP marking on its own.

SCM-002160 [**Required: PEI, AEI, SC, SS**] The exact DSCP method used by the implementer shall comply with Section 6, Network Infrastructure End-to-End Performance. The session's media type (e.g., audio vs. video) and the session's precedence level (R, P, I, F, or FO) shall be used to determine the media stream DSCP for that session.

This DSCP marking data can be provisioned in the AEI or PEI as part of the information downloaded to the EI from a provisioning server after the EI completes its registration with the SC.

2.9.2 Analog and ISDN BRI Telephone Support

SCM-002170 [**Required: SC**] Analog instruments, including secure analog EIs, analog facsimile (fax) EIs, and analog modem EIs, shall be supported by the SC either by a Terminal Adapter, RJ-11 Plain Old Telephone Service (POTS) telephone to RJ-45 Ethernet interface (TA), or an Integrated Access Device (IAD), 4 or more ports of RJ-11 POTS telephone to one port of RJ-45 Ethernet interface.

SCM-002170.a [**Required: TA**] The TA shall support G.711 standards.

SCM-002170.b [**Optional: TA**] The TA shall support V.150.1 Modem Relay and T.38 Fax Relay standards.

SCM-002170.c [**Required: IAD**] The IAD shall support G.711 standards.

SCM-002170.d [**Optional: IAD**] The IAD shall support V.150.1 Modem Relay and T.38 Fax Relay standards.

SCM-002170.e [**Required: EI, TA, IAD, SC, SS**] Analog telephones, when combined with a TA or IAD, together shall comply with TIA-810-B, November 3, 2006.

SCM-002180 [Required: MG Line Card] Analog instruments, including secure analog EIs, analog facsimile EIs, and analog modem EIs, shall be supported by the existing twisted-pair cable plant connected to line cards that are part of the SC MG.

SCM-002180.a [**Required: MG Line Card**] The line card shall support G.711 standards.

SCM-002180.b [**Optional: MG Line Card**] The line card shall support V.150.1 Modem Relay and T.38 Fax Relay standards.

SCM-002180.c [**Required: EI, MG Line Card, SC, SS**] Analog telephones, when connected to a line card, together shall comply with TIA-810-B, November 3, 2006.

NOTE: The acquiring activity should, based on traffic engineering and vendor prices, determine the required number of TAs, IADs, and MG line cards with and without V.150.1 and T.38 capability. V.150.1 and T.38 are required to support analog secure instruments, fax machines, and data modems.

SCM-002180.d [**Optional: SC, SS**] The SC and SS shall support secure analog EIs on analog TAs, IADs, and MG line cards, where the TAs, IADs, and MG line cards support the ITU-T Recommendation V.150.1 standard for Modem Relay.

SCM-002180.e [**Optional: SC, SS**] The SC and SS shall support analog facsimile EIs on analog TAs, IADs, and MG line cards, where the TAs, IADs, and MG line cards support the ITU-T Recommendation T.38 standard for Fax Relay.

SCM-002180.f [**Optional: SC, SS**] The SC and SS shall support analog modem EIs on analog TAs, IADs, and MG line cards, where the TAs, IADs, and MG line cards support the ITU-T Recommendation V.150.1 standard for Modem Relay.

2.9.2.1 ISDN BRI Telephone Support

SCM-002190 [**Optional: SC**] ISDN BRI EIs, including secure ISDN BRI EIs, shall be supported by the SC.

SCM-002200 [**Conditional: SC**] If an SC supports ISDN BRI EIs, they shall be supported by one of the following:

a. A BRI-capable TA that is connected to an Ethernet port.

b. A BRI-capable IAD that is connected to an Ethernet port.

c. The existing twisted-pair cable plant connected to a BRI-capable line card that is part of the SC MG.

SCM-002210 [**Conditional: SC, TA**] If a TA supports standard (nonsecure) ISDN BRI EIs, it shall support the ITU-T Recommendation G.711 standard.

SCM-002220 [**Conditional: SC, IAD**] If an IAD supports standard (nonsecure) ISDN BRI EIs, it shall support the ITU-T Recommendation G.711 standard.

SCM-002230 [**Conditional: SC, TA**] If a TA supports secure ISDN BRI EIs, it shall support both the ITU-T Recommendations G.711 and V.150.1 standards.

SCM-002240 [**Conditional: SC, IAD**] If an IAD supports secure ISDN BRI EIs, it shall support both the ITU-T Recommendations G.711 and V.150.1 standards.

SCM-002250 [**Conditional: SC MG**] If an MG line card supports standard (nonsecure) ISDN BRI EIs, the MG line card shall support the ITU-T Recommendation G.711 standard.

SCM-002260 [**Conditional: SC MG**] If an MG line card supports secure ISDN BRI EIs, it shall support both the ITU-T Recommendations G.711 and V.150.1 standards.

SCM-002270 [**Required: EI**] The ISDN BRI telephones when combined with a BRI-capable TA, BRI-capable IAD, or BRI-capable MG line card shall comply with TIA-810-B, November 3, 2006.

SCM-002280 [**Conditional: SC, TA, IAD, SC MG, EI**] If an SC, TA, IAD, or SC MG support ISDN BRI EIs (both standard and secure), the SC, TA, IAD, or SC MG shall support all the DSN ISDN BRI requirements in the following DSN sections:

a. Section 2.25.1.6, ISDN MLPP BRI.

b. Section 2.25.1.8, MLPP Interactions With Common Optional Features and Services.

c. Section 2.25.1.9, MLPP Interactions With Electronic Key Telephone Systems Features.

d. Section 2.25.2, Signaling.

e. Section 2.25.3, ISDN.

2.9.3 Video End Instrument

Video EIs are considered associated with the SC and must have been designed in conjunction with the SC design.

2.9.3.1 Basic

An IP video EI ~~instrument~~ shall be designed IAW the acquiring activity requirements, but the following capabilities are specifically required or optional as indicated:

SCM-002290 [**Optional: PEI, AEI~~Video EI~~**] DoD CAC card reader.

SCM-002300 [**Required: PEI, AEI~~Video EI~~**] Automatic enabling of the video camera is not permitted after video session negotiation or acceptance. The called party must take a positive action to enable the camera.

SCM-002310 [**Required: PEI, AEI~~Video EI~~**] Display calling number.

SCM-002320 [**Optional: PEI, AEI~~Video EI~~**] Display precedence level of the session.

SCM-002330 [**Optional: PEI, AEI~~Video EI~~**] Support for Multilevel Precedence and Preemption (MLPP) feature.

SCM-002340 [**Required: PEI, AEI~~Video EI~~**] Support for DHCP.

2.9.3.2 Display Messages, Tones, and Announcements

SCM-002350 [**Required: PEI, AEI, SC, SS**] Tones and announcements, as appropriate for voice and video over IP, and as required, in Section 2.9.1.2.1, UC Ringing Tones, Cadences, and Information Signals, and Section 2.9.1.2.2, Announcements, shall be supported by the PEI and AEI, except for the loss of the C2 announcement. These tones and announcements shall be generated locally by the PEI and AEI on the command of the SC, or generated on command of the SC by an internal SC Media Server or an external Media Server connected to the ASLAN, and passed as a media stream to the PEI and AEI. Regardless of how implemented, the Media Server is part of the SC SUT.

2.9.3.3 Video Codecs (Including Associated Audio Codecs)

SCM-002360 [**Required: PEI, AEI**] The product shall support the origination, maintenance, and termination of a video session using the following codecs: one G.xxx and one H.xxx shall be used to create and sustain a video session. (All video and audio capabilities in the PEI or AEI shall be sent to the terminating PEI or AEI for negotiation about which video and audio codec to use for the session.)

SCM-002370 [**Required: PEI, AEI**] Video PEIs and AEIs shall support, at a minimum, G.711 Pulse Code Modulation (PCM), where PCM has a static payload type value of 0 and a clock rate of 8000. The PCM shall support both the μ-law and A-law algorithms.

SCM-002380 [**Optional: PEI, AEI**] It is recommended that video PEIs and AEIs support other audio codecs in addition to G.711 PCM. Recommended audio codecs include the following:

a. ITU-T Recommendation G.722, where G.722 has a static payload type value of 9 and a clock rate of 8000.

b. ITU-T Recommendation G.722.1, where G.722.1 has the encoding name "G7221", a clock rate of 16000, and a standard bit rate of 24 Kbps or 32 Kbps.

c. ITU-T Recommendation G.723.1, where G.723.1 has the encoding name "G723", a clock rate of 8000, and standard bit rates of 5.3 Kbps and 6.3 Kbps.

d. ITU-T Recommendation G.729, where G.729 has the encoding name "G729", a clock rate of 8000, and a standard bit rate of 8 Kbps.

e. ITU-T Recommendation G.729 Annex A (G.729A), where G.729A also has the encoding name "G729", a clock rate of 8000, and a standard bit rate of 8 Kbps.

SCM-002390 [**Required: PEI, AEI**] Video PEI and AEI shall support, at a minimum, the following video codecs:

a. ITU-T Recommendation H.263-2000.

b. ITU-T Recommendation H.264

   SCM-002390.a [**Optional**] ITU-T Recommendation H.264, Scalable Video Coding (SVC).

   SCM-002390.b [**Optional**] ITU-T Recommendation H.261.

2.9.3.4 H.323 Video Teleconferencing

UC support for H.323 video teleconferencing (VTC) is optional.

This section provides the requirements and guidelines for H.323 VTC systems and end points when interfaced to the DSN network:

SCM-002400 [**Optional**] The H.323 VTC system and end points should meet the requirements of Federal Telecommunications Recommendation (FTR) 1080B-2002.

SCM-002410 [**Optional**] The H.323 VTC features and functions used in conjunction with IP network services should meet the requirements of H.323 in accordance with FTR 1080B-2002, and H.323 video EIs should meet the tagging requirements as specified in Section 7, Network Edge Infrastructure.

SCM-002420 [**Required**] A loss of any conferee on a multipoint H.323 videoconference shall not terminate or degrade the DSN service supporting H.323 VTC connections of any of the other conferees on the videoconference.

SCM-002430 [**Optional**] An audio add-on interface shall be provided on H.323 VTC equipment in accordance with Section 3.7, Customer Premise Equipment.

SCM-002440 [**Conditional**] If an H.323VTC system or end point uses an integrated BRI interface to connect to the DSN, then it shall be in conformance with the requirements associated with a TA as described in Section 3.7, Customer Premise Equipment, and Section 2.9.2.1, ISDN BRI Telephone Support.

SCM-002450 [**Conditional**] If a VTC system or end point uses a serial interface to another device, such as a cryptographic device or TA, for eventual connection to the DSN, it shall be in conformance with the requirements for that serial interface as described in FTR 1080B-2002.

SCM-002460 [**Required**] Physical, electrical, and software characteristics of a video teleconferencing unit (VTU) system or end point that is used in the DSN network shall not degrade, or impair, the serving DSN switch and its associated network operations.

As noted in the introduction to Section 2.3.3, ASAC Requirements for the SC and the SS Related to Video Services, the SC and the SS will process only AS-SIP video. H.323 video will be processed by a gatekeeper appliance.

2.9.4 Authentication to SC

SCM-002470 [**Required: PEI, AEI, SC**] The PEI and AEI shall each be capable of authenticating itself to its associated SC and vice versa IAW Section 4, Information Assurance.

2.9.5 End Instrument to ASLAN Interface

SCM-002480 [**Required: PEI, AEI**] The interface to the ASLAN shall be IAW Ethernet (IEEE 802.3) Local Area Network (LAN) technology. The 10-Mbps and 100-Mbps Fast Ethernet (IEEE 802.3u) shall be supported.

2.9.6 Operational Framework for AEIs ~~and Video EIs~~

This section contains SC and AS-SIP EI requirements to support a generic, multivendor-interoperable interface between a VVoIP SC and an AS-SIP VVoIP EI, which can be a voice EI, a secure voice EI, or a video EI. This generic, multivendor-interoperable interface uses AS-SIP protocol instead of the various vendor-proprietary SC-to-EI protocols.

~~NOTE: The SC must be a supplicant for AEIs, but the SC SUT does not need to include AEIs.~~

NOTE: ITU Recommendation H.323 and Internet Engineering Task Force (IETF) SIP (commercial SIP, not DISA-specified AS-SIP) are both considered vendor-proprietary SC-to-EI protocols here.

2.9.6.1 Requirements for Supporting AS-SIP EIs

This section provides the requirements for supporting an AS-SIP interface between SCs and AS-SIP EIs. This section focuses on what capabilities need to be added to SCs and AS-SIP EIs to support a generic AS-SIP interface between them. ~~(Instances of SS here refer to the internal SC within the SS.)~~

SCM-002490 [**Required: SC, AEI~~SS, AS-SIP Voice EI, AS-SIP Secure Voice EI, AS-SIP Video EI~~**] The AS-SIP EIs (voice, secure voice, and video) shall follow all of the previous requirements for EIs (voice and video, with secure voice EIs following the previous requirements for voice EIs), except for those requirements that involve vendor-proprietary SC-to-EI signaling.

SCM-002500 [**Required: SC, AEI~~SS, AS-SIP Voice EI, AS-SIP Secure Voice EI, AS-SIP Video EI~~**] The SCs and AS-SIP EIs (voice, secure voice, and video) shall support mutual authentication using AS-SIP and TLS signaling instead of vendor-proprietary signaling. That is, each AS-SIP EI shall authenticate itself with its serving SC using AS-SIP and TLS signaling, and each SC shall authenticate itself with the AS-SIP EIs that it serves using AS-SIP and TLS signaling.

SCM-002510 [**Required: SC~~, SS~~**] The SC shall allow a single AS-SIP EI to support voice, secure voice, and video capabilities. In this case, the SC shall support that EI using the combined requirements for an AS-SIP voice EI, an AS-SIP secure voice EI, and an AS-SIP video EI, as given below. The SC shall also allow a single AS-SIP EI to support either of the following subset of these three capabilities:

a. Voice and Secure Voice.

b. Voice and Video.

SCM-002520 [**Optional: AEI~~AS-SIP Voice EI, AS-SIP Secure Voice EI, AS-SIP Video EI~~**] A single AS-SIP EI shall support voice, secure voice, and video capabilities. In this case, the EI shall support those capabilities IAW the combined requirements for an AS-SIP voice EI, an

AS-SIP secure voice EI, and an AS-SIP video EI, as given in Section 2.9.6.2, Requirements for AS-SIP Voice EIs; Section 2.9.6.3, Requirements for AS-SIP Secure Voice EIs; and Section 2.9.6.4, Requirements for AS-SIP Video EIs.

SCM-002530 [**Optional: AS-SIP Voice EI, AS-SIP Secure Voice EI**] A single AS-SIP EI shall support both voice and secure voice capabilities. In this case, the EI shall support those capabilities IAW the combined requirements for an AS-SIP voice EI and an AS-SIP secure voice EI, as given in Section 2.9.6.2, Requirements for AS-SIP Voice EIs, and Section 2.9.6.3, Requirements for AS-SIP Secure Voice EIs.

SCM-002540 [**Optional: AS-SIP Voice EI, AS-SIP Video EI**] A single AS-SIP EI shall support both Voice and Video capabilities. In this case, the EI shall support those capabilities IAW the combined requirements for an AS-SIP voice EI and an AS-SIP video EI, as given in Section 2.9.6.2, Requirements for AS-SIP Voice EIs, and Section 2.9.6.4, Requirements for AS-SIP Video EIs.

SCM-002550 [**Required: AS-SIP Secure Voice EI**] An AS-SIP secure voice EI shall also support the capabilities of an AS-SIP Voice EI IAW the AS-SIP voice EI requirements given in Section 2.9.6.2, Requirements for AS-SIP Voice EIs. The AS-SIP secure voice EI shall support these capabilities for "voice communication in the clear" using the Audio media type and the G.7XX codecs.

NOTE: (If an AS-SIP Secure Voice EI is a "Modem Relay Preferred" EI and supports only Audio media using the "NoAudio" payload type, then the AS-SIP secure voice EI is not required to support the G.7XX codecs.)

2.9.6.2 Requirements for AS-SIP Voice EIs

SCM-002560 [~~**Required**~~**Optional: SC**~~**, SS**~~] The SCs shall support AS-SIP voice EIs that use AS-SIP for EI-to-SC signaling. The SCs shall support these AS-SIP voice EIs using the AS-SIP SC-to-AS-SIP-EI interface defined in Section 2.9.7, Multiple Call Appearance Requirements for AS-SIP EIs, and in AS-SIP 2013.

SCM-002570 [**Required: AS-SIP Voice EI**] The AS-SIP voice EIs shall support AS-SIP for EI-to-SC signaling. These AS-SIP voice EIs shall support the AS-SIP SC-to-AS-SIP-EI interface defined in Section 2.9.7, Multiple Call Appearance Requirements for AS-SIP EIs, and in AS-SIP 2013.

SCM-002580 [**Required: SC,** ~~**SS,**~~ **AS-SIP Voice EI**] The SCs and AS-SIP Voice EIs shall support the following supplementary services for voice calls, consistent with Section 2.2, Voice Features and Capabilities, using AS-SIP signaling.

a. Precedence Call Waiting [**Required**].

b. Call Forwarding [**Required**].

c. Call Transfer [**Required**].

d. Call Hold [**Required**].

e. UC Conferencing [**Optional**].

f. Three-Way Calling [**Required**].

g. Calling Number Delivery [**Required**].

(1) Calling Name [**Optional**].

(2) Calling Party Org and Location [**Optional**].

h. Call Pickup [**Optional**].

SCM-002590 [**Removed~~Required: SC, SS, AS-SIP Voice EI~~**] ~~The SCs and AS-SIP voice EIs shall support a mechanism to limit the total number of voice calls at that EI at any given time.~~

~~The SC shall keep track of the total number of voice calls at the AS-SIP voice EI at all times, where this total number includes active calls, calls on hold, additional calls that are being offered to the EI using CW, and additional calls that are being originated by the EI using Call Transfer or TWC. The SC shall compare this total number of calls to the voice call limit for that EI, and shall block further voice call requests to and from the AS-SIP EI once this voice call limit is reached.~~

SCM-002600 [**Removed~~Required: SC, SS, AS-SIP Voice EI~~**] ~~For AS-SIP voice EIs, the voice call limit depends on the number of voice call appearances supported on the EI. The AS-SIP voice EIs are required to support two voice call appearances for one DSN number in this document (per Section 2.9.7, Multiple Call Appearance Requirements for AS-SIP EIs). But one of these call appearances might not be used, because the SC is configured to support only one voice call appearance for one DSN number on this EI.~~

~~As a result, the voice call limit that the SC maintains for the AS-SIP voice EI depends on whether the SC is configured to support one call appearance or two call appearances for that EI.~~

~~a. When the SC is configured to support two call appearances on an AS-SIP voice EI, the SC shall use a voice call limit of "Two" for that EI.~~

~~b. When the SC is configured to support one call appearance on an AS-SIP voice EI (even though the EI might support two call appearances), the SC shall use a voice call limit of "One" for that EI.~~

2.9.6.3 Requirements for AS-SIP Secure Voice EIs

SCM-002610 [**~~Required~~Optional: SC~~, SS~~**] The SCs shall support AS-SIP secure voice EIs that use AS-SIP for EI-to-SC signaling. The SC~~s~~ shall support these AS-SIP secure voice EIs using the AS-SIP SC-to-AS-SIP-EI interface defined in Section 2.9.7, Multiple Call Appearance Requirements for AS-SIP EIs, and in AS-SIP 2013.

SCM-002620 [**Required: AS-SIP Secure Voice EI**] AS-SIP Secure Voice EIs shall support AS-SIP for EI-to-SC signaling. These AS-SIP secure voice EIs shall support the AS-SIP SC-to-

AS-SIP-EI interface defined in Section 2.9.7, Multiple Call Appearance Requirements for AS-SIP EIs, and in AS-SIP 2013.

SCM-002630 [**Required: SC~~, SS~~**] The SC~~s and SSs~~ shall support the following supplementary services for voice calls on AS-SIP secure voice EIs, consistent with Section 2.2, Voice Features and Capabilities, using AS-SIP signaling:

a. Precedence Call Waiting [**Required**].

b. Call Forwarding [**Required**].

c. Call Transfer [**Required**].

d. Call Hold [**Required**].

e. UC Conferencing [**Optional**].

f. Three-Way Calling [**Required**].

g. Calling Number Delivery [**Required**].

(1) Calling Name [**Optional**].

(2) Calling Party Org and Location [**Optional**].

h. Call Pickup [**Optional**].

NOTE: An AS-SIP secure voice EI is not required to support any supplementary services for secure voice calls (calls using SCIP/modem relay media).

SCM-002640 [**Required: AS-SIP Secure Voice EI**] An AS-SIP secure voice EI shall be able to operate as an AS-SIP voice EI for voice calls (calls using Audio media and not SCIP/modem relay media).

SCM-002650 [**Required: AS-SIP Secure Voice EI**] An AS-SIP secure voice EI shall be able to operate as an AS-SIP voice EI for the portions of calls where Audio media is used (and SCIP/modem relay media is not used). This AS-SIP secure voice EI requirement applies during the time before a call converts from Audio media to SCIP/modem relay media, and during the time after a call converts from SCIP/modem relay media back to Audio media. This requirement also applies to a call that never converts to SCIP/modem relay media, and uses Audio media for the lifetime of the call.

SCM-002660 [**Required: AS-SIP Secure Voice EI**] An AS-SIP Secure Voice EI shall not allow the end user to activate any supplementary services when a call on that EI is operating in "Secure Voice" mode, and SCIP/modem relay media is being used.

When an end user tries to use a supplementary service when a call on the EI is operating in secure voice mode, the EI shall prevent the user from activating the service, and shall return an error indication (i.e., a locally generated tone and a visual display) back to that user. The error

indication shall indicate that the end user must return the secure voice call to a "Clear Voice" call before the supplementary service can be used.

SCM-002670 [**Required: AS-SIP Secure Voice EI**] Whenever the local end user returns the Secure Voice call to a Clear Voice call, or the remote end user returns the secure voice call to a clear voice call, the AS-SIP secure voice EI shall return a "clear voice confirmation" indication (i.e., a locally generated tone and a visual display) to the local end user. This lets the local end user know that the call has returned from secure voice mode to clear voice mode. It also lets them know that they are no longer communicating in secure voice mode, and lets them know that they can activate supplementary services if desired.

SCM-002680 [**Required: AS-SIP Secure Voice EI**] An AS-SIP secure voice EI shall support supplementary services when all calls on that EI are operating in clear voice mode, and Audio media alone is being used.

When an end user tries to use a supplementary service when all calls on the EI are operating in clear voice mode, the EI shall allow the user to activate the service, and shall process the service request accordingly. This requirement shall also apply after the user has returned a secure voice call to a clear voice call (e.g., in response to an error indication from the EI during the secure voice call), and then tries to use a supplementary service on the clear voice call.

SCM-002690 [**Required: AS-SIP Secure Voice EI**] When operating as an AS-SIP voice EI (i.e., all EI calls are in clear voice mode), an AS-SIP secure voice EI shall support the following supplementary services for voice calls, consistent with Section 2.2, Voice Features and Capabilities, using AS-SIP signaling:

a. Precedence Call Waiting [**Required**].
b. Call Forwarding [**Required**].
c. Call Transfer [**Required**].
d. Call Hold [**Required**].
e. UC Conferencing [**Optional**].
f. Three-Way Calling [**Required**].
g. Calling Number Delivery [**Required**].
h. Call Pickup [**Optional**].

SCM-002700 [**Required: AS-SIP Secure Voice EI**] When an AS-SIP secure voice EI has a secure voice call active, the SC sends that EI a Precedence CW or ROUTINE CW indication, and the EI user attempts to place the secure voice call on hold and answer the waiting call, the EI shall send an error indication (tone and display) to the user as described previously. If the user converts the secure voice call back to a clear voice call, and then tries to place the clear voice call on hold and answer the waiting call, the EI shall accept the user's request and relay it to the SC.

SCM-002710 [**Required: AS-SIP Secure Voice EI**] When an AS-SIP secure voice EI has a secure voice call active, and the EI user attempts to activate Call Transfer by placing the secure voice call on hold and setting up another call, the EI shall send an error indication (tone and display) to the user as described previously. If the user converts the secure voice call back to a clear voice call, and then tries to activate Call Transfer by placing the clear voice call on hold and setting up another call, the EI shall accept the user's request and relay it to the SC.

SCM-002720 [**Required: AS-SIP Secure Voice EI**] When an AS-SIP secure voice EI has a secure voice call active, and the EI user attempts to activate Call Hold by placing the secure voice call on hold, the EI shall send an error indication (tone and display) to the user as described previously. If the user converts the secure voice call back to a clear voice call, and then tries to activate Call Hold by placing the clear voice call on hold, the EI shall accept the user's request and relay it to the SC.

SCM-002730 [**Required: AS-SIP Secure Voice EI**] When an AS-SIP secure voice EI has a secure voice call active, and the EI user attempts to activate TWC by placing the secure voice call on hold and setting up another call, the EI shall send an error indication (tone and display) to the user as described previously. If the user converts the secure voice call back to a clear voice call, and then tries to activate TWC by placing the clear voice call on hold and setting up another call, the EI shall accept the user's request and relay it to the SC.

SCM-002740 [**Required: AS-SIP Secure Voice EI**] When an AS-SIP secure voice EI has a secure voice call active, and the SC sends that EI a Precedence CW or Routine CW indication and provides Calling Party ID and Precedence Level information within the CW indication, the AS-SIP Secure Voice EI shall display both the Calling Party ID and Precedence Level information to the called user at the EI, as part of the CW indication that the EI delivers to the called user. (This gives the called users a basis for deciding whether to answer or ignore a "waiting" voice call when they have a secure voice call active on their EI. "Ignore," as used here, means that the user allows the call to be forwarded by the CFDA feature or deflected by the Precedence Call Diversion feature.)

2.9.6.4 Requirements for AS-SIP Video EIs

SCM-002750 [~~**Required**~~**Optional: SC**~~**, SS**~~] The SC~~s~~ shall support AS-SIP Video EIs that use AS-SIP for EI-to-SC signaling. The SCs shall support these AS-SIP Video EIs using the AS-SIP SC-to-AS-SIP-EI interface defined in Section 2.9.7, Multiple Call Appearance Requirements for AS-SIP EIs, and in AS-SIP 2013.

SCM-002760 [**Required: AS-SIP Video EI**] The AS-SIP Video EIs shall support AS-SIP for EI-to-SC signaling. These AS-SIP Video EIs shall support the AS-SIP SC-to-AS-SIP-EI interface defined in Section 2.9.7, Multiple Call Appearance Requirements for AS-SIP EIs, and in AS-SIP 2013.

SCM-002770 [**Optional: SC, ~~SS,~~ AS-SIP Video EI**] The SC~~s, SSs,~~ and AS-SIP Video EI~~s~~ shall support the following supplementary services for video calls, as an extension of the requirement to support these services for voice calls in Section 2.2, Voice Features and Capabilities:

a. Precedence Call Waiting.
b. Call Forwarding.
c. Call Transfer.
d. Call Hold.
e. UC Conferencing.
f. Three-Way Calling.
g. Calling Number Delivery.
h. Call Pickup.

SCM-002780 [**Optional: SC, ~~SS,~~ AS-SIP Video EI**] The SC, SS, and the AS-SIP Video EI shall support the transmission of H.281 far-end camera control (FECC) messages when used in conjunction with video systems (e.g., MCUs and VTC bridges) that employ far-end camera control capabilities. The specific requirements for implementing this capability are provided in AS-SIP 2013, Section 10.3.6.1, General H.224 Control Channel for Far-End Camera Control Messages, and in Section 10.3.6, FECC.

SCM-002790 [**Optional: SC, SS, AS-SIP Video EI**] The SC, SS, and the AS-SIP Video EI shall support (when used in multipoint conferences) the Binary Floor Control Protocol (BFCP) that uses a floor control server to manage the control of media streams that are shared resources (i.e., "floors") as specified in RFC 4582. The specific requirements for implementing this capability are provided in Section 5.3.4.9.7.5, SDP Attributes for Binary Floor Control Protocol Streams.

SCM-002800 [**Conditional: SC, ~~SS,~~ AS-SIP Video EI**] If the SC~~s, SSs,~~ and AS-SIP Video EI~~s~~ support the optional supplementary services noted above (within Section 2.9.6.4), they shall support them using AS-SIP signaling.

SCM-002810 [**Removed~~Required: SC, SS, AS-SIP Video EI~~**] ~~The SCs and AS-SIP Video EIs shall support a mechanism to limit the total number of video calls at that EI at any given time.~~

~~The SC shall keep track of the total number of video calls at the AS-SIP Video EI at all times. The SC shall compare this total number of calls to the configured video call limit for that EI, and shall block further video call requests to and from the AS-SIP EI once this video call limit is reached.~~

SCM-002820 [**Optional: SC, ~~SS,~~ AS-SIP Video EI**] The SC~~, SS,~~ and the AS-SIP Video EI shall support a mechanism to identify the amount of video call bandwidth, expressed in VSUs, in use at that EI at any given time.

A 500-Kbps video call uses one VSU of bandwidth, a 1-Mbps video call uses two VSUs of bandwidth, a 2.5-Mbps video call uses five VSUs of bandwidth, and a 4.0-Mbps video call uses eight VSUs of bandwidth.)

SCM-002830 [**Optional: SC, ~~SS,~~ AS-SIP Video EI**] The SC~~, SS,~~ and the AS-SIP Video EI shall support the conversion of a lower-bandwidth video call to a higher-bandwidth video call (and vice-versa), using AS-SIP re-INVITE messages on the SC-to-AS-SIP-EI interface to signal the bandwidth change.

SCM-002840 [**Optional: SC, ~~SS,~~ AS-SIP Video EI**] The SC~~, SS,~~ and the AS-SIP Video EI shall support the conversion of a video call to a voice call (and vice-versa), using AS-SIP re-INVITE messages on the SC-to-AS-SIP-EI interface to signal the media change.

2.9.6.5 AS-SIP Video EI Features

SCM-002850 [**Conditional: AS-SIP Video EI**] If the AS-SIP Video EI supports FECC based on the following:

- ITU-T Recommendation H.224.
- ITU-T Recommendation H.281.

Then the EI shall support all the AS-SIP and SDP protocol requirements for FECC in the following:

- AS-SIP 2013, Section 10.3.6.1, General H.224 Control Channel for Far End Camera Control Messages.

SCM-002860 [**Conditional: AS-SIP Video EI**] If the AS-SIP Video EI supports BFCP based on the following:

- RFC 4582.
- RFC 4583.

Then the EI shall support all the AS-SIP and SDP protocol requirements for BFCP Streams in the following:

- AS-SIP 2013, Section 10.3.3.2.1, SDP Requirements for the Binary Control Protocol (Based on RFC 4583).

SCM-002870 [**Conditional: AS-SIP Video EI**] If the AS-SIP Video EI supports Video Channel Flow Control [VCFC] based on the following:

- RFC 4585.

Then the EI shall support all the AS-SIP and SDP protocol requirements for VCFC in the following:

- AS-SIP 2013, Section 10.3.4, Video Channel Flow Control.

SCM-002880 [**Conditional: AS-SIP Video EI**] If the AS-SIP Video EI supports Video Channel Flow Control (VCFC) based on the following:

- RFC 4585.

Then the EI shall support all of the following sections of RFC 4585:

- Section 3.1, Compound RTCP Feedback Packets.
- Section 3.2, Algorithm Outline.
- Section 3.3, Modes of Operation.
- Section 3.4, Definitions and Algorithm Overview.
- Section 3.5, AVPF RTCP Scheduling Algorithm, and all subsections 3.5.1 – 3.5.4, inclusive.
- Section 3.6.1, ACK Mode.
- Section 3.6.2, NACK Mode.
- Section 4.1, Profile Identification.
- Section 4.2, RTCP Feedback Capability Attribute.
- Section 4.3, RTCP Bandwidth Modifiers.
- Section 5, Interworking and Coexistence of AVP and AVPF Entities.
- Section 6, Format of RTCP Feedback Messages.
- Section 6.1, Common Packet Format for Feedback Messages.
- Section 6.2, Transport Layer Feedback Messages (including 6.2.1 Generic NACK).
- Section 6.3, Payload-Specific Feedback Messages, including:
  - Section 6.3.1, Picture Loss Indication (PLI) and its subsections.
  - Section 6.3.2, Slice Loss Indication (SLI) and its subsections.
  - Section 6.3.3, Reference Picture Selection Indication (RPSI) and its subsections.
- Section 6.4, Application Layer Feedback Messages.

SCM-002890 [**Conditional: AS-SIP Video EI**] If the AS-SIP Video EI supports Video Channel Fast Update Requests (VCFURs) based on the following:

- RFC 5104.

Then the EI shall support all the AS-SIP and SDP protocol requirements for VCFUR in the following:

- AS-SIP 2013, Section 10.3.5, Video Channel Fast Update Requests.

SCM-002900 [**Conditional: AS-SIP Video EI**] If the AS-SIP Video EI supports VCFUR, Full Intra Request (FIR) payload-specific feedback message shall be used for implementing VCFUR.

2.9.7 Multiple Call Appearance Requirements for AS-SIP EIs

2.9.7.1 Multiple Call Appearance Scenarios

The AS-SIP 2013 document contains requirements on "Multiple Appearances" The first of these requirements is as follows:

> "IP ~~end instruments~~EI MUST be limited to two ~~(2)~~ appearances per ~~DN~~ Directory number and limited to, at most, two ~~(2) DNs~~directory numbers."

This requirement applies for both voice (audio) sessions and for video sessions. An "appearance" or "call appearance" on an IP EI can be used to originate or terminate either a voice session or a video session. An existing voice session on an EI call appearance can be preempted by a new incoming video session of higher precedence, and an existing video session on an EI call appearance can be preempted by a new incoming voice session of higher precedence.

This requirement is being extended to AS-SIP EIs here, with two exceptions:

1. On AS-SIP EIs, support for two appearances per DN and one DN per phone is required. But support for two appearances per DN and two DNs per phone is not required.
2. On AS-SIP EIs, support for call appearances is required for voice calls on AS-SIP Voice EIs, and for Secure voice calls on AS-SIP Secure Voice EIs. But support for call appearances is not required for video calls on AS-SIP Video EIs.

An AS-SIP Video EI is required to support only one DN, and to support one video call on that DN at a time. An AS-SIP Video EI is not required to use a call appearance to support this single video call. An AS-SIP Video EI that is also an AS-SIP Voice EI (and supports voice calls and two voice call appearances) is not required to use either of its voice call appearances to support this video call. The following requirements and recommendations also apply to the SCs that serve the AS-SIP EIs, and to the SC-to-AS-SIP-EI interface:

1. An AS-SIP Voice EI must be able to support two simultaneous voice calls (media type equals Audio) using two call appearances of the same DN (10-digit DSN number).
2. When operating as an AS-SIP Voice EI (no Secure voice calls active), an AS-SIP Secure Voice EI must be able to support two simultaneous voice calls (media type equals Audio) using two call appearances of the same DN.
3. When operating as an AS-SIP Secure Voice EI (one secure voice call active), an AS-SIP Secure Voice EI must be able to support one Secure voice call (media type equals modem relay) using one of its two call appearances. The EI may also support a voice call (media type equals Audio) on Hold using its other call appearance in this case.
4. An AS-SIP Video EI must be able to support one video call (media type equals Video). If the AS-SIP EI is also an AS-SIP Voice EI or AS-SIP Secure Voice EI, the EI is not required to use either of its voice call appearances to support the video call.

2.9.7.2 Multiple Call Appearances – Specific Requirements

SCM-002910 [**Required: AS-SIP Voice EI, AS-SIP Secure Voice EI**] An AS-SIP EI shall allow multiple call appearances of the same DN (10-digit DSN number) to be assigned to it. An AS-SIP EI shall allow at least two appearances of the same DN to be assigned to it. This requirement does not apply to AS-SIP Video EIs.

SCM-002920 [**Required: AS-SIP Voice EI, AS-SIP Secure Voice EI**] An AS-SIP EI shall allow each call appearance of a DN to be used for voice and secure voice calls to and from that DN. This requirement does not apply to AS-SIP Video EIs. Dedication of call appearances on an EI to a particular call type (Voice, Secure Voice, or Video) is not a requirement.

SCM-002930 [**Required: AS-SIP Video EI**] An AS-SIP Video EI shall support at least one DN for video calls, and support at least one video call on that DN at a time. An AS-SIP Video EI is not required to use a call appearance to support this video call. An AS-SIP Video EI that is also an AS-SIP Voice EI (and supports voice calls and two voice call appearances) is not required to use either of its voice call appearances to support this video call.

SCM-002940 [**Required: AS-SIP Voice EI**] An AS-SIP Voice EI shall be able to support two simultaneous voice calls (media type equals Audio) using two call appearances of the same DN (10-digit DSN number).

SCM-002950 [**Required: AS-SIP Secure Voice EI**] When operating as an AS-SIP Voice EI (no Secure voice calls active), an AS-SIP Secure Voice EI shall be able to support two simultaneous voice calls (media type equals Audio) using two call appearances of the same DN.

SCM-002960 [**Required: AS-SIP Secure Voice EI**] When operating as an AS-SIP Secure Voice EI (one Secure voice call active), an AS-SIP Secure Voice EI shall be able to support one Secure voice call (media type equals modem relay) using one of its two call appearances. The EI may also support a voice call (media type equals Audio) on Hold using its other call appearance in this case.

SCM-002970 [**Required: AS-SIP Video EI**] An AS-SIP Video EI shall be able to support at least one video call (media type equals Video). If the AS-SIP EI is also an AS-SIP Voice EI or AS-SIP Secure Voice EI, the EI is not required to use either of its voice call appearances to support the video call

SCM-002980 [**Required: SC, ~~SS,~~ AS-SIP Voice EI, AS-SIP Secure Voice EI**] The SC and AS-SIP EI and SC shall allow multiple media types to be requested (as part of SDP capability declaration) in the same EI-to-SC INVITE message.

SCM-002990 [**Required: SC, ~~SS,~~ AS-SIP Voice EI, AS-SIP Secure Voice EI**] The SC and AS-SIP EI shall allow multiple media types to be requested (as part of SDP capability declaration) in the same SC-to-EI INVITE message.

SCM-003000 [**Required: AS-SIP Voice EI, AS-SIP Secure Voice EI**] An AS-SIP EI shall allow only one voice call (voice or secure voice) to be associated with one call appearance at a time. An AS-SIP EI shall not allow multiple calls (e.g., one active call and one held call) to be associated with the same call appearance at the same time.

SCM-003010 [**Required: AS-SIP Voice EI, AS-SIP Secure Voice EI**] An AS-SIP EI shall allow multiple voice calls to be associated with itself, as long as each call is associated with one, and only one, call appearance on that AS-SIP EI. AN AS-SIP EI shall allow each call associated with the EI to be in either an "active" state, a "held" state, or a "call in progress" state (a call in the process of being established).

SCM-003020 [**Required: AS-SIP Secure Voice EI**] An AS-SIP secure voice EI shall allow only one secure voice call (media equals modem relay) to be associated with the EI at a time, and allow that call to be associated with one call appearance on that EI. The AS-SIP EI shall allow this secure voice call to be in only an "active" state, and not in a "held" state, or a "call in progress" state.

SCM-003030 [**Required: AS-SIP Secure Voice EI**] When a secure voice call is active, the AS-SIP secure voice EI shall also allow an additional voice call (media equals Audio) to be associated with the EI, and allow that call to be associated with the second call appearance on that EI. The AS-SIP EI shall allow this additional voice call to be in only a "held" state or a "call in progress" state (a call in the process of being established), and not in an "active" state. For example, if the CW feature is assigned, the EI shall allow an active Secure voice call on one call appearance and an incoming "in progress" voice call on the other call appearance.

SCM-003040 [**Required: AS-SIP Voice EI, AS-SIP Secure Voice EI**] An AS-SIP EI shall allow a call on a single call appearance to transition from one media type to another, using an in-band media message for a media change (like a V.150.1 modem relay SSE message). An AS-SIP EI shall support transitions from voice media to secure voice media, and transitions from secure voice media to voice media.

2.9.7.3 Multiple Call Appearances – Interactions With Precedence Calls

This section describes the requirements for handling incoming precedence calls (i.e., PRIORITY, IMMEDIATE, FLASH, and FLASH OVERRIDE) on the SC-to-AS-SIP-EI interface, for an AS-SIP Voice EI or AS-SIP Secure Voice EI that supports multiple appearances of a single DN. These requirements are not currently applicable to AS-SIP video EIs because these EIs do not support multiple call appearances of a single DN.

SCM-003050 [**Required: AS-SIP Voice EI, AS-SIP Secure Voice EI**] When an incoming precedence call is offered on a multiple-call-appearance AS-SIP EI, the EI shall do all of the following:

a. Play a precedence ringing tone for that call.

b. Offer the call on the next available call appearance for the indicated DN.

c. Provide a visual precedence level display to the called user.

d. Allow the called user to place any currently active call (on the currently active appearance) on hold and answer the incoming precedence call on the new call appearance.

SCM-003060 [**Required: SC, ~~SS,~~ AS-SIP Voice EI, AS-SIP Secure Voice EI**] When the called user of an incoming precedence call offered on a multiple-call-appearance AS-SIP EI, does not answer that precedence call, the call shall be forwarded IAW the Call Forwarding Don't Answer feature, or diverted to a designated UC DN IAW the Precedence Call Diversion feature.

SCM-003070 [**Required: AS-SIP Secure Voice EI**] If the AS-SIP EI is a secure voice EI and the currently active call is a secure voice call using modem relay media, the EI shall require the called user to convert the currently active call back to a voice call using Audio media before placing it on hold. The AS-SIP EI shall not allow a Secure voice call using modem relay media to be placed on hold.

SCM-003080 [**Required: AS-SIP Voice EI, AS-SIP Secure Voice EI**] The AS-SIP voice EI shall offer subsequent incoming precedence calls to the end user, up to the total number of call appearances supported by the EI. For each additional incoming precedence call, the AS-SIP EI shall offer the call as described previously, and allow the end user to place the existing active call on hold (if it is a voice call using Audio media) and answer the precedence call as described previously. The ability to place an existing call on hold and answer a new precedence call shall be supported until the AS-SIP EI is saturated (i.e., all of its call appearances are in use).

SCM-003090 [**Required: AS-SIP Voice EI, AS-SIP Secure Voice EI**] When an AS-SIP EI is saturated, and an incoming precedence call is made to that EI, the EI shall determine the lowest precedence call from all of the calls on all of the EI's call appearances (including those calls that are on hold), and shall preempt that call.

SCM-003100 [**Required: AS-SIP Voice EI, AS-SIP Secure Voice EI**] If the lowest precedence call is a call on hold, then the AS-SIP EI shall send a preemption tone to the remote party on this held call (the party on hold).

SCM-003110 [**Required: AS-SIP Voice EI, AS-SIP Secure Voice EI**] The AS-SIP EI shall also send a preemption tone to the local party on this held call by playing this tone on the EI call appearance for this call.

SCM-003120 [**Required: AS-SIP Voice EI, AS-SIP Secure Voice EI**] After a preset period, the AS-SIP EI shall clear this call on hold and shall play a precedence ringing tone and provide a precedence level display for the call appearance from which the held call has been cleared.

As a result, the called user will hear the preemption tone followed by the precedence ringing tone (indicating that the call on hold has been dropped), and see the precedence level of the new call on the AS-SIP EI's display.

SCM-003130 [**Required: AS-SIP Voice EI, AS-SIP Secure Voice EI**] The AS-SIP EI shall then give the called user the option of answering the call, or letting it forward to an alternate party (if CFDA is assigned), or letting it divert to an attendant (if Precedence Call Diversion is assigned).

SCM-003140 [**Required: AS-SIP Voice EI, AS-SIP Secure Voice EI**] If the lowest precedence call is not a call on hold, but instead is the active call at the EI, the AS-SIP EI shall send a preemption tone to both the remote party and the local party on the active call (the local party on the active call appearance).

SCM-003150 [**Required: AS-SIP Voice EI, AS-SIP Secure Voice EI**] When the local party on the active call appearance goes "on hook," the AS-SIP EI shall offer the incoming precedence call to that party by playing a precedence ringing tone and providing a precedence level display on the call appearance from which the active call has been cleared.

SCM-003160 [**Required: AS-SIP Voice EI, AS-SIP Secure Voice EI**] The AS-SIP EI shall then give the called user the option of answering the call, or letting it forward to an alternate party (if CFDA is assigned), or letting it divert to an attendant (if Precedence Call Diversion is assigned).

SCM-003170 [**Required: AS-SIP Voice EI, AS-SIP Secure Voice EI**] In both of the previous cases (held call preempted and active call preempted), the AS-SIP EI shall not preempt any of the other calls that are on hold (on any other the other call appearances), and shall allow the end user to retrieve any of those calls at any time.

2.9.8 PEIs, AEIs, TAs, and IADs Using the V.150.1 Protocol

SCM-003180 [**Required: PEI, AEI, Secure AEI, TA with V.150.1, IAD with V.150.1**] Whenever these types of IP EIs, TAs, or IADs use ITU-T Recommendation V.150.1, the following shall apply:

a. ITU-T Recommendation V.150.1 provides for three states: audio, voiceband data (VBD), and modem relay. After call setup, inband signaling shall be used to transition from one state to another. In addition, ITU-T Recommendation V.150.1 provides for the transition to FoIP using Fax Relay per ITU-T Recommendation T.38.

b. When the product uses ITU-T Recommendation V.150.1 inband signaling to transition between audio, Fax over IP (FoIP), modem relay, or VBD states or modes, the product shall continue to use the established session's protocol (e.g., decimal 17 for User Datagram Protocol [UDP]) and port numbers so that the transition is transparent to the SBC.

2.9.9 UC Products With Non-Assured Services Features

SCM-003190 [**Conditional: All UC APL Products identified in the UCR Session Control and Auxiliary Services Sections**] If the UC product has a component that provides Non-

Assured-Services Features (Non-ASFs), and these Non-ASFs do not affect any of the product's Assured-Services Features (ASFs), then all voice or video sessions within the UC product with precedence above ROUTINE that are offered to a Non-ASF component (for example, a Non-ASF End Instrument or Automatic Call Distributor) shall be diverted immediately to an attendant console station.

SCM-003200 [**Optional: SC**] The SC shall support Non-Assured-Service EIs.

SCM-003210 [**Conditional: SC**] If the SC supports Non-Assured-Service EIs, then it shall support Assured-Service EIs that are included in the SC SUT.

2.9.10 ROUTINE-Only EIs

~~ROUTINE-only EIs are EIs that meet the PEI requirements in UCR 2013 Section 2 except that they provide minimal support for precedence and preemption, as specified below in this section.~~

SC support for ROUTINE-only EIs is optional. Items marked Required below that include SC in the marking are required only when the SC supports ROUTINE-only EIs.

SCM-003220 [**Conditional: SC**] If an SC supports ROUTINE-only voice EIs, it shall also support voice EIs that fully support precedence and preemption.

NOTE: There is no analogous requirement for an SC that supports ROUTINE-only video EIs.

SCM-003230 [**Removed**~~**Optional: SC**~~] ~~An SC shall support ROUTINE-only video EIs without providing support for video EIs that fully support precedence and preemption.~~

SCM-003240 [**Required: SC, ROEI**] ROUTINE-only ~~(RO)~~ EIs ~~(ROEIs)~~ shall not be able to originate precedence (i.e., PRIORITY and above) calls.

SCM-003250 [**Required: SC**] Precedence calls to ROEIs that use proprietary signaling shall be diverted immediately to an attendant.

SCM-003255 [**Optional: SC**] Precedence calls to ROEIs that use AS-SIP signaling shall be diverted immediately to an attendant.

NOTE: For diverted precedence video calls, if the attendant console is not video capable, then the precedence call will complete as an audio-only call.

SCM-003260 [**Required: SC, ROEI**] Sessions involving ROEIs affect ASAC Session Counts in the same way as sessions involving EIs that fully support precedence and preemption.

SCM-003270 [**Required: SC, ROEI, non-RO EI**] MLPP/PBAS requirements shall apply to non-ROEIs in sessions involving both RO and non-ROEIs.

SCM-003280 [**Optional: SC, ROEI**] Preemption Tone shall be provided to ROEIs on preempted sessions involving both ROUTINE-only and non-ROEIs.

SCM-003290 [**Optional: ROEI**] An ROEI shall display the precedence level of the session on which it participates~~, but is not required to do so~~.

SCM-003300 [**Removed**~~**Optional: ROEI**~~] ~~An ROEI shall support AS-SIP signaling, but will be tested and certified as a PEI, with the precedence and preemption exceptions noted above in this section.~~

2.10 SESSION CONTROLLER

The Session Controller (SC) is a software-based call processing product that provides voice and video services to IP telephones and media processing devices within a service domain. An SC extends signaling and session (call) control services to allow sessions to be established with users outside a given service domain via an IP-based long-haul network or via gateways to non-IP networks.

The SC software and functions may be distributed physically among several high-availability server platforms with redundant call management modules and subscriber tables to provide robustness.

Different types of SCs can be deployed, depending upon the service environment. These types are Local, Enterprise, and Master and Subtended. Please see DoD UC Framework 2013, Section 2.8, Session Controller, for additional information about SC applications. Section 2 requirements marked with an "SC" product qualifier apply to all types of SCs, unless an exception is explicitly noted.

2.10.1 PBAS/ASAC

SCM-003310 [**Required: SC**] The SC shall meet all the requirements for Precedence-Based Assured Services (PBAS) and ASAC, as appropriate for VoIP and Video over IP services, as specified in Section 2.25.1, Multilevel Precedence and Preemption and Section 2.3, ASAC.

2.10.2 SC Signaling

SCM-003320 [**Required: SC**] The SC shall support AS-SIP over IP for signaling to ~~AS-SIP End Instruments (AEI) and~~ Softswitches (SS).

SCM-003325 [**Optional: SC**] The SC shall shpport AS-SIP over IP for signaling to AS-SIP End Instruments (AEI).

SCM-003330 [**Optional: SC**] The SC shall support proprietary VVoIP signaling to interface with Proprietary End Instruments (PEI).

2.10.3 Session Controller Location Service

SCM-003340 [**Required: SC**] The SC shall support a Session Controller Location Service (SCLS) functionality that provides information on call routing and called address translation (where a called address is contained within the called SIP URI in the form of the called number). The CCA uses the routing information stored in the SCLS to route the following:

a. Internal calls from one SC PEI or AEI to another PEI or AEI on the same SC.

b. Outgoing calls from an SC PEI or AEI to another SC, an SS, or a TDM network.

c. Incoming calls from another SC, an SS, or a TDM network to an SC PEI or AEI.

2.10.4 SC Management Function

SCM-003350 [**Required: SC**] The SC shall support the applicable Fault, Configuration, Accounting, Performance, and Security (FCAPS) management and audit log requirements specified in Section 2.19, Management of Network Appliances.

2.10.5 SC-to-VVoIP EMS Interface

SCM-003360 [**Required: SC**] The SC shall provide an interface to the DISA VVoIP EMS. The interface consists of a 10/100-Mbps Ethernet connection as specified in Section 2.7.4, DISA VVoIP EMS Interface.

2.10.6 SC Transport Interface Functions

SCM-003370 [**Required: SC**] The SC shall provide Transport Interface functions to interface with the ASLAN and its IP packet transport network. Examples of Transport Interface functions include the following:

a. Network Layer functions: IP, IP security (IPSec).

b. Transport Layer functions: IP Transport Protocols (TCP, UDP, TLS).

c. LAN Protocols.

The CCA interacts with Transport Interface functions by using them to communicate with PEIs or AEIs and the SBC (and through the SBC to other SCs and the SS) over the ASLAN. The following Local Assured Services Domain elements are all IP end-points on the ASLAN:

- Each PEI or AEI served by the SC.
- Each MG served by the SC (even though the MG may be physically connected to the CCA/MGC over an internal proprietary interface, instead of being connected logically to the CCA/MGC over the ASLAN).
- The CCA/IWF/MGC itself.

- The SBC (for SC, PEI, AEI, and MG communication with other SCs, SSs, PEIs, AEIs, and MGs over the DISN WAN).

2.10.7 Custom Line-Side Features Interference

SCM-003380 [**Optional: SC**] Vendors shall implement unique custom features applicable to the line side of the SC.

SCM-003390 [**Conditional: SC**] If custom line-side features are implemented, then they shall not interfere with the Assured Services requirements.

2.10.8 Loop Avoidance for SCs

SCM-003400 [**Required: SC**] During the call establishment process, the product shall be capable of preventing or detecting and stopping hairpin routing loops over American National Standards Institute (ANSI) T1.619a and commercial PRI trunk groups (i.e., T1 PRI and E1 PRI) between a legacy switch (e.g., TDM EO) and an SC (see Figure 2.10-1, Example of a Hairpin Routing Loop). The Loop Avoidance mechanism shall not block call requests that are legitimately redirected or forwarded between the two interconnected products. In the event that a routing loop is detected, the SC shall clear the call in the backwards direction, either sending a 404 (Not Found) response to a SIP originator, or an ISDN DISCONNECT message (from the MG) to a TDM originator. The SC shall provide a VCA to the caller in each case.

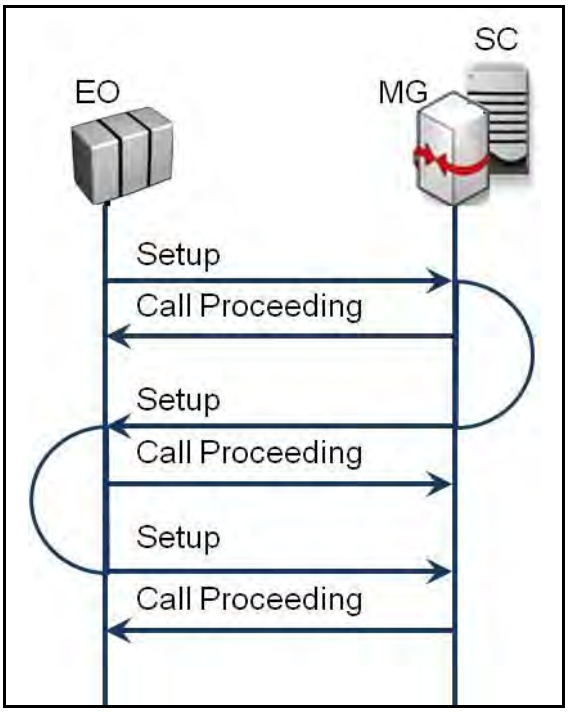


Figure 2.10-1. Example of a Hairpin Routing Loop

2.10.9 Local Session Controller Application

The requirements in this section are unique to the distributed application for the Session Controller, the Local Session Controller (LSC). An LSC provides management for the EIs within a single B/P/C/S or enclave and is deployed at the same location as the EIs it serves.

2.10.9.1 Service Requirements Under Total Loss of WAN Transport Connectivity

SCM-003410 In the event that total loss of connectivity to the DISN WAN occurs, the LSC shall provide the following functions:

SCM-003410.a [**Required: LSC**] Completion of local calls (i.e., calls between EIs the LSC serves).

SCM-003410.b [**Required: LSC**] Routing of calls to and from the PSTN, using a local MG (PRI or CAS as required by the local interface), that originate or terminate on EIs the LSC serves.

SCM-003410.c [**Optional: LSC**] User look-up of local directory information.

2.11 AS-SIP GATEWAYS

2.11.1 AS-SIP TDM Gateway

NOTE: All of the requirements in this section are AS-SIP TDM Gateway requirements and do not include a product qualifier.

Table 2.11-1, Summary of AS-SIP TDM Gateway Functions, provides a summary of AS-SIP TDM Gateway functions.

Table 2.11-1. Summary of AS-SIP TDM Gateway Functions

FUNCTION	DESCRIPTION
Session Control and Signaling	Signaling interworking ANSI T1.619a PRI non-ANSI T1.619a PRI [**Optional**] AS-SIP Call stateful, maintains local active session state knowledge (including precedence level)
Network Management	Provides traffic call information to and responds to traffic flow control commands from, an EMS
MGC	Required
MG	Interworking of B-channel PCM with SRTP/UDP/IP packets Generation and receipt/processing of SRTCP/UDP/IP packets Delivery of Q.931 messages Assignment of appropriate value to DSCP field when generating SRTP/UDP/IP packets

FUNCTION	DESCRIPTION
LEGEND	
AS-SIP: Unified Capabilities Session Initiation Protocol	EMS: Element Management System
DSCP: Differentiated Services Code Point	PCM: Pulse Code Modulation
IP: Internet Protocol	PRI: Primary Rate Interface
ISDN: Integrated Services Digital Network	SRTCP: Secure Real-Time Transport Control Protocol
MG: Media Gateway	SRTP: Secure Real-Time Transport Protocol
MGC: Media Gateway Controller	UDP: User Datagram Protocol
MLLP: Multilevel Precedence and Preemption	

SCM-003420 [**Required**] The AS-SIP TDM Gateway shall support the ANSI T1.619a PRI TDM interface.

SCM-003430 [**Optional**] The AS-SIP TDM Gateway shall support non-ANSI T1.619a PRI TDM interfaces.

2.11.1.1 AS-SIP TDM Gateway Signaling

The AS-SIP TDM Gateway provides signal interworking between the connected TDM switch and the designated SS. Table 2.11-2, AS-SIP TDM Gateway Support for VoIP and Video Signaling Interfaces, provides the list of the AS-SIP TDM Gateway signaling requirements.

Table 2.11-2. AS-SIP TDM Gateway Support for VoIP and Video Signaling Interfaces

FUNCTIONAL COMPONENT	VOIP AND VIDEO SIGNALING INTERFACES	VOIP AND VIDEO SIGNALING PROTOCOLS
CCA	CCA (AS-SIP TDM Gateway) – to – CCA (SS)	AS-SIP over IP
CCA/MGC and MG	CCA (MGC) – to – MG	Internal interface to integrated MG functional component (used with ANSI T1.619a PRI trunks and optional non-ANSI T1.619a PRI trunks)

LEGEND		
AS-SIP: Assured Services Session Initation Protocol	MLPP: Multilevel Precedence and Preemption	PRI: Primary Rate Interface
CCA: Call Connection Agent	MG: Media Gateway	SS: Softswitch
IP: Internet Protocol	MGC: Media Gateway Controller	TDM: Time Division Multiplexing

SCM-003440 [**Required**] The AS-SIP TDM Gateway shall provide signal interworking between the connected TDM switch and the designated SS. The signaling protocol for interfacing with the SS shall be AS-SIP over IP.

SCM-003450 [**Required**] When the AS-SIP TDM Gateway receives a SETUP message from aANSI T1.619a PRI, the AS-SIP TDM Gateway shall interwork the SETUP message to an AS-

SIP INVITE and forward the AS-SIP INVITE to the SBC. The MLPP IE network identity digits, precedence level bits, and service domain shall be interworked into the Resource-Priority header's network domain subfield, r-priority field, and precedence domain subfield, respectively, consistent with AS-SIP 2013.

SCM-003460 [**Required**] The AS-SIP TDM Gateway shall add a CCA-ID parameter to the Contact header.

SCM-003470 [**Required**] The AS-SIP TDM Gateway shall add a route set comprising two Route headers where the first Route header is the SIP URI for the SBC at the enclave, and the second Route header is the SIP URI for the SBC serving the SS.

SCM-003480 [**Required**] When the AS-SIP TDM Gateway receives an AS-SIP INVITE from the SS via the SBC intended for a ANSI T1.619a PRI, the AS-SIP TDM Gateway shall interwork the INVITE to a SETUP message and forward the SETUP message on the D-channel.

SCM-003490 [**Required**] The AS-SIP TDM Gateway shall interwork INVITEs received from the SBC to the TDM switch, even if all DS0s are currently in use.

2.11.1.2 SIP URI and Mapping of Telephone Number

SCM-003500 [**Required**] When the AS-SIP TDM Gateway receives a call request over an ANSI T1.619a PRI then the AS-SIP TDM Gateway shall map the telephony numbers received from the Q.931 SETUP message to SIP URIs IAW AS-SIP 2013, Section 12.3, SIP URI and Mapping of Telephony Number into SIP URI, and Section 4.6, SIP URI and Mapping of Telephone Number into SIP URI.

2.11.1.3 AS-SIP TDM Gateway Media

SCM-003510 [**Required**] The AS-SIP TDM Gateway MG shall support the ITU-T Recommendation G.711 (μ-law and A-law) audio codec and shall perform A-law/μ-law conversion when needed.

SCM-003520 [**Required**] The AS-SIP TDM Gateway MG shall support RFC 4040 and the signaling for establishing the 64kbps unrestricted bearer per AS-SIP 2013, Section 4.7, 64 Kbps Transparent Calls (Clear Channel).

SCM-003530 [**Required**] The AS-SIP TDM Gateway MG shall support T.38 Fax Relay (see Section 2.16.8.9, MG Support for Group 3 Fax Calls.

SCM-003540 [**Required**] The AS-SIP TDM Gateway MG shall support the SCIP-216 subset of V.150.1 Modem Relay (see Section 2.20.1, SCIP/V.150.1 Gateway) and the AS-SIP signaling requirements in support of modem relay (See AS-SIP 2013, Section 11.1, AS-SIP Signaling Requirements in Support of Modem Relay-Capable Gateways).

2.11.1.4 Information Assurance

SCM-003550 [**Required**] The AS-SIP TDM Gateway shall satisfy the Information Assurance requirements in Section 4, Information Assurance for an MG.

2.11.1.5 AS-SIP TDM Gateway Management Function

SCM-003560 [**Required**] The CCA shall interact with the AS-SIP TDM Gateway Management function by doing the following:

a. Making changes to its configuration in response to commands from the Management function that requests these changes.

b. Returning information to the Management function on its FCAPS, in response to commands from the Management function that requests this information.

c. Sending information to the Management function on a periodic basis (e.g., on a set schedule), keeping the Management function up-to-date on CCA activity.

2.11.1.6 AS-SIP TDM Gateway-to-EMS Interface

SCM-003570 [**Required**] The AS-SIP TDM Gateway shall provide an interface to the DISA VVoIP EMS. The interface shall consist of a 10/100-Mbps Ethernet connection, as specified in Section 2.7.4, DISA VVoIP EMS Interface.

2.11.2 AS-SIP IP Gateway

NOTE: Requirements in this section apply to either the AS-SIP IP Gateway or the Softswitch (SS) product. Requirements in this section that do not include an SS product qualifier in the requirement marking are AS-SIP IP Gateway requirements.

The AS-SIP IP Gateway is a VVoIP interworking appliance, and its purpose is to enable the interconnection and interoperation of proprietary IP-based UC signaling platforms and their associated IP EIs with the DISN UC system to support E2E voice and video sessions.

NOTE: The AS-SIP IP Gateway is not an Assured Services appliance.

The AS-SIP IP Gateway provides interworking functions for the signaling and bearer planes (see Table 2.11-3, Summary of AS-SIP IP Gateway Functions).

Table 2.11-3. Summary of AS-SIP IP Gateway Functions

FUNCTION	DESCRIPTION
SCS	Verifies call request is consistent with SAC: Signaling interworking (proprietary to AS-SIP; AS-SIP to proprietary)
SAC	Maintains call thresholds. Maintains active session state knowledge (local access bandwidth used and available, direction,

FUNCTION	DESCRIPTION
	session type: voice, video).
Media IWF	Converts proprietary media packets to UCR-compliant IP/UDP/SRTP packets. Converts UCR compliant IP/UDP/SRTP packets to proprietary media packets.
NM	Provides traffic call information to, and responds to traffic flow control commands from, an EMS.

LEGEND

AS-SIP: Assured Services Session Initiation Protocol	SAC: Session Admission Control
EMS: Element Management System	SCS: Session Control and Signaling
IP: Internet Protocol	SRTP: Secure Real-time Transport Protocol
IWF: Interworking Function	UCR: Unified Capabilities Requirements
NM: Network Management	UDP: User Datagram Protocol

SCM-003580 [**Required**] The AS-SIP IP Gateway shall implement call count thresholds for voice sessions and for video sessions in order to perform Session Admission Control (SAC). See Section 2.11.3.4, Session Admission Control, for more details.

2.11.2.1 AS-SIP IP Gateway Call Request Processing

SCM-003590 [**Required**] When the AS-SIP IP Gateway receives a call request from the proprietary UC signaling platform then the AS-SIP IP Gateway shall:

a. Check the appropriate (voice or video) call count (and outbound call count in the case of directionalization) to determine whether there are available bandwidth resources to support the call request.

b. If the new call request would not exceed the appropriate (voice or video) call count threshold (and outbound call count threshold) then the AS-SIP IP Gateway interworks the call request by doing the following:

   (1) Incrementing the call count (and outbound call count in the case of directionalization).

   (2) Generating a “routine” level AS-SIP INVITE that advertises equivalent capabilities to those specified in the received call request.

   (3) Adding a CCA-ID parameter to the Contact header.

   (4) Adding a route set comprising two Route headers where the first Route header is the SIP URI for the SBC at the enclave, and the second Route header is the SIP URI for the SBC serving the SS.

   (5) Forwarding the INVITE message to the SBC at the enclave.

SCM-003600 [**Required**] If the appropriate (voice or video) call count (or outbound call count) is at threshold or the call request would cause the AS-SIP IP Gateway to exceed the call count threshold (or outbound call count threshold) then the AS-SIP IP Gateway shall reject the call.

NOTE: If the proprietary signaling interface is SIP, then the response message shall be 488 (Not Acceptable Here) and may include an optional Warning header field with warning code 370 (Insufficient Bandwidth).

2.11.2.2 SS Policing Requirements When Serving an AS-SIP IP Gateway

SCM-003610 [**Required: SS**] The SS shall apply the standard ASAC policing rules for outbound routine voice and video requests when it receives an AS-SIP INVITE from a served AS-SIP IP Gateway.

NOTE: The AS-SIP IP Gateway sends only routine AS-SIP INVITEs to the SS.

See AS-SIP 2013, Requirements 7.2.8, 7.2.10, 7.2.11, and 7.2.12 for policing routine outbound telephony requests.

See AS-SIP 2013, Requirements 7.3.9, 7.3.11, 7.3.12, and 7.3.13 for policing routine outbound video requests.

SCM-003620 [**Required: SS**] The SS shall apply the standard ASAC policing rules for inbound routine voice and video requests when it receives an initial "routine" AS-SIP INVITE intended for forwarding to a served AS-SIP IP Gateway.

See AS-SIP 2013, Requirements 7.2.13, 7.2.13.1, 7.2.13.3, 7.2.13.4, 7.2.13.5, 7.2.14, 7.2.14.1, 7.2.14.2, 7.2.14.5, 7.2.14.6, 7.2.14.7, 7.2.14.8, 7.2.14.9, 7.2.14.10, 7.2.15, 7.2.15.1, 7.2.15.3, 7.2.15.4, and 7.2.15.5 for policing inbound routine telephony requests.

See AS-SIP 2013, Requirements 7.3.14, 7.3.14.1, 7.3.14.3, 7.3.14.4, 7.3.14.5, 7.3.14.6, 7.3.15, 7.3.15.1, 7.3.15.3, 7.3.15.4, 7.3.15.5, and 7.3.15.6 for policing inbound routine video requests.

SCM-003630 [**Required: SS**] The SS shall implement one of the following two policing rules when it receives an initial precedence AS-SIP INVITE intended for forwarding to a served AS-SIP IP Gateway:

SCM-003630.a [**Preferred**] Forward the AS-SIP INVITE to the AS-SIP IP Gateway and if the AS-SIP IP Gateway responds with either a 1xx response code greater than 100 or a 2xx response and the call request would cause the appropriate (voice or video) call count threshold (or inbound call count threshold) to be exceeded then the SS:

(1) Sends a 488 (Not Acceptable Here) response code to the remote initiating party of the AS-SIP INVITE that may include a Warning header field with warning code 370 (Insufficient Bandwidth).

(2) Sends a CANCEL request (in the case of a 1xx response code) or a BYE request (in the case of a 2xx response code) to the local AS-SIP IP Gateway.

NOTE: This approach has the SS applying the standard ASAC policing rules for a ROUTINE request to a precedence request.

SCM-003630.b [**Alternative**] (Standard ASAC Policing Rules for precedence call request) Forward the AS-SIP INVITE to the AS-SIP IP Gateway and if the AS-SIP IP Gateway responds with either a 1xx response code greater than 100 or a 2xx response and the call request would cause the appropriate (voice or video) call count threshold (or inbound call count threshold) to be exceeded, then the SS applies the standard ASAC policing rules for a precedence call request. That is, the SS preempts a ROUTINE or lesser precedence call by sending a BYE request with a reason header for preemption to the AS-SIP IP Gateway. The AS-SIP IP Gateway shall ignore the reason header for preemption, interwork the BYE to the proprietary UC signaling platform, and respond with a 200 (OK) response . The routine or lesser precedence call will be terminated and the SS will forward the 1xx response greater than 100 or the 2xx response to the precedence inbound call request over the UC WAN.

2.11.2.3 AS-SIP IP Gateway SCS

Table 2.11-4, AS-SIP IP Gateway support for VoIP and Video Signaling Interfaces, provides a complete list of the AS-SIP IP Gateway signaling requirements. NOTE: the term proprietary signaling encompasses any vendor-proprietary signaling, SIP, H.323, or other signaling protocol transported over IP that is not AS-SIP.

Table 2.11-4. AS-SIP IP Gateway Support for VoIP and Video Signaling Interfaces

FUNCTIONAL COMPONENT	VOIP AND VIDEO SIGNALING INTERFACES	VOIP AND VIDEO SIGNALING PROTOCOLS
CCA	CCA (AS-SIP IP Gateway) – to – CCA (SS)	AS-SIP over IP
CCA	CCA (AS-SIP IP Gateway) – to – proprietary UC signaling platform	Proprietary signaling over IP
LEGEND		
AS-SIP: Assured Services Session Initiation Protocol	IP: Internet Protocol	
CCA: Call Connection Agent	SS: Softswitch	
	VoIP: Voice over IP	

2.11.2.3.1 CCA Function

The CCA is part of the SCS functions and includes the IWF (signaling) function.

SCM-003640 [**Required**] The CCA IWF shall support the AS-SIP consistent with the detailed AS-SIP requirements in AS-SIP 2013.

SCM-003650 [**Required**] The CCA IWF shall secure the AS-SIP protocol using TLS, as described in Section 4, Information Assurance.

SCM-003660 [**Required**] The CCA IWF component of the AS-SIP IP Gateway shall ensure that when supported supplementary services enumerated in the UCR (e.g., Call Hold, Call Waiting,

Call Forwarding, Call Transfer) are performed by a served proprietary UC signaling platform that the AS-SIP IP Gateway presents UCR-compliant call flows to the signaling appliances in the UC network per AS-SIP 2013, Section 9.

2.11.2.3.2 AS Precedence Capability Requirements and Resource Priority Header

SCM-003670 [**Required**] Whenever the AS-SIP IP Gateway receives a proprietary signaling message from the proprietary UC signaling platform that translates it into an INVITE, UPDATE, or REFER request, then the AS-SIP IP Gateway shall generate a Resource-Priority header having a ROUTINE priority level IAW AS-SIP 2013, Section 6.1, Precedence Level Communicated over SIP Signaling.

SCM-003680 [**Required**] Whenever the AS-SIP IP Gateway receives an INVITE, UPDATE, or REFER request from the SS via the SBC, then the AS-SIP IP Gateway shall process the Resource-Priority header to distinguish a ROUTINE call from a precedence call.

SCM-003690 [**Required**] When an AS-SIP IP Gateway receives an initial ROUTINE AS-SIP INVITE (i.e., not a re-INVITE) from the SS (via the SBC), then the AS-SIP IP Gateway shall:

a. Check the appropriate (voice or video) call count (and inbound call count in the case of directionalization) to determine whether there are available bandwidth resources to support the call request.

b. If the new call request would not exceed the appropriate (voice or video) call count threshold (and inbound call count threshold) then the AS-SIP IP Gateway increments the appropriate (voice or video) call count (and inbound call count) and interworks the INVITE to the signaling protocol of the proprietary UC signaling platform.

c. If the appropriate (voice or video) call count (or inbound call count) is at threshold or the call request would cause the AS-SIP IP Gateway to exceed the appropriate (voice or video) call count threshold (or inbound call count threshold) then the AS-SIP IP Gateway shall reject the call. NOTE: The response message is 488 (Not Acceptable Here) and may include a Warning header field with warning code 370 (Insufficient Bandwidth).

SCM-003700 [**Required**] The AS-SIP IP Gateway shall support the following 2 methods for processing initial precedence AS-SIP INVITEs received from the SS via the SBC and the choice of method shall be software configurable:

a. Upon receipt of the initial precedence AS-SIP INVITE request the AS-SIP IP Gateway diverts the precedence INVITE to the attendant, or

b. Upon receipt of the initial precedence AS-SIP INVITE request the AS-SIP IP Gateway determines whether the appropriate (voice or video) call count (or inbound call count in the case of directionalization) is at threshold or whether the call request would cause the AS-SIP IP Gateway to exceed the appropriate (voice or video) call count threshold or inbound call count threshold:

(1) If the precedence AS-SIP INVITE would cause the appropriate (voice or video) call count threshold (or inbound call count threshold) to be exceeded, then the precedence AS-SIP INVITE is forwarded to the attendant.

NOTE: The AS-SIP IP Gateway shall NOT conduct preemption on behalf of an inbound precedence AS-SIP INVITE.

(2) If the precedence AS-SIP INVITE would NOT cause the appropriate call count threshold (or inbound call count threshold) to be exceeded, then the AS-SIP IP Gateway treats the inbound precedence AS-SIP INVITE request as if it were a routine inbound call request and increments the appropriate (voice or video) call count (and inbound call count) and interworks the INVITE to the signaling protocol of the proprietary UC signaling platform.

2.11.2.3.3 SIP URI and Mapping of Telephone Number

SCM-003710 [**Required**] When the AS-SIP IP Gateway receives a call request from the proprietary UC signaling platform, then the AS-SIP IP Gateway shall map the telephony numbers received from the initial proprietary signaling message to SIP URIs IAW AS-SIP 2013, Sections 12.3, SIP URI and Mapping of Telephony Number into SIP URI, and 4.6, SIP URI and Mapping of Telephone Number into SIP URI.

2.11.2.3.4 Session Admission Control

SCM-003720 [**Required**] The AS-SIP IP Gateway shall conduct SAC as detailed in this section in lieu of the ASAC required for SCs.

SCM-003730 [**Optional**] The AS-SIP IP Gateway shall support directionalization.

NOTE: Whenever the proprietary UC signaling platform supports directionalization, then directionalization will be performed in the proprietary UC signaling platform and not in the AS-SIP IP Gateway.

SCM-003740 [**Conditional**] If the proprietary UC signaling platform does not support code blocking then the AS-SIP IP Gateway shall support code blocking.

SCM-003750 [**Required**] The AS-SIP IP Gateway shall support configuration of total voice call thresholds and total video call thresholds.

SCM-003760 [**Optional**] The AS-SIP IP Gateway shall support configuration of outbound voice call thresholds, inbound voice call thresholds, outbound video call thresholds, and inbound video call thresholds.

SCM-003770 [**Required**] Session Admission Control (SAC) refers to the enforcement of voice and video session thresholds whereby the AS-SIP IP Gateway shall:

a. Reject call requests received from the proprietary UC signaling platform that would exceed the appropriate (voice or video) call count threshold (or outbound call count threshold)

b. Reject initial routine INVITEs (i.e., not re-INVITEs) received from the SS that would exceed the appropriate (voice or video) call count threshold (or inbound call count threshold).

c. Per the requirement for precedence calls in Section 2.11.2.3.2, either divert all precedence INVITEs to the attendant, or divert the precedence INVITE to the attendant if the INVITE would cause the appropriate (voice or video) call count threshold (or inbound call count threshold) to be exceeded.

2.11.2.4 AS-SIP IP Gateway Media Interworking

SCM-003780 [**Required**] The AS-SIP IP Gateway shall support the audio Codecs in Section 2.9.1.3, Audio Codecs, Voice Instruments.

SCM-003790 [**Required**] The AS-SIP IP Gateway shall comply with Section 2.9.1.5, Voice over IP Sampling Standard, for the sampling rates.

SCM-003800 [**Required**] The AS-SIP IP Gateway shall support the audio and video Codecs as specified in Section 2.9.3.3, Video Codecs (Including Associated Audio Codecs).

SCM-003810 [**Required**] The voice media packets generated by the IP EIs served by the proprietary UC signaling platform that are intended for a destination outside the enclave shall be interworked by the AS-SIP IP Gateway into UCR-compliant voice packets that shall be sent to the SBC.

SCM-003820 [**Required: SBC**] The enclave SBC shall send the UCR-compliant voice media packets received from the UC WAN and intended for the IP EIs served by the proprietary UC signaling platform to the AS-SIP IP Gateway.

SCM-003830 [**Required**] The AS-SIP IP Gateway shall interwork the UCR-compliant voice media packets received from the SBC into the proprietary voice media packets used by the IP EIs, and then the proprietary voice media packets shall be forwarded to the IP EIs.

SCM-003840 [**Required**] The video media packets generated by the IP EIs served by the proprietary UC signaling platform that are intended for a destination outside the enclave shall be interworked by the AS-SIP IP Gateway into UCR-compliant video packets that shall be sent to the SBC.

SCM-003850 [**Required: SBC**] The enclave SBC shall send the UCR-compliant video media packets received from the UC WAN and intended for the IP EIs served by the proprietary UC signaling platform to the AS-SIP IP Gateway.

SCM-003860 [**Required**] The AS-SIP IP Gateway shall interwork the UCR-compliant video media packets received from the SBC into the proprietary video media packets employed by the IP EIs and then the proprietary video media packets shall be forwarded to the IP EIs.

2.11.2.5 Information Assurance

SCM-003870 [**Required**] The AS-SIP IP Gateway shall satisfy the Information Assurance requirements in Section 4, Information Assurance, for an MG.

2.11.2.6 AS-SIP IP Gateway Management Function

SCM-003880 [**Required**] The CCA shall interact with the AS-SIP IP Gateway Management function by doing the following:

a. Making changes to its configuration in response to commands from the Management function that requests these changes.

b. Returning information to the Management function on its FCAPS, in response to commands from the Management function that requests this information.

c. Sending information to the Management function on a periodic basis (e.g., on a set schedule), keeping the Management function up-to-date on CCA activity.

2.11.2.7 AS-SIP ~~TDM~~ IP Gateway-to-EMS Interface

SCM-003890 [**Required**] The AS-SIP IP Gateway shall provide an interface to the DISA VVoIP EMS. The interface shall consist of a 10/100-Mbps Ethernet connection, as specified in Section 2.7.4, DISA VVoIP EMS Interface.

2.11.3 AS-SIP – H.323 Gateway

NOTE: Requirements in this section apply to either the AS-SIP – H.323 Gateway or the Softswitch (SS) product. Requirements in this section that do not include an SS product qualifier are AS-SIP – H.323 Gateway requirements.

The AS-SIP – H.323 Gateway is a VVoIP interworking appliance, and its purpose is to enable the interconnection and interoperation of H.323 IP-based UC signaling platforms and their associated IP EIs with the DISN UC system to support E2E voice and video sessions.

The Government has adopted RFC 4123 – Session Initiation Protocol (SIP) – H.323 Interworking Requirements as the document which describes the requirements for the AS-SIP – H.323 Gateway. Internet draft-agrawal-sip-h323-interworking-01.txt is cited as guidance to be used in implementing the AS-SIP – H.323 Gateway. The following contents of this section are additional Government requirements.

NOTE: The AS-SIP – H.323 Gateway is not an Assured Services appliance.

The AS-SIP – H.323 Gateway SUT is a standalone SUT for testing purposes.

The AS-SIP – H.323 Gateway provides interworking functions for the signaling and bearer planes (see Table 2.11-5, Summary of AS-SIP – H.323 Gateway Functions).

Table 2.11-5. Summary of AS-SIP – H.323 Gateway Functions

FUNCTION	DESCRIPTION
SCS	Verifies call request is consistent with SAC: Signaling interworking (H.323 to AS-SIP; AS-SIP to H.323)
SAC	Maintains call thresholds. Maintains active session state knowledge (local access bandwidth used and available, direction, session type: voice, video)
Media IWF	Converts H.323 media packets to UCR-compliant IP/UDP/SRTP packets Converts UCR compliant IP/UDP/SRTP packets to H.323 media packets
NM	Provides traffic call information to, and responds to traffic flow control commands from, an EMS

LEGEND

AS-SIP: Assured Services Session Initiation Protocol	SAC: Session Admission Control
EMS: Element Management System	SCS: Session Control and Signaling
IP: Internet Protocol	SRTP: Secure Real-time Transport Protocol
IWF: Interworking Function	UCR: Unified Capabilities Requirements
NM: Network Management	UDP: User Datagram Protocol

SCM-003900 [**Required**] From a signaling perspective, the AS-SIP – H.323 Gateway shall offer an AS-SIP-compliant signaling interface that provides end-to-end signaling interoperability between the AS-SIP – H.323 Gateway SUT and the AS-SIP signaling appliances of the DISN UC WAN system.

SCM-003910 [**Required**] From a media perspective, the AS-SIP – H.323 Gateway shall offer a UCR-compliant bearer interface that provides E2E interoperability for voice and video media packets between the AS-SIP – H.323 Gateway SUT and SBCs, IP EIs of SC SUTs, MGs, and AS-SIP EIs. The AS-SIP – H.323 Gateway shall interwork the voice and video media packets generated by the IP EIs served by the IP-based UC signaling platform and intended for a destination outside the H.323 system enclave to UCR-compliant SRTP/UDP packets having the appropriate DSCP. Similarly, UCR-compliant SRTP/UDP voice and video media packets received from the UC WAN and intended for the IP EIs served by the H.323 UC signaling platform shall be interworked by the AS-SIP – H.323 Gateway into the H.323 media packets supported by the IP EIs.

SCM-003920 [**Required**] The AS-SIP – H.323 Gateway shall implement call count thresholds for voice sessions and for video sessions in order to perform Session Admission Control (SAC). See Section 2.11.3.6, Session Admission Control, for more details.

2.11.3.1 AS-SIP – H.323 Gateway Call Request Processing

SCM-003930 [**Required**] When the AS-SIP – H.323 Gateway receives a call request from the H.323 UC signaling platform then the AS-SIP – H.323 Gateway shall:

a. Check the appropriate (voice or video) call count (and outbound call count in the case of directionalization) to determine whether there are available bandwidth resources to support the call request.

b. If the new call request would not exceed the appropriate (voice or video) call count threshold (and outbound call count threshold) then the AS-SIP – H.323 Gateway interworks the call request by doing the following:

   (1) Incrementing the call count (and outbound call count in the case of directionalization).

   (2) Generating a "routine" level AS-SIP INVITE that advertises equivalent capabilities to those specified in the received call request.

   (3) Adding a CCA-ID parameter to the Contact header.

   (4) Adding a route set comprising two Route headers where the first Route header is the SIP URI for the SBC at the enclave, and the second Route header is the SIP URI for the SBC serving the SS.

   (5) Forwarding the INVITE message to the SBC at the enclave

c. If the appropriate (voice or video) call count (or outbound call count) is at threshold or the call request would cause the AS-SIP – H.323 Gateway to exceed the call count threshold (or outbound call count threshold) then the AS-SIP – H.323 Gateway shall reject the call.

2.11.3.2 SS Policing Requirements When Serving an AS-SIP – H.323 Gateway

SCM-003940 [**Required: SS**] The AS-SIP – H.323 Gateway sends only routine AS-SIP INVITEs to the SS, and the SS shall apply the standard ASAC policing rules for outbound routine voice and video requests.

See AS-SIP 2013, Requirements 7.2.8, 7.2.10 through 7.2.12 for policing routine outbound telephony requests.

See AS-SIP 2013, Requirements 7.3.9, 7.3.11 through 7.3.13 for policing routine outbound video requests.

SCM-003950 [**Required: SS**] When an SS receives an initial "routine" AS-SIP INVITE request intended for forwarding to a served AS-SIP – H.323 Gateway, the SS shall apply the standard ASAC policing rules for inbound routine voice and video requests.

See AS-SIP 2013, Requirements 7.2.13, 7.2.13.1, 7.2.13.3 through 7.2.13.5, 7.2.14, 7.2.14.1, 7.2.14.2, 7.2.14.5 through 7.2.14.10, 7.2.15, 7.2.15.1, 7.2.15.3 through 7.2.15.5 for policing inbound routine telephony requests.

See AS-SIP 2013, Requirements 7.3.14, 7.3.14.1, 7.3.14.3 through 7.3.14.6, 7.3.15, 7.3.15.1, 7.3.15.3 through 7.3.15.6 for policing inbound routine video requests.

SCM-003960 [**Required: SS**] [**5.3.2.7.5.1.7**] When an SS receives an initial precedence AS-SIP INVITE request intended for forwarding to a served AS-SIP – H.323 Gateway, the SS shall implement one of the following two policing rules:

> **SCM-003960.a** [**Preferred**] Forward the AS-SIP INVITE to the AS-SIP – H.323 Gateway and if the AS-SIP – H.323 Gateway responds with either a 1xx response code greater than 100 or a 2xx response and the call request would cause the appropriate (voice or video) call count threshold (or inbound call count threshold) to be exceeded, then the SS:
>
> (1) Sends a 488 (Not Acceptable Here) response code to the remote initiating party of the AS-SIP INVITE that may include a Warning header field with warning code 370 (Insufficient Bandwidth).
>
> (2) Sends a CANCEL request (in the case of a 1xx response code) or a BYE request (in the case of a 2xx response code) to the local AS-SIP – H.323 Gateway.
>
> NOTE: This approach has the SS applying the standard ASAC policing rules for a ROUTINE request to a precedence request.
>
> **SCM-003960.b** [**Alternative**] (Standard ASAC Policing Rules for precedence call request) Forward the AS-SIP INVITE request to the AS-SIP – H.323 Gateway and if the AS-SIP – H.323 Gateway responds with either a 1xx response code greater than 100 or a 2xx response and the call request would cause the appropriate (voice or video) call count threshold (or inbound call count threshold) to be exceeded, then the SS applies the standard ASAC policing rules for a precedence call request. That is, the SS preempts a ROUTINE or lesser precedence call by sending a BYE request with a Reason header for preemption to the AS-SIP – H.323 Gateway. The AS-SIP – H.323 Gateway shall ignore the Reason header for preemption, interwork the BYE request to the H.323 UC signaling platform, and respond with a 200 (OK) response. The ROUTINE or lesser precedence call will be terminated and the SS will forward the 1xx response greater than 100 or the 2xx response to the precedence inbound call request over the UC WAN.

2.11.3.3 AS-SIP – H.323 Gateway SCS

Table 2.11-6, AS-SIP – H.323 Gateway support for VoIP and Video Signaling Interfaces, provides a complete list of the AS-SIP – H.323 Gateway signaling requirements.

Table 2.11-6. AS-SIP – H.323 Gateway Support for VoIP and Video Signaling Interfaces

FUNCTIONAL COMPONENT	VOIP AND VIDEO SIGNALING INTERFACES	VOIP AND VIDEO SIGNALING PROTOCOLS
CCA	CCA (AS-SIP – H.323 Gateway) – to – CCA (SS)	AS-SIP over IP
CCA	CCA (AS-SIP – H.323 Gateway) – to – H.323 UC signaling platform	Proprietary signaling over IP
LEGEND		
AS-SIP: Assured Services Session Initiation Protocol CCA: Call Connection Agent IP: Internet Protocol		SS: Softswitch UC: Unified Capabilities VoIP: Voice over IP

2.11.3.3.1 CCA Function

The CCA is part of the SCS functions and includes the IWF (signaling) function.

SCM-003970 [**Required**] The CCA IWF shall support the AS-SIP consistent with the detailed AS-SIP requirements in AS-SIP 2013.

SCM-003980 [**Required**] The CCA IWF shall secure the AS-SIP protocol using TLS, as described in Section 4, Information Assurance.

SCM-003990 [**Required**] The CCA IWF component of the AS-SIP – H.323 Gateway shall ensure that when the supplementary services enumerated in the UCR (i.e., Call Hold, Call Waiting, Precedence Call Waiting, Call Forwarding, Call Transfer) are performed by a served H.323 UC signaling platform that the AS-SIP – H.323 Gateway presents UCR-compliant call flows to the signaling appliances in the UC network per AS-SIP 2013, Section 9.

2.11.3.4 AS Precedence Capability Requirements and Resource Priority Header

The AS-SIP – H.323 Gateway does NOT conduct preemption.

SCM-004000 [**Required**] Whenever the AS-SIP – H.323 Gateway receives a H.323 signaling message from the H.323 UC signaling platform that translates it into an INVITE, UPDATE, or REFER request, then the AS-SIP – H.323 Gateway shall generate a Resource-Priority header having a ROUTINE priority level IAW AS-SIP 2013, Section 6.1, Precedence Level Communicated Over SIP Signaling.

SCM-004010 [**Required**] Whenever the AS-SIP – H.323 Gateway receives an INVITE, UPDATE, or REFER request from the SS via the SBC, then the AS-SIP – H.323 Gateway shall process the Resource-Priority header to distinguish a ROUTINE call from a precedence call.

SCM-004020 [**Required**] When an AS-SIP – H.323 Gateway receives an initial routine AS-SIP INVITE (i.e., not a re-INVITE) from the SS (via the SBC), then the AS-SIP – H.323 Gateway shall do the following:

a. Check the appropriate (voice or video) call count (and inbound call count in the case of directionalization) to determine whether there are available bandwidth resources to support the call request.

b. If the new call request would not exceed the appropriate (voice or video) call count threshold (and inbound call count threshold) then the AS-SIP – H.323 Gateway increments the appropriate (voice or video) call count (and inbound call count) and interworks the INVITE to H.323.

c. If the appropriate (voice or video) call count (or inbound call count) is at threshold or the call request would cause the AS-SIP – H.323 Gateway to exceed the appropriate (voice or video) call count threshold (or inbound call count threshold) then the AS-SIP – H.323 Gateway shall reject the call.

NOTE: The response message is 488 (Not Acceptable Here) and may include a Warning header field with warning code 370 (Insufficient Bandwidth).

SCM-004030 [**Required**] The AS-SIP – H.323 Gateway shall support the following two methods for processing initial precedence AS-SIP INVITEs received from the SS via the SBC and the choice of method shall be software configurable:

a. Upon receipt of the initial precedence AS-SIP INVITE request the AS-SIP – H.323 Gateway diverts the precedence INVITE to the attendant, or

b. Upon receipt of the initial precedence AS-SIP INVITE request, the AS-SIP – H.323 Gateway determines whether the appropriate (voice or video) call count (or inbound call count in the case of directionalization) is at threshold or whether the call request would cause the AS-SIP – H.323 Gateway to exceed the appropriate (voice or video) call count threshold or inbound call count threshold:

(1) If the precedence AS-SIP INVITE would cause the appropriate (voice or video) call count threshold (or inbound call count threshold) to be exceeded, then the precedence AS-SIP INVITE is forwarded to the attendant.

NOTE: The AS-SIP – H.323 Gateway shall NOT conduct preemption on behalf of an inbound precedence AS-SIP INVITE.

(2) If the precedence AS-SIP INVITE would NOT cause the appropriate call count threshold (or inbound call count threshold) to be exceeded, then the AS-SIP – H.323 Gateway treats the inbound precedence AS-SIP INVITE request as if it were a routine inbound call request and increments the appropriate (voice or video) call count (and inbound call count) and interworks the INVITE to platform..

2.11.3.5 SIP URI and Mapping of Telephone Number

SCM-004040 [**Required**] When the AS-SIP – H.323 Gateway receives a call request from the H.323 UC signaling platform, then the AS-SIP – H.323 Gateway shall map the telephony

numbers received from the initial H.323 signaling message to SIP URIs IAW AS-SIP 2013, Sections 12.3, SIP URI and Mapping of Telephony Number into SIP URI, and 4.6, SIP URI and Mapping of Telephone Number into SIP URI.

2.11.3.6 Session Admission Control

SCM-004050 [**Required**] The AS-SIP – H.323 Gateway shall conduct SAC as detailed in this section in lieu of the ASAC required of SCs.

SCM-004060 [**Optional**] The AS-SIP – H.323 Gateway shall support directionalization.

NOTE: Whenever the H.323 UC signaling platform supports Directionalization, then directionalization will be performed in the H.323 UC signaling platform and not in the AS-SIP – H.323 Gateway.

SCM-004070 [**Conditional**] If the H.323 UC signaling platform does not support code blocking then the AS-SIP – H.323 Gateway shall support code blocking.

SCM-004080 [**Required**] The AS-SIP – H.323 Gateway shall support configuration of total voice call thresholds and total video call thresholds.

SCM-004090 [**Optional**] The AS-SIP – H.323 Gateway shall support configuration of outbound voice call thresholds, inbound voice call thresholds, outbound video call thresholds, and inbound video call thresholds.

SCM-004100 [**Required**] Session Admission Control (SAC) refers to the enforcement of voice and video session thresholds whereby the AS-SIP – H.323 Gateway shall:

a. Reject call requests received from the H.323 UC signaling platform that would exceed the appropriate [voice or video) call count threshold (or outbound call count threshold).

b. Reject initial routine INVITEs (i.e., not re-INVITEs) received from the SS that would exceed the appropriate (voice or video) call count threshold (or inbound call count threshold).

c. Per the requirement for precedence calls in Section 2.11.2.3.2, either divert all precedence INVITEs to the attendant, or divert the precedence INVITE to the attendant if the INVITE would cause the appropriate (voice or video) call count threshold (or inbound call count threshold) to be exceeded.

2.11.3.7 AS-SIP – H.323 Gateway Media Interworking

SCM-004110 [**Required**] The AS-SIP – H.323 Gateway shall support the audio Codecs in Section 2.9.1.3, Audio Codecs, Voice Instruments.

SCM-004120 [**Required**] The AS-SIP – H.323 Gateway shall comply with Section 2.9.1.5, Voice over IP Sampling Standard, for the sampling rates.

SCM-004130 [**Required**] The AS-SIP – H.323 Gateway shall support the audio and video Codecs as specified in Section 2.9.3.3, Video Codecs (Including Associated Audio Codecs).

SCM-004140 [**Required**] The voice media packets generated by the IP EIs served by the H.323 UC signaling platform that are intended for a destination outside the enclave shall be interworked by the AS-SIP – H.323 Gateway into UCR-compliant voice packets that shall be sent to the SBC.

SCM-004150 [**Required: SBC**] The enclave SBC shall send the UCR-compliant voice media packets received from the UC WAN and intended for the IP EIs served by the H.323 UC signaling platform to the AS-SIP – H.323 Gateway.

SCM-004160 [**Required**] The AS-SIP – H.323 Gateway shall interwork the UCR-compliant voice media packets received from the SBC into the H.323 voice media packets used by the IP EIs, and then the H.323 voice media packets shall be forwarded to the IP EIs.

NOTE: The UCR does not specify the internal routing path of the voice media packets between the AS-SIP – H.323 Gateway and the IP EIs.

SCM-004170 [**Required**] The video media packets generated by the IP EIs served by the H.323 UC signaling platform that are intended for a destination outside the enclave shall be interworked by the AS-SIP – H.323 Gateway into UCR-compliant video packets that shall be sent to the SBC.

SCM-004180 [**Required: SBC**] The enclave SBC shall send the UCR-compliant video media packets received from the UC WAN and intended for the IP EIs served by the H.323 UC signaling platform to the AS-SIP – H.323 Gateway.

SCM-004190 [**Required**] The AS-SIP – H.323 Gateway shall interwork the UCR-compliant video media packets received from the SBC into the H.323 video media packets employed by the IP EIs and then the H.323 video media packets shall be forwarded to the IP EIs.

NOTE: The UCR does not specify the internal routing path of the video media packets between the AS-SIP – H.323 Gateway and the IP EIs.

2.11.3.8 Information Assurance

SCM-004200 [**Required**] The AS-SIP – H.323 Gateway shall satisfy the Information Assurance requirements in Section 4, Information Assurance, for an MG.

2.11.3.9 AS-SIP – H.323 Gateway Management Function

SCM-004210 [**Required**] TheAS-SIP – H.323 Gateway Management Function shall support the applicable requirements in Section 2.19, Management of Network Appliances:

2.11.3.10 AS-SIP – H.323 Gateway-to-EMS Interface

SCM-004220 [**Required**] The AS-SIP – H.323 Gateway shall provide an interface to the DISA EMS. The interface shall consist of a 10/100-Mbps Ethernet connection as specified in Section 2.7.4, DISA VVoIP EMS Interface.

NOTE: The AS-SIP – H.323 Gateway shall support one pair of Ethernet management interfaces where one management interface is for communication with a local EMS and one management interface is for communication with a remote EMS. In addition, the AS-SIP – H.323 Gateway shall support at least one additional Ethernet interface for carrying signaling and media streams for VVoIP traffic.

2.11.3.11 Product Quality Factors

SCM-004230 [**Required**] The AS-SIP – H.323 Gateway shall meet the product quality factors specified in Section 2.8.2, Product Quality Factors.

2.12 ENTERPRISE UC SERVICES

2.12.1 Introduction

The Enterprise UC Services Architecture consists of Enterprise Session Controller (ESC) Core Infrastructure products at a centralized "Master Site" location and Edge Infrastructure products at DoD Components' B/P/C/S locations. The ESC Core Infrastructure is composed of centralized ESC components, an ESC-fronting SBC, Enterprise Hosted UC Services and Enterprise Required Ancillary Equipment (RAE). The Edge Infrastructure consists of EIs, MGs, Enclave-fronting SBCs, local survivable call processing appliances (for Environments 1 and 2) and local RAE. When the ESC is implemented in a distributed cluster configuration, individual ESC "cluster members" are deployed within the Edge Infrastructure at Type 1 and 2 Environments (for further clarification, see Section 2.12.3.3.3). The centralized ESC Master Site, together with all of the served DoD Components' B/P/C/S locations, is collectively referred to as the Enterprise Services Area (ESA). This section of the UCR assumes that the reader is familiar with the Enterprise UC Services architecture and concepts defined in UC Framework 2013.

2.12.2 Enterprise Session Controller (ESC) Core Infrastructure

2.12.2.1 Enterprise Session Controller (ESC)

2.12.2.1.1 General

SCM-004240 [**Required**] The ESC shall support the SC requirements defined in Section 2.10, Session Controller (subject to the modifications and additions set forth in this subsection).

SCM-004250 [**Required**] The ESC shall support centralized, integrated voice, video and data session management on behalf of served IP end instruments (EIs) that are located at different enclaves (i.e., B/P/C/S sites) within the associated ESA.

SCM-004260 [**Required**] The ESC shall be capable of autonomously providing session management for all intra-ESA voice and video sessions (where both the caller and called party reside within the ESA).

SCM-004270 [**Required**] The ESC shall be capable of interoperating with other ESCs and SCs using AS-SIP as defined in the AS-SIP 2013.

SCM-004280 [**Required**] Under normal operating conditions, the ESC shall rely upon the SS for all inter-ESA call routing.

SCM-004290 [**Required**] The ESC shall have an availability of at least 99.999%.

SCM-004300 [**Required**] The ESC shall meet the IPv6 requirements defined in Section 5 of the UCR.

SCM-004310 [**Required**] The ESC shall support the DSCP marking requirements defined in Section 6, Network Infrastructure End-to-End Performance.

SCM-004320 [**Required**] Signaling, bearer, and Operations, Administration, Maintenance, and Provisioning (OAM&P) protocol traffic exchanged between the ESC Core infrastructure and the Edge infrastructure shall be capable of traversing DoD Component enclave and Enterprise Information Assurance (IA) accreditation boundaries using protocols that are approved by the Ports, Protocols, and Service Management (PPSM) Category Assurance List (CAL).

SCM-004330 [**Required**] The ESC shall support an interface to a Local RTS Routing Database (LRDB) to support database (DB) queries and DB responses in support of the Commercial Cost Avoidance feature as defined in Section 3, Auxiliary Services.

SCM-004340 [**Required**] The ESC shall support an interface to a Master RTS Routing Database (MRDB) in order to support the DB update capability as defined in Section 3, Auxiliary Services.

SCM-004350 [**Required**] Each time an end user/EI registers for service with the ESC, the ESC shall determine the served enclave where the originating EI resides. This information shall permit the ESC to correctly associate a served enclave with every inbound (EI-to-ESC) or outbound (ESC-to-EI) call leg. Such an association is essential to the correct execution of services such as ASAC, Commercial Access, and Precedence Call Diversion. The precise mechanism for determining the enclave from which the registration request originated is left up to the vendor's discretion.

2.12.2.1.2 Support for End Instruments (EIs)

SCM-004360 [**Required**] The ESC shall support EI session management functions defined for the SC in Section 2.10, Session Controller (subject to the modifications and additions set forth in this subsection).

SCM-004370 [**Required**] The ESC shall offer hardware based voice, video and videophone EIs.

SCM-004380 [**Required**] The ESC shall offer soft clients that provide access to integrated UC services from a common user interface. In performing this function, the ESC shall comply with the softphone requirements defined in Section 2.9.1.6, Softphones.

SCM-004390 [**Required**] The ESC shall support an AS-SIP "ESC-to-EI" signaling interface in support of AS-SIP EIs (AEIs) as defined in this section and the AS-SIP 2013.

NOTE: The ESC solution is not required to include AEIs.

SCM-004400 [**Conditional**] If the ESC supports Proprietary EIs (PEIs), then the vendor-proprietary "ESC-to-EI" signaling interface shall comply with the PEI signaling requirements as defined in Section 2.9.1, IP Voice End Instruments (subject to the modifications and additions set forth in this subsection).

SCM-004410 [**Required**] The ESC shall provide registrar functionality for all of its served EIs.

2.12.2.1.3 Centralized Configuration and OAM&P

SCM-004420 [**Required**] The ESC shall provide a centralized configuration service that permits served Edge Infrastructure products (EIs, MGs, SBCs, F1SCs, F2SCs, and distributed ESC cluster members) to securely retrieve/download configuration files. The signaling and transport used to initiate and complete the retrieval and download of configuration files must be able to traverse DoD Component enclave and Enterprise IA accreditation boundaries using protocols that are approved by the PPSM CAL.

SCM-004430 [**Required**] The ESC shall enable centralized management and distribution of firmware/software updates directly to Edge Infrastructure products (including EIs, SBCs, MGs, F1SCs, F2SCs, and distributed ESC "cluster members"). The signaling and transport used to initiate and complete the distribution of firmware/software updates must be able to traverse DoD Component enclave and Enterprise IA accreditation boundaries using protocols that are approved by the PPSM CAL.

SCM-004440 [**Required**] The ESC vendor shall provide management solutions that enable the "centralized" provisioning, administration, management, accounting and monitoring of all ESC Cor Infrastructure components (i.e., including the centralized ESC, ESC-fronting SBC, and Enterprise Hosted UC Services) and all Edge Infrastructure components within the ESA (including EIs, Enclave-fronting SBCs, MGs, F1SCs, F2SCs, and distributed ESC "cluster members").

SCM-004450 [**Required**] The ESC shall permit local enclave administrators at served B/P/C/S locations to have secure, restricted access to the provisioning capabilities of the ESC for the purpose of provisioning local moves, adds and changes (MACs). Enclave administrative access privileges to the ESC's centralized provisioning capabilities shall be restricted to the extent that the local administrators can see and make only the provisioning changes that affect their local user community.

NOTE: The local administrator must be able to provision local moves, adds and changes without having root/super user access to ESC system management.

2.12.2.1.4 Commercial Access

SCM-004460 [**Required**] The ESC shall centrally provide MG Controller (MGC) functionality as defined in this section. In performing this function, the ESC shall be capable of routing commercial calls to an MG that resides in the same local enclave as the call originator. In the execution of this capability, the ESC shall leverage end user/EI-to-enclave association data determined at the time of end user/EI registration as described in Section 2.12.2.1.1.

SCM-004470 [**Required**] The ESC shall be capable of using AS-SIP to route commercial calls to the SS. To disambiguate an E.164 telephony number from a 10-digit DSN number within the AS-SIP Request URI, the ESC shall strip away any prefix digits and shall add the leading "+" character to the commercial numbers which shall be composed of the country code (CC) and national specific numbers.

NOTE: The SS is responsible for routing commercial traffic to an SBC at a DoD Internet Access Point (IAP) in order to interface with a Voice Internet Service Provider (ISP) carrier.

SCM-004480 [**Required**] The ESC shall permit the provisioning of a Commercial Access Route on a per DoD Component Enclave-basis. Commercial Access Route provisioning data shall dictate whether a commercial call is routed to an MG that resides in the same local enclave as the call originator or to the SS.

2.12.2.1.5 ASAC

SCM-004490 [**Required**] The ESC shall support the ASAC requirements for the SC related to voice and video session management as defined in this section and the AS-SIP 2013 (subject to the modifications and additions set forth in this subsection).

SCM-004500 [**Required**] To regulate IP access link utilization, the ESC shall manage a separate voice and video budget for each of its served enclaves.

SCM-004510 [**Required**] The ESC shall provide the capability for the system administrator to configure a separate voice and video budget for each enclave.

SCM-004520 [**Required**] In the execution of centralized line-side ASAC enforcement, the ESC shall be capable of assigning calls to or from a served EI to the correct ASAC budget. In the execution of this capability, the ESC shall leverage end user/EI-to-enclave association data determined at the time of end user/EI registration as described in Section 2.12.2.1.1.

SCM-004530 [**Required**] To enable the correct execution of ASAC, the ESC shall be able to differentiate between intra-enclave calls (which will not consume IP access link bandwidth) and inter-enclave calls (which will consume IP access link bandwidths):

a. The ESC shall increment the corresponding ASAC budget based upon each inter-enclave session origination.

b. The ESC shall, likewise, decrement the corresponding ASAC budgets based upon each inter-enclave session termination.

c. The ESC shall not increment or decrement ASAC budgets based upon intra-enclave session originations or terminations.

SCM-004540 [**Required**] The ESC shall be capable of supporting up to 500 ASAC budgets across the ESA.

SCM-004550 [**Required**] With regards to the management of voice and video call counts across IP access links internal to the ESA, the ESC shall not be subject to ASAC policing by the SS.

NOTE: The ESC autonomously manages (without the involvement of the SS) intra-ESA voice and video sessions. Because the SS is not involved in the session management of intra-ESA voice and video sessions, it is not able to maintain an accurate accounting of voice and video call counts across IP access links internal to the ESA. As a result the SS is not in a position to police ASAC compliance across these IP access links which are internal to ESA.

2.12.2.2 Centralized Enterprise Hosted UC Services

2.12.2.2.1 UC Audio and Video Conferencing

SCM-004560 [**Required**] The centralized ESC shall provide AS-SIP based audio and video conferencing capabilities by means of a collocated UC audio and video conference system.

SCM-004570 [**Required**] The ESC shall be in the signaling path for all signaling messages exchanged between EIs served by the ESC and the associated audio and video conference system.

SCM-004580 [**Required**] The conference system is not required to understand or act upon call precedence or to support the preemption of participants or conferences.

SCM-004590 [**Required**] The conference system shall provide a “service portal” for end user access to UC conferencing services, features, and capabilities.

SCM-004600 [**Required**] The conference system shall provide notification of participants joining and leaving a conference and provide an end-of-conference warning to all participants.

SCM-004610 [**Required**] The conference system shall provide the following conferencing chair control functionality:

a. Voice-activated switching.

b. Continuous presence.

c. Mute and unmute all conference participants.

d. Enable/disable extension of a conference.

e. Capability to "force disconnect" select participants from a conference.

SCM-004620 [**Required**] A video conference system shall be capable of accepting audio-only participants into a conference call.

SCM-004630 [**Optional**] Audio conference systems shall support the following audio codes: G.711, G.722, G.722.1, G.723.1, G.728, G.729A.

SCM-004640 [**Required**] Video conference systems shall support the following audio codecs: G.711, G.722, G.722.1, G.723.1, G.728, G.729A and video codecs: H.263-200 and H.264.

SCM-004650 [**Required**] The conference system shall provide a Reservationless, Meet-Me Audio Conference service.

SCM-004660 [**Required**] The conference system shall provide an Ad hoc Audio Conference service.

SCM-004670 [**Required**] The conference solution shall provide a Scheduled Audio Conference service.

SCM-004680 [**Required**] The conference solution shall provide Preset Conferencing capabilities.

2.12.2.2.2 Announcements and Music on Hold

SCM-004690 [**Required**] The ESC shall be capable of centrally providing announcements for served EIs without a noticeable degradation in the quality of the audio transmission. The delivery of the announcement shall not be adversely impacted by traversing Enterprise or DoD Component IA accreditation boundaries (using protocols that are approved by the PPSM CAL) or by WAN transport impairments (e.g., delay, packet loss).

SCM-004700 [**Required**] The ESC shall centrally provide the set of announcements required of an SC as defined in this section.

SCM-004710 [**Conditional**] If the ESC provides music-on-hold capabilities, the music-on-hold shall be implemented as defined in AS-SIP 2013.

2.12.2.2.3 Enterprise E911 Call Management

SCM-004720 [**Required**] The ESC shall support an integrated E911 Management capability that enables EI location information to be provided to the local emergency response dispatch center (e.g., an off-base or on-base PSAP) that is associated with each enclave within the ESA.

SCM-004730 [**Required**] For each enclave served by the ESC, the integrated E911 Management capability shall support the generation of enclave-specific Private Switch/Automatic Location Information (PS/ALI) database records that maps Emergency Response Locations (ERLs) to corresponding Emergency Location Identification Numbers (ELINs) as described in Section 3, Auxiliary Services.

NOTE: The DoD Component enclave administrator is responsible for establishing/defining ERLs across a particular B/P/C/S location. This information must be reliably provided to the system administrator for the E911 management capability associated with the ESC.

SCM-004740 [**Required**] After the individual PS/ALI database records have been generated, the integrated E911 Management solution shall be capable of exporting the enclave-specific PS/ALI record to the ALI database provider associated with the local off-base or on-base PSAP that is geographically responsible for the 911 caller. The integrated E911 Management solution shall be capable of exporting the enclave-specific PS/ALI records using the file formats defined in Section 3, Auxiliary Services.

SCM-004750 [**Required**] The provisioning capabilities associated with the ESC's integrated 911 Management solution shall permit the manual association of an end user/EI to an ERL based upon the physical location of the end user/EI at the time of end user/EI provisioning.

SCM-004760 [**Optional**] During the end user/EI registration process, the ESC shall prompt the user to establish/update their location leveraging the display capabilities of the associated softphone or hardphone:

a. The end user shall have the option of selecting from a list of locations that is presented to the end user via the user interface associated with the softphone or hardphone. Additionally, the end user should be permitted to select their last location or select from a list of "favorites."

b. Once the location has been selected by the end user, the integrated E911 management capability shall have the capability to map the location selected by the end user to an associated ERL.

SCM-004770 [**Required**] Based on available end user/EI-to-ERL association data, the integrated E911 management capabilities shall permit the ESC to dynamically determine the correct ELIN to associate with each EI that originates a 911 emergency call.

SCM-004780 [**Required**] If the integrated E911 management capability cannot determine the physical location of the EI originating the 911 call (i.e., it does not have specific EI-to-ERL association data for the EI that is originating the 911 call), it shall assign an enclave-specific "default ERL" to the call based on EI-to-enclave association data the ESC established during the EI registration process (see Section 2.12.2.1.1). The integrated E911 management solution shall be capable of generating and exporting ALI database records for the default ERL and the associated ELIN. The ALI record associated with the default ERL shall include:

a. The address associated with the main Listed Directory Number (LDN) for the associated B/P/C/S location.

b. An explicit notification that the caller's detailed location is not known and that a default routing of the emergency call has occurred.

c. Contact information for on-site emergency personnel.

SCM-004790 [**Required**] Using ISDN PRI trunks off an MG in the same enclave as the 911 caller, the ESC shall route the emergency call to the regional 911 network provider who is responsible for routing the emergency call to the PSAP that is geographically responsible for the 911 caller.

SCM-004800 [**Required**] Prior to sending the call to the 911 network provider, the ESC's MGC capability shall substitute the appropriate ELIN number in place of the original Calling Party Number in the ISDN PRI setup message as described in Section 3 of the UCR. The ELIN will enable the proper routing of the call and location identification at the appropriate PSAP.

SCM-004810 [**Required**] The ESC shall be capable of routing a "911 PSAP call back" to the EI that originated the 911 call. In the process of substituting the original Calling Party Number with an ELIN, the ESC shall temporarily cache the telephone number of the EI from which the 911 call was made (indexed against the corresponding ELIN). In the event that the PSAP dispatcher calls back using the ELIN, the ESC shall use the cached telephone number to route the "call back" to the EI that initiated the 911 call.

2.12.2.2.4 Voicemail and Unified Messaging

SCM-004820 [**Required**] The ESC shall provide a voicemail capability inherent to the solution or be configurable to interface with the Microsoft Unified Messaging (MS-UM) Voicemail solution as its voicemail platform.

SCM-004830 [**Required**] The ESC shall provide a mechanism that allows for Voicemail messages to be accessed via the Microsoft Outlook Email Client.

SCM-004840 [**Conditional**] If the ESC interfaces with a MS-UM Server within Microsoft Exchange Server 2010 Suite, it shall follow the requirements as stated in Section 2.12.2.2.4.1. Else, the ESC shall support EWS APIs to interface with the Microsoft Client Access Server (CAS) to provide UM functionalities as described in Section 2.12.2.2.4.2.

2.12.2.2.4.1 ESC Requirements for Interfacing With Microsoft Unified Messaging (MS-UM) Voicemail Server

SCM-004850 [**Required**] The ESC shall support the capability to forward unanswered or diverted calls to an AS-SIP enabled MS-UM appliance capable of traversing DoD Components IA accreditation boundaries in accordance with Facility Security Office (FSO) and PPSM policy.

SCM-004860 [**Required**] The ESC shall support the capability to signal SIP with TLS to a SIP enabled MS-UM appliance using TCP port 5061.

SCM-004870 [**Required**] The ESC shall support SRTP for delivery and encryption of media when interfacing with a SIP enabled MS-UM appliance.

SCM-004880 [**Required**] The ESC shall support SIP Diversion as specified in historic RFC 5806; in particular, the ESC shall recognize warning code 302 "Moved Temporarily" to redirect the message to the MS-UM worker process using media channels TCP ports 5065 or 5066.

SCM-004890 [**Required**] The ESC shall wait until the ACK message is sent for the 200 OK messages before media exchange can begin as MS-UM does not support early media.

SCM-004900 [**Conditional**] If the IP address of the "To:" header does not match the MS-UM IP Gateway object IP address or if the extension does not match a MS-UM pilot number listed in a MS-UM hunt group, then the ESC shall support SIP Diversion as specified in historic RFC 5806; in particular, the ESC shall recognize warning code 302 "Moved Temporarily" to anticipate repackaging a second SIP Invite in order for the MS-UM appliance to be able to recognize the proper voicemail box.

SCM-004910 [**Required**] The ESC shall support local certificate stores to enable TLS communications.

SCM-004920 [**Required**] The ESC shall support mutual TLS authentication and negation to establish sessions with MS-UM.

SCM-004930 [**Required**] The ESC shall support seamless integration of email and voicemail messages into a single Outlook Client.

SCM-004940 [**Required**] The ESC shall support synchronization of the Message-Waiting Indicator (MWI) on the end user's phone based on user interaction (i.e., Play, Delete, Read) with voicemails in the Outlook Client.

SCM-004950 [**Required**] The ESC shall support configuration for at least two independent paths for redundancy to help ensure voicemails can always be sent to the MS-UM Appliance in case of outage or offline maintenance.

SCM-004960 [**Required**] The ESC shall support configuration with a primary and backup MS-UM servers.

SCM-004970 [**Required**] The ESC shall support verification and notification that the primary MS-UM server is down.

SCM-004980 [**Required**] The ESC shall support verification and notification that the backup MS-UM server is operational and is currently handling calls when the link to the primary server is down.

SCM-004990 [**Required**] The ESC shall support mutual synchronization of voicemail and email message status (i.e., "read"/"unread") between Outlook and the EI and shall reciprocate seamlessly between the EI and Outlook.

SCM-005000 [**Required**] The ESC shall have the capability to support E.164 or Alpha-Numeric "UserInfo" resource identifiers to be passed to MS-UM for processing as subscriber extensions.

2.12.2.2.4.2 ESC Requirements for Interfacing With Exchange Web Services Application Programming Interface

SCM-005010 [**Required**] The ESC shall support Exchange Web Services (EWS) Application Programming Interface (API) integration with DoD Enterprise Email (DEE). This includes support of the Simple Object Access Protocol (SOAP) and XML based EWS operations which provide the messaging framework for integration between the ESC and the DEE server.

SCM-005020 [**Required**] The ESC shall support DoD Directory Services integration with DEE.

SCM-005030 [**Required**] The ESC shall support integration with the DEE Client Access Server (CAS) which is responsible for interfacing the different DEE server roles with the ESC.

SCM-005040 [**Required**] The ESC shall use EWS to support mutual synchronization of voicemail and email message status (i.e., "read"/"unread") between DEE clients and the EI and reciprocate seamlessly between the EI and DEE clients.

SCM-005050 [**Required**] The ESC shall use EWS to support synchronization of the Message-Waiting Indicator (MWI) on the end user's phone based on user interaction with voicemails in the DEE clients.

SCM-005060 [**Required**] The ESC shall use EWS to provide a Voicemail Form window which is embedded within the DEE clients.

SCM-005070 [**Required**] The Voicemail Form shall provide the following options:

a. Clearly delineates a Voice Message from an Email Message.
b. Embeds Media Player Controls with the following functional buttons: Stop, Play, Pause, Progress Bar, Volume Bar, Previous, Next and Mute.
c. Assimilates the look and feel of the DEE client interface.

SCM-005080 [**Optional**] The ESC shall use EWS to provide the Play-on-Phone Feature, which enables users to send a request to the UM server, via the Voicemail Form, to play a selected voice message on their phone or send the voice message to another telephone number they specify.

SCM-005090 [**Optional**] The ESC shall use EWS to support the DEE client speech-to-text feature; that enables users to view the text transcription of the actual voice mail message as was left by a caller.

SCM-005100 [**Optional**] The ESC shall use EWS to support the DEE client speech-to-text feature; that enables subscribers to retrieve e-mail messages from their individual mailbox using an analog, digital, or mobile telephone.

2.12.2.2.5 IM/Chat/Presence Federation

SCM-005110 [**Required**] The ESC shall support secure Extensible Messaging and Presence Protocol (XMPP) server-to-server federation (i.e., server-to-server interoperability) in support of near real-time, text-based messaging (including instant messaging, group chat, and the exchange of presence) in accordance with the UC XMPP 2013.

SCM-005120 [**Required**] The ESC shall have a migration path to federate with the IM/Chat/Presence services of Defense Connection Online (DCO) in accordance with the server-to-server interface requirements defined in the UC XMPP 2013.

SCM-005130 [**Required**] In support of IM/Chat/Presence services within the ESA, the ESC shall provide secure client-to-server connections to served EIs. The client-to-server protocol from the ESC to the EI shall be either XMPP or vendor-proprietary (e.g., a vendor specific implementation of SIP/SIMPLE).

SCM-005140 [**Conditional**] If vendor-proprietary, client-to-server protocols are used, the proprietary protocols shall be able to federate with native XMPP servers through the use of an XMPP gateway implementation that provides the bidirectional translation between XMPP and the proprietary protocol as defined in the UC XMPP 2013.

2.12.2.2.6 Enterprise Directory Services

This section provides requirements for Enterprise Directory Services (EDS), provided by Enterprise Session Controllers (ESCs) and UC Video Conference Bridges for Enterprise UC end users.

The term “UC Video Conference Bridge,” as used in this section, has the same meaning as “UC Audio and Video Conferencing System,” as specified in Section 3.4, UC Audio and Video Conference System.

Acronyms used in this section are as follows:

- DEE GAL: DoD Enterprise Email Global Address List.
- DMDC: Defense Manpower Data Center (part of OSD, not DISA).
- EASF: Enterprise Applications and Services Forest.
- IDMI: IdSS Machine Interface.
- IdSS: Identity Synchronization Service.

2.12.2.2.6.1 EDS Client

SCM-005150 [**Required: Voice EI with EDS Client, Video EI with EDS Client**] The EDS Client application shall support an interface to the EDS Gateway. This interface shall support transmission of directory queries in the Client-to-Gateway direction, and transmission of directory query responses in the Gateway-to-Client direction.

NOTE: The protocol used on this interface is up to the EDS Client (EI) and EDS Gateway (ESC or Conference Bridge) supplier.

SCM-005160 [**Required: Voice EI with EDS Client, Video EI with EDS Client**] The EDS Client shall be able to authenticate itself with the EDS Gateway using a set of EDS Authentication Credentials that are stored in the EDS Client and signaled to the EDS Gateway before an EDS directory query is sent.

SCM-005160.a [**Required: Voice EI with EDS Client, Video EI with EDS Client**] The EDS Client shall support the storage and signaling of a Username and Password as EDS Authentication Credentials. In this case, the Username and Password should be unique to that EDS Client, and should not be shared with other EDS Clients on Voice EIs and Video EIs served by that EDS Gateway.

SCM-005170 [**Required: Voice EI with EDS Client, Video EI with EDS Client**] The EDS Client shall be able to generate directory queries containing the following IdSS directory attributes. The query shall include all or some of the following attributes:

- First Name.
- Middle Initials.
- Last Name.
- Company Name (DoD Component or CC/S/A Name, e.g., “DISA”).
- Department Name (e.g., Organization Name within Component or CC/S/A, e.g., “ESD”).
- E-mail address.
- Business phone number.
- Mobile phone number.
- Rank.
- Office.

- DoD SIP URI (e.g., sip:FirstName.MiddleInitials.LastName.civ@uc.mil).

SCM-005180 [**Optional: Voice EI with EDS Client, Video EI with EDS Client**] The EDS Client shall also be able to generate directory queries containing the following additional IdSS directory attributes. The query shall include all or some of the following attributes:

- LDAP Distinguished Name.
- Address
- City.
- State.
- Zip Code.
- Country / Region.
- Display Name (e.g., "Captain John A Smith USAF ACC").
- Fax number.
- Job Title.
- Alias (Mail Nickname).

SCM-005190 [**Required: Voice EI with EDS Client, Video EI with EDS Client**] The EDS Client shall be capable of accepting EDS query responses from the EDS Gateway, and displaying those query responses to the EI end user. The attributes shall be as follows:

- LDAP Distinguished Name.
- First Name.
- Middle Initials.
- Last Name.
- Alias (Mail Nickname).
- Country / Region.
- Address.
- City.
- State.
- Zip Code.
- Rank.
- Office.
- Display Name (e.g., "Captain John A Smith USAF ACC").
- Job Title.
- Company Name (DoD Component or CC/S/A Name, e.g., "DISA").
- Department Name (Organization Name within Component or CC/S/A, e.g., "ESD").
- E-mail address.
- Business phone number.
- Mobile phone number.
- Fax number.
- DoD SIP URI (e.g., sip:FirstName.MiddleInitials.LastName.civ@uc.mil).

SCM-005200 [**Required: Voice EI with EDS Client, Video EI with EDS Client**] The EDS Client shall also be capable of accepting any attribute from the EDS Gateway in an EDS query

response, and displaying that attribute in the EDS query response to the EI end user, without deleting or removing that attribute from the EDS query response.

NOTE: In other words, the set of attributes that the EDS Client displays to the EI end user should be limited by the set of attributes that the EDS Gateway returns to the EDS Client, and should not be limited by the set of required IdSS directory attributes listed in the previous requirement.

SCM-005210 [**Required: Voice EI with EDS Client**] The EDS Client on the Voice EI shall allow the EI end user to review the query responses returned by the EDS Gateway, and set up a Voice call to a target DoD end user by 1) selecting that end user's data record from the set of responses received, and 2) selecting the called address (DSN number, commercial wireline number, commercial mobile number, or DoD SIP URI) from that record. The Voice EI shall then use that record and address to place a VoIP call to the target DoD end user.

SCM-005220 [**Required: Video EI with EDS Client**] The EDS Client on the Video EI shall allow the EI end user to review the query responses returned by the EDS Gateway, and set up a Video call to a target DoD end user by 1) selecting that end user's data record from the set of responses received, and 2) selecting the called address (DSN number or DoD SIP URI) from that record. The Video EI shall then use that record and address to place a Video call to the target DoD end user.

2.12.2.2.6.2 EDS Gateway

SCM-005230 [**Required: ESC with EDS Gateway, UC Video Conference Bridge with EDS Gateway**] The EDS Gateway shall support interfaces to EDS Clients on both Voice EIs and Video EIs.

a. Each of these interfaces shall support transmission of directory queries in the Client-to-Gateway direction, and transmission of directory query responses in the Gateway-to-Client direction.

NOTE: The protocol used on these interfaces is up to the EDS Client (EI) and EDS Gateway (ESC or Conference Bridge) supplier. For example, the LDAP protocol can be used, or another protocol like Hypertext Transfer Protocol Secure (HTTPS)/XML can be used instead. In the latter case, the format of the queries and responses exchanged within the XML messages is up to the supplier.

SCM-005240 [**Required: ESC with EDS Gateway, UC Video Conference Bridge with EDS Gateway**] The EDS Gateway shall require each EDS Client to authenticate itself with the EDS Gateway, before accepting EDS queries from that EDS Client, or returning EDS query responses to that EDS Client.

a. The EDS Gateway shall require each EDS Client to authenticate using a set of EDS Authentication Credentials that are stored in the EDS Gateway and signaled by the EDS

Client before an EDS directory query is sent. At a minimum, the EDS Gateway shall support the storage and signaling of a Username and Password as EDS Authentication Credentials. In this case, the Username and Password should unique to each EDS Client, and should not be shared with other EDS Clients on other Voice EIs and Video EIs served by that EDS Gateway.

SCM-005250 [**Required: ESC with EDS Gateway, UC Video Conference Bridge with EDS Gateway**] The EDS Gateway shall be able to accept and process directory queries from EDS Clients containing the following IdSS directory attributes. The query shall include all or some of the following attributes:

- First Name.
- Middle Initials.
- Last Name.
- Company Name (DoD Component or CC/S/A Name, e.g., "DISA").
- Department Name (Organization Name within Component or CC/S/A, e.g., "ESD").
- E-mail address.
- Business phone number.
- Mobile phone number.
- Rank.
- Office.
- DoD SIP URI (e.g., sip:FirstName.MiddleInitials.LastName.OrgName@uc.mil).

SCM-005260 [**Optional: ESC with EDS Gateway, UC Video Conference Bridge with EDS Gateway**] The EDS Gateway shall also be able to accept and process directory queries from EDS Clients containing the following additional IdSS directory attributes. The query shall include all or some of the following attributes:

- LDAP Distinguished Name.
- Address.
- City.
- State.
- Zip Code.
- Country / Region.
- Display Name (e.g., "Captain John A Smith USAF ACC").
- Fax number.
- Job Title.
- Alias (Mail Nickname).

SCM-005270 [**Required: ESC with EDS Gateway, UC Video Conference Bridge with EDS Gateway**] The EDS Gateway shall be able to authenticate itself with the UC DEE GAL Server, using LDAP Authentication Credentials that are stored in the EDS Gateway and signaled to the DEE GAL Server before an LDAP directory query is sent. At a minimum, the EDS Gateway shall support the storage and signaling of a Username and Password as LDAP Authentication Credentials. In this case, the Username and Password should unique to that EDS Gateway, and

should not be shared with other EDS Gateways on other ESCs and Video Conference Bridges that are served by that DEE GAL Server.

SCM-005280 [**Required: ESC with EDS Gateway, UC Video Conference Bridge with EDS Gateway**] Upon receipt of an EDS directory query from an EDS Client, the EDS Gateway shall convert this EDS query to a LDAP query, and send this LDAP query on to the UC DEE GAL Server that serves the ESC or Video Conference Bridge.

a. The EDS Gateway shall include all of the EDS query attributes signaled by the EDS Client in the LDAP query that it sends to the UC DEE GAL Server.

b. The EDS Gateway shall use its own Authentication Credentials to authenticate itself with the UC DEE GAL Server before sending the LDAP query; it should not use any EDS Client Authentication Credentials for that purpose.

SCM-005290 [**Required: ESC with EDS Gateway, UC Video Conference Bridge with EDS Gateway**] Upon receipt of an LDAP query response from the UC DEE GAL Server, the EDS Gateway shall convert this LDAP query response to an EDS query response that is compatible with the EDS Client (e.g., an HTTPS/XML query response, if the EDS Client supports HTTPS/XML instead of LDAP). The EDS Gateway shall then send this EDS query response on to the EDS Client on the Voice EI or Video EI that originally sent the EDS query to the Gateway.

a. The EDS Gateway shall include all of the query response components (both user records and user record attributes) in the LDAP response that it received from the UC DEE GAL server, in the EDS query response that it sends on to the EDS Client.

SCM-005300 [**Required: ESC with EDS Gateway, UC Video Conference Bridge with EDS Gateway**] The EDS Gateway shall be capable of accepting LDAP query responses from the UC DEE GAL Server that contain the following IdSS directory attributes:

a. The EDS Gateway shall also be capable of sending EDS query responses to the EDS Client that contain the following IdSS directory attributes:

- LDAP Distinguished Name.
- First Name.
- Middle Initials.
- Last Name.
- Job Title.
- Alias (Mail Nickname).
- Rank.
- Office.
- Display Name (e.g., “Captain John A Smith USAF ACC”)
- Company Name (DoD Component or CC/S/A Name, e.g., “DISA”).
- Department Name (Organization Name within Component or CC/S/A, e.g., “ESD”).

- Country / Region.
- Address.
- City.
- State.
- Zip Code.
- E-mail address.
- Business phone number.
- Mobile phone number.
- Fax number.
- DoD SIP URI (e.g., sip:FirstName.MiddleInitials.LastName.civ@uc.mil).

SCM-005310 [**Required: ESC with EDS Gateway, UC Video Conference Bridge with EDS Gateway**] The EDS Gateway shall also be capable of accepting any LDAP attribute from the UC DEE GAL Server in an LDAP query response, and sending that attribute on to the EDS Client in the corresponding EDS query response, without deleting or removing that attribute from the EDS query response.

NOTE: In other words, the set of attributes that the EDS Gateway returns to the EDS Client should be limited by the set of LDAP attributes that the UC DEE GAL Server returns to the EDS Gateway, and should not be limited by the set of required IdSS directory attributes listed in the previous requirement.

2.12.2.2.7 Enterprise Accounting Management

SCM-005320 [**Required**] The ESC shall centrally support the minimum set of requirements to capture basic call information for accounting purposes as defined in ~~this section~~Section 2.19.2.3, Accounting Management.

2.12.2.2.8 Precedence Call Diversion

SCM-005330 [**Required**] The ESC shall provide a default diversion of all unanswered calls above ROUTINE precedence to a designated DN (e.g., an attendant console) as defined in this section. The designated DN shall be a DN associated with an EI (e.g., an attendant console) in the same enclave as the original called party.

2.12.3 Edge Infrastructure

2.12.3.1 End Instruments

2.12.3.1.1 Proprietary End Instrument (PEI)

SCM-005340 [**Conditional**] If a PEI is served by the ESC, the PEI shall comply with the PEI requirements defined in Section 2.9.1.6, (subject to the modifications and additions set forth in this subsection).

SCM-005350 [**Conditional**] If a PEI is served by the centralized ESC, the proprietary signaling exchanged between the PEI and the ESC shall be capable of traversing DoD Component enclave and Enterprise IA accreditation boundaries using protocols that are approved by the PPSM CAL.

SCM-005360 [**Conditional**] If a PEI is served by the centralized ESC and the PEI is relying upon the enclave-fronting SBC to facilitate the traversal of the enclave IA accreditation boundary, the PEI shall comply with the following:

a. As a part of the normal startup and configuration process, the PEI shall obtain the IPv4 address and IPv6 address of the local enclave-fronting SBC.

b. The PEI shall establish a secure persistent connection (TLS or equivalent) with the enclave-fronting SBC.

c. The PEI shall send and receive all signaling messages over the TLS or equivalent connection with the enclave-fronting SBC.

NOTE: The requirement above is not intended to exclude the alternative of PEIs being served by the ESC which do NOT rely upon the enclave-fronting SBC to facilitate the traversal of the enclave IA accreditation boundary.

SCM-005370 [**Conditional**] If a PEI is served by the centralized ESC and the PEI is not relying upon the enclave-fronting SBC to facilitate the traversal of the enclave IA accreditation boundary, then the signaling traffic and bearer traffic associated with the PEI must be capable of traversing the enclave IA accreditation boundary via the data firewall using protocols that are approved by the PPSM CAL and in a manner acceptable to the FSO.

SCM-005380 [**Conditional**] If a PEI is being served by the centralized ESC and access to the ESC is interrupted, then the PEI shall failover to a survivable call processing appliance within the local enclave (Environments 1 and 2).

a. When access to the ESC is restored, the PEI shall failback and re-register with the ESC.

2.12.3.1.2 AS-SIP End Instrument (AEI)

SCM-005390 [**Required**] The AEIs shall comply with AEI requirements in this section and the AS-SIP 2013 (subject to the modifications and additions set forth in this subsection).

SCM-005400 [**Required**] As a part of the normal startup and configuration process, AEIs served by the centralized ESC shall obtain the IPv4 address and IPv6 address of their enclave-fronting SBC.

SCM-005410 [**Required**] AEIs served by the centralized ESC shall establish a persistent TLS connection with the enclave-fronting SBC.

SCM-005420 [**Required**] AEIs served by the centralized ESC shall send and receive all AS-SIP messages over the TLS connection with the enclave-fronting SBC (i.e., the enclave-fronting SBC serves as the outbound and inbound proxy for all SIP signaling including REGISTER requests).

SCM-005430 [**Required**] In the event that access to the serving centralized ESC is interrupted for AEIs served by the centralized ESC, the AEI shall failover to a survivable call processing instance within the local enclave.

a. When access to the ESC is restored, the AEI shall be capable of discovering the service restoration and of subsequently re-registering with the centralized ESC.

2.12.3.2 Media Gateway

SCM-005440 [**Required**] MGs that reside at DoD Component enclaves within the ESA shall support the MG requirements defined in this section (subject to the modifications and additions set forth in this subsection).

SCM-005450 [**Required**] The MG shall be capable of securely registering with and sending/receiving control signaling to and from the MGC component of the centralized ESC. Registration messages and control signaling sent or received by the MG to or from the centralized ESC shall be capable of traversing DoD Component enclave and Enterprise IA accreditation boundaries using protocols that are approved by the PPSM CAL.

SCM-005460 [**Required**] In the event that access to the serving centralized ESC is interrupted, the MG shall failover to a survivable call processing appliance within the local enclave.

When access to the ESC is restored, the MG shall failback to the ESC.

2.12.3.3 COOP

2.12.3.3.1 Environment Types

DoD Components shall determine the appropriate Mission Environment Type for each B/P/C/S site in line with the mission being performed at each respective location. A site's Mission Environment Type dictates the Continuity of Operations (COOP) requirements (i.e., the requirement for locally provided UC services when access to the centralized ESC is interrupted) for that location. The COOP requirements in turn dictate the technical solution components that must be deployed at each location.

SCM-005470 [**Required**] During normal operating conditions, end users at Environment 1, 2, or 3 locations shall all have access to the full complement of UC services provided by the ESC and the associated Enterprise hosted UC services.

2.12.3.3.1.1 Environment 1: Mission Critical (B/P/C/S)

SCM-005480 [**Required**] When access to the ESC is interrupted, an Environment 1 location shall have access to a minimum essential set of locally-provided UC services. The minimum essential set of locally provided UC services shall include the following:

a. Intra-base precedence calling capability with TLS (or equivalent) for signaling and SRTP for bearer.

b. Preset audio conferencing services (sized per customer requirements).

c. Video point-to-point.

d. Local-user presence, IM, and cha (sized per customer requirements).

e. 911 services.

f. PSTN/DSN access via local MG (sized per customer requirements).

g. Support for both PEIs and AEIs.

NOTE: Voicemail services are expected to be centrally provided by the ESC. In the event that access to the ESC is interrupted, ESC-based voicemail services will not be available.

2.12.3.3.1.2 Environment 2: Mission and Combat Support (B/P/C/S)

SCM-005490 [**Required**] When access to the ESC is interrupted, an Environment 2 location shall have access to locally provided voice services. Locally-provided voice services shall include the following:

a. Basic intra-base calling capability (ROUTINE service only) with TLS (or equivalent) for signaling and SRTP for bearer.

b. PSTN and 911 access via local MG (sized per customer requirements).

c. Support for both PEIs and AEIs.

2.12.3.3.1.3 Environment 3: Non Mission Critical Locations (B/P/C/S)

SCM-005500 [**Required**] When access to the ESC is interrupted, an Environment 3 location requires no survivable, locally provided UC services. In this case, PSTN, E911 and other services shall be provided by other means (e.g., cellular).

2.12.3.3.2 Survivable Call Processing

2.12.3.3.2.1 Failover Session Controller

SCM-005510 [**Required**] The Failover Type 1 Session Controller (F1SC) shall support the COOP requirements of Environment 1 sites (see Section 2.12.3.3.1.1). When access to the ESC is interrupted, the F1SC shall locally provide the following UC services:

a. Intra-base precedence calling capability with TLS (or equivalent) for signaling and SRTP for bearer.

b. Preset audio conferencing services (sized per customer requirements).

c. Video point-to-point.

d. Local-user presence, IM, and chat (sized per customer requirements).

e. 911 services.

f. PSTN/DSN access via local MG (sized per customer requirements).

g. Support for both PEIs and AEIs.

NOTE: An F1SC is not intended to provide the full suite of capabilities required of an SC.

SCM-005520 [**Required**] The F1SC shall provide local registrar functionality to EIs and MGs during the period of the ESC outage.

SCM-005530 [**Required**] The F1SC shall provide MGC functionality to local MGs during the period of the ESC outage.

NOTE: A F1SC will normally be deployed in a simplex configuration (without full server redundancy). However, the vendor must also support a redundant F1SC configuration option for select Environment Type 1 locations that stipulate a need for that kind of system/platform redundancy.

2.12.3.3.2.2 Failover Type 2 Session Controller (F2SC)

SCM-005540 [**Required**] The Failover Type 2 Session Controller (F2SC) shall support the COOP requirements of Environment 2 sites (see Section 2.12.3.3.1.2). When access to the ESC is interrupted, the F2SC shall locally provide the following voice services:

a. Basic intra-base calling capability (ROUTINE service only) with TLS (or equivalent) for signaling and SRTP for bearer.

b. PSTN and 911 access via local MG (sized per customer requirements).

c. Support for both PEIs and AEIs.

NOTE: An F2SC is not intended to provide the full suite of capablilities required of an SC.

SCM-005550 [**Required**] The F2SC shall provide local registrar functionality to EIs and MGs during the period of the ESC outage.

SCM-005560 [**Required**] The F2SC shall provide MGC functionality to local MGs during the period of the ESC outage.

2.12.3.3.3 ESC Cluster Configuration

An ESC may consist of a grouping of server pairs that are collectively referred to as an ESC cluster. In an ESC cluster configuration, individual server pairs are referred to as cluster members. Cluster members within the ESC cluster configuration may be distributed across the ESA. For example, a cluster member may reside locally within an Environment 1 or 2 location. During normal operations, end users within an Environment 1 or 2 location may draw services directly from the local cluster member.

SCM-005570 [**Required**]In the event that Environment 1 location loses access to the WAN, the local cluster member shall provide all the capabilities of a F1SC.

SCM-005580 [**Required**]In the event that Environment 2 location loses access to the WAN, the local cluster member shall provide all the capabilities of an F2SC.

SCM-005590 [**Required**] As described above, individual cluster members consist of a pair of servers that shall operate in either an active/standby or active/active configuration.

SCM-005600 [**Required**]The ESC Core infrastructure shall include a "tertiary cluster member" that shall provide the capacity to handle a single instance where both the active and standby or active/active components of a cluster member have "failed" and the associated enclave still has WAN access to the ESC Core. In the event that both the active and standby or active/active components of a cluster member have "failed," the EIs and MGs served by the failed cluster member, shall failover to the "tertiary cluster member at the ESC Core.

2.12.4 Session Border Controller (SBC)

2.12.4.1 General SBC Functionality

SCM-005610 [**Required**] SBCs deployed within the Enterprise UC Services architecture shall support SBC functionality defined in this section (subject to the modifications and additions set forth in this subsection).

2.12.4.2 Enclave-Fronting SBC Functionality

SCM-005620 [**Required**] The enclave-fronting SBC shall be able to differentiate an intra-enclave VVoIP sessions from an inter-enclave VVoIP sessions. For inter-enclave VVoIP sessions routed through the enclave-fronting SBC, the enclave-fronting SBC shall perform the bidirectional anchoring of the associated media as defined in this section. For all intra-enclave

VVoIP sessions, the enclave-fronting SBC shall not perform the bidirectional anchoring of the associated media.

NOTE: Enclave-fronting SBCs may be deployed locally within the enclave or they may be deployed "centrally" within the DISN. In the "centralized" deployment, a single server platform will typically support multiple, segmented SBC instances where each SBC instance serves a particular enclave within the ESA. A centralized enclave-fronting SBC that serves multiple enclaves is a cost effective alternative to an SBC deployed at each site (subject to FSO/DAA approval).

SCM-005630 [**Required**] The ESC APL SUT shall offer Enclave-Fronting SBC solutions that meet High Available SBC or Medium Available SBC requirements as defined in this section.

SCM-005640 [**Required**] The Enclave-Fronting SBC solution deployed at an Environment 1 location shall meet High Available SBC requirements defined in this section.

SCM-005650 [**Optional**] The Enclave-Fronting SBC solution deployed at an Environment 2 or 3 location may comply with Medium Available SBC requirements as defined in this section.

2.12.4.2.1 Enclave-Fronting SBC Support of AEIs Served by a Centralized ESC

SCM-005660 [**Required**] To enable full topology hiding [Network Address Translation (NAT)] of signaling and bearer traffic, the enclave-fronting SBC shall function as the outbound and inbound signaling proxy for all AS-SIP signaling traffic exchanged between AEIs and the centralized ESC.

SCM-005670 [**Required**] For the routing of AS-SIP signaling traffic exchanged between AEIs and the centralized ESC, the enclave-fronting SBC shall be capable of maintaining a persistent TLS connection with every served AEI within the enclave and the ESC-fronting SBC.

NOTE: In an ESC Cluster configuration, the ESC cluster member may reside within the local enclave (e.g., in the case of an Environment 1 or 2 site). In this particular use case, the served AEIs within the enclave will maintain a persistent TLS connection with the local cluster member.

SCM-005680 [**Required**] The enclave-fronting SBC shall function as a registration proxy for all AEIs located within the associated enclave:

a. When a served AEI sends an AS-SIP REGISTER request to the enclave-fronting SBC, the enclave-fronting SBC shall replace the IP address and port value contained in the Contact header of the REGISTER message (i.e., the inside-address/port) with an IP address and port value associated with a WAN-facing interface on the enclave-fronting SBC (i.e., the outside-address/port).

   NOTE: In an ESC Cluster configuration, the ESC cluster member may reside within the local enclave (e.g., in the case of an Environment 1 or 2 site). In this particular

use case, the served AEIs within the enclave will send their AS-SIP REGISTER request to the local cluster member.

b. For the life of the registration, the enclave-fronting SBC shall maintain a binding between the inside-address/port and outside-address/port.

c. When the enclave-fronting SBC receives an inbound SIP request/response where the embedded address (e.g., in the Request URI or Via header) matches a particular outside-address/port, the enclave-fronting SBC shall replace the outside-address/port value with the original inside-address/port value and shall forward the request to the associated AEI.

2.12.4.2.2 Enclave-fronting SBC Support of PEIs

SCM-005690 [**Conditional**] If served PEIs are relying upon the enclave-fronting SBC to facilitate the traversal of the enclave IA accreditation boundary, the enclave-fronting SBC shall function as a VVoIP aware firewall for vendor-proprietary signaling exchanged between PEIs and the centralized ESC. The enclave-fronting SBC shall maintain a secure, persistent connection (TLS or equivalent) with each served PEI within the enclave and with the ESC-fronting SBC within the ESC Core Infrastructure.

NOTE: In an ESC Cluster configuration, the ESC cluster member may reside within the local enclave (e.g., in the case of an Environment 1 or 2 site). In this particular use case, the PEIs within the local enclave will maintain a secure, persistent connection (TLS or equivalent) with the local cluster member.

SCM-005700 [**Conditional**] If served PEIs are relying upon the enclave-fronting SBC to facilitate the traversal of the enclave IA accreditation boundary, the enclave-fronting SBC shall function as a Application-Layer Gateway (ALG) capable of performing the bidirectional mapping of embedded inside-addresses/port values (within the signaling stream) to an outside-address/port value associated with a WAN-facing interface on the enclave-fronting SBC.

NOTE: The requirements above are not intended to exclude the alternative of PEIs being served by the centralized ESC which do NOT rely upon the enclave-fronting SBC to facilitate the traversal of the enclave IA accreditation boundary.

NOTE: The preceding requirements are not intended to exclude the implementation of a distributed ESC Cluster where individual ESC cluster members may reside within the local enclave (e.g., in the case of an Environment 1 or 2 site).

2.12.4.3 ESC-fronting SBC within the ESC Core Infrastructure

SCM-005710 [**Required**] For the routing of AS-SIP signaling exchanged between AEIs and the centralized ESC, the ESC-fronting SBC shall maintain a persistent TLS connection with the ESC and with the enclave-fronting SBC at each AEI-hosting enclave within the ESA.

SCM-005720 [**Conditional**] If served PEIs are relying upon the ESC-fronting SBC to facilitate the traversal of the ESC Core IA accreditation boundary, the ESC-fronting SBC shall maintain a secure, persistent connection (TLS or equivalent) with the centralized ESC and the enclave-fronting SBC at each PEI-hosting enclave within the ESA.

SCM-005730 [**Required**] The ESC-fronting SBC shall perform media anchoring on media streams to or from Enterprise media resources which are co-located with the ESC (e.g., an Enterprise conference bridge or an announcement server).

SCM-005740 [**Required**] With the exception of media streams to or from media resources co-located with the ESC (e.g., an Enterprise conference bridge or an announcement server), the ESC-fronting SBC shall NOT conduct media anchoring.

SCM-005750 [**Required**] The ESC-fronting SBC shall be a High Available SBC as defined in this section.

NOTE: The preceding requirements are not intended to exclude the implementation of an ESC Cluster where individual ESC cluster members may reside within the local enclave (e.g., in the case of an Environment 1 or 2 site).

2.13 NETWORK-LEVEL SOFTSWITCH

SSNetwork-level SSs are backbone devices that provide long-haul signaling between local service enclaves and act as an AS-SIP B2BUA within the UC framework. It provides the equivalent functionality of a commercial SS.

Support for the functionality of an internal SC is optional.

SCM-005760 [**Required: SS**] The SS product shall provide the following functional components, IAW the applicable requirements in the sections referenced:

SCM-005760.a [**Required**] Section 2.13.1, Softswitch Location Server.

SCM-005760.b [**Optional**] Section 2.10, Session Controller.

SCM-005760.c [**Required**] Section 2.14, Call Connection Agent, including the CCA-associated IWF that applies to both the SS and the [**Optional**] SC functionality, if deployed.

SCM-005760.d [**Required**] Section 2.15.10, CCA Interactions With Service Control Functions, that addresses media servers.

SCM-005760.e [**Required**] Section 2.3.2, ASAC Requirements for the SS Related to Voice, and Section 2.3.3, ASAC Requirements for the SC and the SS Related to Video Services. These sections address WAN-level ASAC policing requirements.

SCM-005760.f [**Required**] Section 2.25.1, Multilevel Precedence and Preemption, as appropriate for VoIP and Video over IP services.

SCM-005760.g [**Required**] Section 2.2.8, Calling Number Delivery

SCM-005760.h [**Required**] Section 2.16, Media Gateway, including MG and MGC requirements as well as ISDN T1.619a PRI and commercial PRI trunking interfaces. The MGC may connect via the DISN WAN to remotely located MGs.

SCM-005760.i [**Required**] Section 2.19, Management of Network Appliances.

SCM-005760.j [**Required**] Section 2.10.6, SC Transport Interface Functions, that addresses the IP Transport Interface functions.

SCM-005760.k [**Required**] Section 2.8.2, Product Quality Factors.

SCM-005760.l [**Required**] AS-SIP 2013.

SCM-005760.m [**Required**] Section 4, Information Assurance, for SS, MG, and [**Optional**] SC.

SCM-005760.n [**Optional**] The MG of the SS shall support an OC-3 physical interface for transport of multiplexed PRI trunk groups between 1) the SS and MFSs in the DISA TDM network, and 2) the SS and EOs in the commercial TDM network (in the case where the SS contains an SC, and the SC end users need access to the commercial TDM network). The OC-3 physical interface shall support multiplexing of both T1-based T1.619A PRI trunk groups and T1-based commercial PRI trunk groups (e.g., NI-2 PRI trunk groups in the United States). The OC-3 multiplexing of E1-based Q.955.3 PRI trunk groups and E1-based commercial PRI trunk groups (e.g., ETSI PRI Trunk Groups in Europe) is not required.

NOTE:

- The SS MG is required to support only ISDN T1.619A PRI trunks to a Multifunction Switch (MFS). If the optional SC is supported, the SS MG also needs to support commercial PRI trunks to the local PSTN (or to an adjacent MFS that has its own commercial PRI trunks to the local PSTN).
- The SS MG(s) may be remotely located from the MGC within the CCA of the SS.
- The SS does not need to implement an ASLAN; it can use a proprietary switched Ethernet LAN for interconnecting its components within itself, and to the CE-R via an SBC.

NOTE: The only connections required between the SS MG and the MFS are ISDN T1.619A PRI and commercial PRI, IAW ANSI Standards T1.619-1992 and T1.619a-1994, plus the U.S. National ISDN documents, which include the

NFAS feature. Support for the NFAS feature of the ANSI Standards is an Optional requirement for PRIs.

2.13.1 Softswitch Location Server

The Softswitch Location Service (SSLS) provides global location services and supports call routing where the called address points to a global destination (i.e., outside the SS) rather than a local destination (i.e., within the SS). A called address is contained within a SIP URI in the form of a called number. Section 2.15.7, CCA Interactions With Softswitch Location Service, describes how the CCA uses routing information stored in the SSLS to route calls between SS EIs and the following:

- SCs served by the SS.
- Other SSs.
- DoD TDM networks.
- Allied TDM networks.
- Coalition TDM networks.
- PSTN (CONUS and Global).

However, when an optional, internal SC is deployed with the SS, the SS uses the routing information stored in its SCLS to do the following:

- Route internal calls from one SS PEI or AEI to another.
- Route incoming calls to local SS PEIs or AEIs from the following:
  - An SC.
  - Another SS.
  - A DoD TDM network.
  - An allied or coalition TDM network.
  - The PSTN (CONUS and Global).

2.13.2 SS Signaling Interfaces

SCM-005770 [**Required: SS**] The SS shall support AS-SIP signaling for IP communication with other SSs and SCs.

SCM-005780 [**Required: SS**] The SS shall support PRI signaling for TDM communication with other systems.

SCM-005790 [**Optional: SS MG**] The SS MG shall support CAS signaling as required by local implementations.

2.13.3 Network Management System Interface

SCM-005800 [**Required: SS**] The SS-to-EMS interface shall be an Ethernet connection as specified in Section 2.7.4, DISA VVoIP EMS Interface.

2.14 CALL CONNECTION AGENT

2.14.1 Introduction

This section provides GRs for the CCA function in the SC and SS.

Both of these appliances have a DISN-defined design that includes Session Control and Signaling functions. These functions include both a Signaling Protocol IWF and an MGC function.

The CCA described in the following requirements is part of the SCS functions, and includes both the IWF and the MGC.

SCM-005810 [**Required: SC, SS**] A CCA in an SS or SC shall be able to support multiple MGs on a single ASLAN.

SCM-005820 [**Required: SC, SS**] A CCA in an SS or SC shall be able to support multiple MGs on multiple ASLANs, where those ASLANs are interconnected to form a Metropolitan Area Network (MAN) or Community of Interest Network (COIN). In this arrangement, it is expected that the set of ASLANs forming the MAN or COIN will meet the single-ASLAN performance requirements in Section 7, Network Edge Infrastructure. In this case, the SC shall support sessions between an MG on one ASLAN and a PEI, AEI, MG, or SBC on another ASLAN, as long as both ASLANs are part of the same MAN or COIN.

SCM-005830 [**Required: SC, SS**] A CCA in an SS or SC shall be able to support MGs at multiple physical locations. In some deployments, an SC in one location will serve ASLANs and EIs at distant locations, where both locations are part of the same regional MAN or COIN. In these cases, each distant ASLAN may want to have its own gateway to the local PSTN. In these cases, the SC shall support MGs at multiple locations over MAN or COIN infrastructures that meet the ASLAN performance requirements in the UCR.

2.14.2 Functional

2.14.2.1 CCA IWF Component

The IWF within the CCA does the following:

- Supports all the VoIP and TDM signaling protocols that the SC supports for EIs, MGs, and SBCs, and
- Interworks all these various signaling protocols with one another.

SCM-005840 [**Required: SC, SS**] The CCA IWF shall support the following VoIP and TDM signaling protocols:

SCM-005840.a [**Required: SC,SS**] AS-SIP.

SCM-005840.b [**Optional: SC**] Proprietary VoIP for PEIs on the EI-SC interface. Proprietary VoIP protocols include vendor-specific SIP, vendor-specific H.323, and other vendor-proprietary protocols).

SCM-005840.c [**Required: SC,SS**] North American ISDN PRI, including MLPP.

SCM-005840.d [**Optional: SC, SS**] European or other foreign ISDN PRI, including MLPP.

SCM-005840.e [**Required: SC,SS**] Facility Associated Signaling (FAS) shall be supported for T1.619A and commercial PSTN PRIs.

SCM-005840.f [**Optional: SC, SS**] Non-Facility Associated Signaling (NFAS) shall be supported for T1.619A and commercial PSTN PRIs.

SCM-005840.g [**Optional: SC, SS**] CAS, including MLPP.

2.14.2.2 CCA MGC Component

SCM-005850 [**Required: SC, SS**] The CCA MGC component shall support the following trunks:

SCM-005850.a [**Required: SC, SS**] Support for DoD ISDN trunks.

SCM-005850.b [**Optional: SC, SS**] Support for CAS trunks.

The MGC within the CCA does the following:

- Controls all MGs within the SC or SS.
- Controls all trunks (e.g., PRI, CAS) within each MG.
- Controls all signaling and media streams on each trunk within each MG.
- Accepts IP-encapsulated signaling streams from an MG, and return IP-encapsulated signaling streams to the MG accordingly.
- Within the SC, uses either ITU-T Recommendation H.248 or a vendor-proprietary protocol to accomplish these controls.

The MGC and the MG that it controls are considered Optional – Deployable for the SC.

2.14.3 Role of the CCA in Network Appliances

The role of the CCA is to provide session control for all VoIP sessions and Video over IP sessions that are originated by or terminated by EIs on the SC. These VoIP and Video sessions can be established using either AS-SIP or a proprietary VoIP protocol.

The CCA takes on the role of a SIP B2BUA in the traditional SIP architecture.

The CCA takes on the role of a SIP Registrar for all EIs, MGs, and SBCs served by the SC, allowing EIs, MGs, and SBCs to register their SIP URIs (i.e., Addresses of Record) and current IP addresses with the CCA. The CCA is responsible for maintaining a SIP URI-to-IP-address "binding" for each PEI, AEI, MG, and SBC that is active on the SC at any time.

The CCA is responsible for providing call control and feature control for all VoIP and Video–over-IP calls and features that the SC provides. All VoIP and Video-over-IP calls that are originated by or answered by SC PEI and AEI end users are controlled by the CCA. All VoIP and Video-over-IP features that are provided to SC PEI and AEI end users, on either a per-call basis, a per-feature-request basis, or an all-calls basis, are controlled by the CCA.

In the current DISN design for an SC, the CCA includes an IWF and an MGC, and the MGC controls all the TDM interfaces served by the MG (ISDN PRI trunks, and CAS trunks). This section reviews the role of the CCA in the SC and SS reference models, and covers the role of the CCA, IWF, and MGC in each case.

2.14.4 CCA-IWF Signaling Protocol Support

This section describes the requirements for the CCA Signaling Protocol IWF to support the various VoIP and TDM signaling protocols used in the SC and SS. In summary, the role of the IWF within the CCA is to support all the VoIP and TDM signaling protocols that are used by the EIs, MGs, and SBCs, and interwork all these various signaling protocols with one another.

2.14.4.1 CCA-IWF Support for AS-SIP

SCM-005860 [**Required: SC, SS**] The CCA IWF shall support the AS-SIP protocol consistent with the detailed AS-SIP protocol requirements in AS-SIP 2013.

SCM-005870 [**Required: SC, SS**] The CCA IWF shall use the AS-SIP protocol on SC-SS and SS-SS sessions.

SCM-005880 [**Required: SC, SS**] When the CCA IWF uses the AS-SIP protocol over the Access Segment between the SBC and the DISN WAN, or over the DISN WAN itself, the CCA IWF shall secure the AS-SIP protocol using TLS, as described in Section 4, Information Assurance.

2.14.4.2 CCA-IWF Support for PRI, via MG

SCM-005890 [**Required: SC, SS**] The CCA IWF shall support the U.S./National ISDN version of the ISDN PRI protocol, consistent with the detailed ISDN PRI protocol requirements in the following DoD and ANSI documents:

a. Section 2.25.3, ISDN, including Table 2.25-12, PRI Access, Call Control, and Signaling, and Table 2.25-13, PRI Features.

   (1) The "MFS" column in these tables shall apply to the SS.

   (2) The "PBX1" and "PBX2" columns in these tables shall apply to the SC.

b. Section 2.25.1, Multilevel Precedence and Preemption, including:

   (1) Section 2.25.2.3, Line Signaling.

   (2) Section 2.25.1.7, ISDN MLPP PRI.

c. ANSI T1.619-1992 (R2005).

d. ANSI T1.619a-1994 (R1999).

   (1) Facility Associated Signaling is required for T1.619A PRIs, and NFAS is optional for T1.619A PRIs.

   (2) Facility Associated Signaling is required for commercial PSTN PRIs, and NFAS is optional for commercial PSTN PRIs, for access to the U.S. PSTN.

SCM-005900 [**ETSI PRI: Required – Other Foreign PRIs: Optional**] The appliance supplier (i.e., SC or SS supplier) has the option of supporting one or more foreign versions of the ISDN PRI protocol on its product. As used here, the term "Foreign version of ISDN PRI protocol" means the version of the PRI protocol that is used in the PSTN of a foreign country.

If an appliance supplier supports a foreign version of the ISDN PRI protocol on its product, the CCA IWF in that product shall support that foreign version of the ISDN PRI protocol consistent with the PRI protocol standards that are used in the PSTN of that foreign country.

Examples of these standards follow:

- ETSI standards on the use of ISDN PRI in European countries (and other countries that also support ETSI PRI standards).
- Japanese Telecommunication Technology Committee (TTC) and South Korean Telecommunication Technology Association (TTA) standards on the use of ISDN PRI in Japan and South Korea, respectively.
- ITU-T standards on the use of ISDN PRI worldwide (in countries that support only ITU-T standards).

NOTE: The ISDN-PRI/AS-SIP interworking requirements in this document apply only to the U.S. version of ISDN PRI. The ISDN-PRI/AS-SIP interworking requirements

for foreign versions of ISDN PRI (e.g., European, Japanese, South Korean) are outside the scope of this document.

NOTE: Support for ETSI PRI is required when the SC or SS is used in the European Theater or in other OCONUS ETSI-compliant countries.

SCM-005910 [**ETSI PRI: Required**] When used in the European Theater and in other OCONUS ETSI-compliant countries, the CCA IWF shall support the ITU-T Recommendation Q.955.3 MLPP extensions to the ITU-T ISDN PRI protocol, consistent with the UCR and ITU-T Recommendation Q.955.3.

SCM-005920 [**Required: SC, SS**] The CCA IWF shall support reception of ISDN PRI messages from the MG and transmission of ISDN PRI messages to the MG.

SCM-005930 [**Required: SC, SS**] The CCA IWF shall be able to determine the ISDN PRI (and its D-Channel signaling link) that an incoming PRI message was received on, when processing an incoming PRI message from the MG.

SCM-005940 [**Required: SC, SS**] The CCA IWF shall be able to identify the ISDN PRI (and its D Channel signaling link) that an outgoing PRI message will be sent on, when generating an outgoing PRI message to the MG.

SCM-005950 [**Required: SC, SS**] The CCA IWF shall be able to support multiple ISDN PRIs (and their D Channel signaling links) at the MG, where each PRI is connected to a different PRI end point (e.g., to a different DoD PBX, DoD TDM switch, SS, SC, PSTN PBX, or PSTN TDM switch).

SCM-005960 [**Required: SC, SS**] The CCA IWF shall be able to differentiate between the individual ISDN PRIs (and their D-Channel signaling links) at the MG. The CCA IWF shall know, as part of its configuration data, which DoD PBX, DoD TDM switch, SS, SC, PSTN PBX, or PSTN TDM switch each ISDN PRI (and its D-Channel signaling link) is connected to.

SCM-005970 [**Required: SC, SS**] In conjunction with the MG, the CCA IWF shall support ISDN PRIs (and D-Channel signaling links) to the following:

a. TDM PBXs and switches in the DoD network (This includes the TDM EO and Tandem components of the local SS, in the SS CCA/MG case).

b. SSs and SCs in the DoD network.

c. TDM PBXs and switches in the U.S. PSTN.

d. TDM PBXs and switches in allied and coalition partner networks (when those networks support U.S. “National ISDN” PRI).

SCM-005980 [**Required: SC, SS**] The CCA IWF shall support the full set of ISDN MLPP requirements in ANSI T1.619 and ANSI T1.619a, including the following from ANSI T1.619:

a. Precedence level.

b. Cause.

c. Notification Indicator.

d. Signal.

e. Call Identity.

f. Information elements in ISDN PRI messages, on ISDN PRIs to do the following:

(1) TDM PBXs in the DoD TDM network.

(2) TDM switches in the DoD TDM network.

(3) SSs in the DoD network.

(4) SCs in the DoD network.

SCM-005990 [**Required: SC, SS**] The CCA IWF shall not support any of the ISDN MLPP requirements in ANSI T1.619 and ANSI T1.619a, on ISDN PRIs to TDM PBXs and switches in the U.S. PSTN.

In other words, the MLPP feature and its associated ISDN PRI signaling shall be supported on ISDN PRIs from the CCA/MG to PBXs and switches in the DoD TDM network (or to appliances in the network), but shall not be supported on ISDN PRIs from the CCA/MG to PBXs and switches in the U.S. PSTN.

SCM-006000 [**Required: SC, SS**] On ISDN PRIs from the CCA/MG to TDM PBXs and switches in allied and coalition partners (where those networks support U.S. "National ISDN" PRI), the CCA IWF shall support a DoD-user-configurable per-PRI option that allows the PRI to support or not support the ANSI T1.619/619a PRI MLPP feature on calls to and from that PRI.

SCM-006010 [**ETSI PRI: Required – Other Foreign PRIs: Optional**] When the appliance supplier supports a foreign ISDN PRI on its product, consistent with the PRI protocol standards used in the PSTN of that foreign country, the CCA IWF (along with the MG) shall support ISDN PRIs and D Channel signaling links to the following:

a. TDM PBXs and switches in the PSTN in that foreign country.

b. TDM PBXs and switches in allied and coalition partner networks (where those networks support the ISDN PRI used in the home country of the allied or coalition partner).

Support for ETSI PRI is required when the SC or SS is used in the European Theater or in other OCONUS ETSI-compliant countries.

SCM-006020 [**Required: SC, SS**] The CCA IWF shall be able to associate individual PRI configuration data with each individual PRI served by the MG and the CCA. The CCA IWF shall not require groups of PRIs served by the MG and the CCA to share "common" PRI configuration data.

2.14.4.3 CCA-IWF Support for CAS Trunks, via MG

SCM-006030 [**Optional**] The CCA IWF (with the MG) shall support the U.S. version of CAS trunks and trunk signaling, consistent with the CAS trunk and trunk signaling requirements in the following sections:

a. Section 2.25.2, Signaling, including the following:

   (1) Section 2.25.2.4, Trunk Supervisory Signaling.

   (2) Section 2.25.2.5, Control Signaling.

   (3) Section 2.25.2.6, Alerting Signals and Tones.

b. Section 2.25.1, Multilevel Precedence and Preemption, including:

   (1) Section 2.25.1.4.1, Channel-Associated Signaling.

SCM-006040 [**Optional**] The appliance supplier (i.e., SC or SS supplier) has the option of supporting one or more foreign versions of CAS trunks and trunk signaling on its product. As used here, the term "foreign version of CAS trunks and trunk signaling," means the version of CAS trunks and trunk signaling used in the PSTN of a foreign country.

If an appliance supplier supports a foreign version of CAS trunks and trunk signaling on its product, the CCA IWF shall support the version of CAS trunks and trunk signaling used in the PSTN of a foreign country, consistent with the CAS trunk standards used in the PSTN of that foreign country. Examples of these standards include the following:

a. ETSI standards on the use of CAS trunks in European countries (and other countries that also support ETSI CAS trunk standards).

b. Japanese TTC and South Korean TTA standards on the use of CAS trunks in Japan and South Korea, respectively.

c. ITU-T standards on the use of CAS trunks worldwide (in countries that support only ITU-T standards).

NOTE: The CAS trunk/AS-SIP interworking requirements in this document apply only to the U.S. version of CAS trunks. The CAS trunk/AS-SIP interworking requirements for foreign versions of CAS trunks (i.e., European, Japanese, South Korean) are outside the scope of this document.

SCM-006050 [**Conditional**] If CAS trunks and trunk signaling are supported, the CCA IWF shall support reception of CAS signaling sequences (i.e., Supervisory, Control, and Alerting) from the MG, and transmission of CAS signaling sequences to the MG.

SCM-006060 [**Conditional**] If CAS trunks and trunk signaling are supported, the CCA IWF shall be able to determine the MG CAS trunk and CAS trunk group that an incoming CAS signaling sequence was received on when processing an incoming CAS signaling sequence from the MG.

SCM-006070 [**Conditional**] If CAS trunks and trunk signaling are supported, the CCA IWF shall be able to identify the MG CAS trunk and CAS trunk group that an outgoing CAS signaling sequence will be sent on when generating an outgoing CAS signaling sequence to the MG.

SCM-006080 [**Conditional**] If CAS trunks and trunk signaling are supported, the CCA IWF shall be able to support multiple CAS trunk groups at the MG, where each CAS trunk group is connected to a different end point (e.g., to a different DoD PBX, DoD TDM switch, SS, SC, PSTN PBX, or PSTN TDM switch).

SCM-006090 [**Conditional**] If CAS trunks and trunk signaling are supported, the CCA IWF shall be able to differentiate between the individual CAS trunk groups at the MG. The CCA IWF shall know, as part of its configuration data, which DoD PBX, DoD TDM switch, SS, SC, PSTN PBX, or PSTN TDM switch each CAS trunk group is connected to.

SCM-006100 [**Conditional**] If CAS trunks and trunk signaling are supported, the CCA IWF shall. in conjunction with the MG, support CAS trunk groups to the following:

a. TDM PBXs and switches in the DoD TDM network.
b. SSs and SCs in the DISN.
c. TDM PBXs and switches in the U.S. PSTN.
d. TDM PBXs and switches in allied and coalition networks (where those networks support U.S. CAS trunk groups).

SCM-006110 [**Conditional**] If CAS trunks and trunk signaling are supported, the CCA IWF shall support the MLPP signaling requirements for CAS trunk groups in Section 2.25.1.4.1, Channel-Associated Signaling. This MLPP signaling support shall include the following four cases:

a. Answered call, Trunk to be reused.
b. Unanswered call, Trunk to be reused.
c. Answered call, Trunk not to be reused.
d. Unanswered call, Trunk not to be reused.

SCM-006120 [**Conditional**] If CAS trunks and trunk signaling are supported, when the IWF is the appliance sending the preemption request over the CAS trunk group, the CCA IWF shall generate the measured supervisory signal (preemption signal) causing trunk circuit disconnect, with the following four variations:

a. Answered call, Trunk to be reused.
b. Unanswered call, Trunk to be reused.
c. Answered call, Trunk not to be reused.
d. Unanswered call, Trunk not to be reused.

SCM-006130 [**Conditional**] If CAS trunks and trunk signaling are supported, when the IWF is the appliance receiving the preemption signal over the CAS trunk group, the CCA IWF shall be able to receive and act on the measured supervisory signal (preemption signal) causing trunk circuit disconnect, with the following four variations:

a. Answered call, Trunk to be reused.

b. Unanswered call, Trunk to be reused.

c. Answered call, Trunk not to be reused.

d. Unanswered call, Trunk not to be reused.

SCM-006140 [**Conditional**] If CAS trunks and trunk signaling are supported, when the IWF is the appliance receiving the preemption request over the CAS trunk group, the CCA IWF shall generate the Preempt warning tone to the CCA-served party on the preempted call (e.g., a VoIP EI served by the CCA that is active on the preempted call).

SCM-006150 [**Conditional**] If CAS trunks and trunk signaling are supported, when the IWF is the appliance receiving the preemption request over the CAS trunk group, the CCA IWF shall detect the Returned disconnect signal from the CCA-served party on the preempted call, and remove the Preempt warning tone from the party after this detection.

SCM-006160 [**Conditional**] If CAS trunks and trunk signaling are supported, the CCA IWF shall support the CAS MLPP signaling as described earlier on CAS trunk groups to:

a. TDM PBXs and switches in the DoD TDM network (This includes the TDM EO and Tandem components of the local SS, in the SS CCA/MG case).

b. SSs and SCs in the DISN.

SCM-006170 [**Conditional**] If CAS trunks and trunk signaling are supported, the CCA IWF shall not use the CAS MLPP signaling described earlier on CAS trunk groups to TDM PBXs and switches in the U.S. PSTN.

In other words, the MLPP feature and its associated CAS signaling shall be supported on CAS trunk groups from the CCA/MG to PBXs and switches in the DoD TDM network (or to appliances in the network), but shall not be supported on CAS trunk groups from the CCA/MG to PBXs and switches in the U.S. PSTN.

SCM-006180 [**Conditional**] If CAS trunks and trunk signaling are supported, the CCA IWF shall support a DoD-user-configurable per-CAS trunk group option on CAS trunk groups from the CCA/MG to TDM PBXs, and in allied and coalition partners (where those networks support U.S. CAS trunks), that allows the CAS trunk group to either:

a. Support the CAS MLPP feature on calls to and from that trunk group, or

b. Not support the CAS MLPP feature on calls to and from that trunk group.

When the "Support" option is configured, the CCA IWF shall support the CAS MLPP feature for allied and coalition partner calls on that trunk group.

When the "Not Support" option is configured, the CCA IWF shall not support the CAS MLPP feature for allied and coalition partner calls on that trunk group.

SCM-006190 [**Conditional**] If CAS trunks and trunk signaling are supported, when the appliance supplier supports foreign CAS trunk groups on its product, the CCA IWF, along with the MG, shall support CAS trunk groups to the following:

a. TDM PBXs and switches in the PSTN in a foreign country.

b. TDM PBXs and switches in allied and coalition partner networks (where those networks support the CAS trunk groups used in the home country of the allied or coalition partner).

SCM-006200 [**Conditional**] If CAS trunks and trunk signaling are supported, the CCA IWF shall be able to associate individual CAS trunk group configuration data with each individual CAS trunk group served by the MG and the CCA. The CCA IWF shall not require groups of CAS trunk groups served by the MG and the CCA to share "common" CAS trunk group configuration data.

SCM-006210 [**Conditional**] If CAS trunks and trunk signaling are supported, the CCA IWF shall know the identity of the CAS device at the far end of each CAS trunk group, as part of CAS trunk group configuration data. Specifically, the CCA IWF shall know the following:

a. The identity of each interconnected TDM PBX and switch in the TDM portion of the network (This includes the TDM EO and Tandem components of the local SS, in the SS CCA/MG case.)

b. The identity of each interconnected SS and SC in the DISN.

c. The identity of each interconnected TDM PBX and switch in the U.S. PSTN.

d. The identity of each interconnected TDM PBX and switch in each allied and coalition partner network (when that network supports U.S. CAS trunk groups).

SCM-006220 [**Conditional**] If CAS trunks and trunk signaling are supported,when the appliance supplier supports foreign CAS trunk groups on its product, the CCA IWF shall know, as part of CAS trunk group configuration data, the identity of the foreign CAS device at the far end of each foreign CAS trunk group. Specifically, the CCA IWF shall know:

a. The identity of each interconnected TDM PBX and switch in the foreign PSTN.

b. The identity of each interconnected TDM switch in the foreign PSTN.

c. The identity of each interconnected TDM PBX and switch in each allied and coalition partner network (when that network supports the foreign CAS trunk group of the allied or coalition partner's home country).

NOTE: These "foreign" CAS trunk group requirements are included to support DoD users in interconnecting their SSs and SCs with the networks of foreign PSTNs, U.S. Allies, and U.S. Coalition Partners using CAS trunk groups. Detailed requirements for support of foreign CAS trunk groups are outside the scope of this document.

2.14.4.4 CCA-IWF Support for PEI and AEI Signaling Protocols

SCM-006230 [**Required: SC, SS**] The CCA IWF shall support vendor-proprietary Voice and Video EIs and their associated proprietary EI signaling protocols. Proprietary EI signaling protocols include a vendor's version of SIP or H.323.

SCM-006240 [**Required**] The CCA IWF shall support the following Voice and Video EIs, and their associated EI signaling protocols:

SCM-006240.a [**Optional**] Voice and Video SIP EIs.

SCM-006240.b [**Optional**] Voice and Video H.323 EIs.

SCM-006240.c [**Required**] Voice and Video AS-SIP EIs.

SCM-006250 [**Conditional**] If the CCA IWF supports Voice and Video SIP EIs, the IWF shall support these EIs using the set of IETF SIP and SDP RFCs listed in AS-SIP 2013.

SCM-006260 [**Conditional**] If the CCA IWF supports Voice and Video H.323 EIs, the IWF shall support these EIs using ITU-T Recommendation H.323.

NOTE: An SC or SS ASLAN may support two different types of Voice and Video H.323 EIs:

a. H.323 EIs that are served by an H.323 Gatekeeper that is completely separate from the CCA and its IWF.
b. H.323 EIs that are served by the CCA and its IWF (where the CCA IWF is, effectively, an H.323 Gatekeeper for these EIs).

In the first case, the H.323 EIs are completely independent of the CCA, MG, and SBC. This arrangement is considered an "H.323 Overlay Network" and is outside the scope of this document.

In the second case, the H.323 EIs are dependent on the CCA, MG, and SBC for interworking with TDM voice networks, for interworking with AS-SIP, and for gaining access to the DISN WAN. When an H.323 EI on the local ASLAN makes an H.323 Voice or Video call to another H.323 EI on a remote ASLAN in this case, the "originating SC" does H.323/AS-SIP protocol conversion, the terminating SC does AS-SIP/H.323 protocol conversion, and the call is treated as an AS-SIP session (with resulting Voice or Video budget impacts) between the calling SC, the called SC, and any intermediate SSs.

This second case, while unusual, is an "H.323/AS-SIP Interworking" case, and is within the scope of this document. The details on how the CCA and IWF perform the protocol interworking between EI H.323 and CCAN AS-SIP are left to the vendor's discretion.

SCM-006270 [**Required**] When the CCA IWF supports Voice and Video AS-SIP EIs, the IWF shall support these EIs using the set of AS-SIP protocol requirements in AS-SIP 2013.

2.14.4.5 CCA-IWF Support for VoIP and TDM Protocol Interworking

Per Section 2.14.2.1, CCA IWF Component, the role of the IWF within the CCA is to support all the VoIP and TDM signaling protocols that the appliance supports for PEIs, AEIs, MGs, and SBCs, and interwork all these various signaling protocols with one another.

The requirements in this section support the IWF's interworking of the various VoIP and TDM signaling protocols together. Table 2.14-1, Full IWF Interworking Capabilities for VoIP and TDM Protocols, summarizes the various interworking capabilities that the appliance is required to support.

Table 2.14-1. Full IWF Interworking Capabilities for VoIP and TDM Protocols

IWF INPUT PROTOCOL	IWF OUTPUT PROTOCOL				
	AS-SIP (TO AN AEI)	AS-SIP (TO AN SBC)	PV	ISDN PRI	CAS
AS-SIP (from a AEI)	N/A	Required	Required if PV is supported	Required	Optional
AS-SIP (from an SBC)	Required	N/A	Required if PV is supported	Required	Optional
PV	Required if PV is supported	Required if PV is supported	N/A	Required if PV is supported	Optional
ISDN PRI	Required	Required	Required if PV is supported	N/A	Optional
CAS	Optional	Optional	Optional	Optional	N/A

LEGEND

AEI: AS-SIP End Instrument
AS-SIP: Assured Services Session Initiation Protocol
CAS: Channel-Associated Signaling
ISDN: Integrated Services Digital Network
IWF: Interworking Function
N/A: Not Applicable
PRI: Primary Rate Interface
PV: Proprietary VoIP
SBC: Session Boundary Controller

When they are present in the network appliance, the CCA IWF shall interwork the protocols for the following cases, including support for both Voice and Video AEIs, unless noted otherwise:

SCM-006280 [**Required**] AS-SIP protocol vian AS-SIP AEIs with the vendor's proprietary VoIP EI protocol.

SCM-006290 [**Required**] AS-SIP protocol vian AS-SIP AEIs with the U.S. ISDN PRI protocol.

SCM-006300 [**Required: ETSI PRI – Optional: Other Foreign PRIs**] AS-SIP protocol vian AS-SIP AEIs with the appropriate foreign ISDN PRI protocol.

SCM-006310 [**Optional**] AS-SIP protocol vian AS-SIP AEIs with the U.S. CAS trunk protocol.

SCM-006320 [**Optional**] AS-SIP protocol vian AS-SIP AEIs with the appropriate foreign CAS trunk protocol.

SCM-006330 [**Required**] Proprietary VoIP EI protocol with the U.S. ISDN PRI protocol.

SCM-006340 [**Required: ETSI PRI – Optional: Other Foreign PRI**] Proprietary VoIP EI protocol with the appropriate foreign ISDN PRI protocol.

SCM-006350 [**Optional**] Proprietary VoIP EI protocol with the U.S. CAS trunk protocol.

SCM-006360 [**Optional**] Proprietary VoIP EI protocol with the appropriate foreign CAS trunk protocol.

SCM-006370 [**Required**] AS-SIP protocol via SBCs with the suppliers' Proprietary VoIP EI protocol.

SCM-006380 [**Required**] AS-SIP protocol via SBCs with the U.S. ISDN PRI protocol.

SCM-006390 [**Required: ETSI PRI – Optional: Other Foreign PRI**] AS-SIP protocol via SBCs with the appropriate foreign ISDN PRI protocol.

SCM-006400 [**Optional**] AS-SIP protocol via SBCs with the U.S. CAS trunk protocol.

SCM-006410 [**Optional**] AS-SIP protocol via SBCs with the appropriate foreign CAS trunk protocol.

2.15 CCA INTERACTION WITH NETWORK APPLIANCES AND FUNCTIONS

This section specifies how the CCA interacts with network appliances and appliance functions. These other appliance functions include the following:

- ASAC.
- Service Control functions.
- NM (FCAPS and audit logs).
- Transport Interface functions.
- SBC (not part of the SC, but part of the local Assured Services domain).

2.15.1 CCA Interactions With Transport Interface Functions

The Transport Interface functions in an appliance provide interface and connectivity functions with the ASLAN and its IP packet transport network. High-level requirements for these functions are outlined in this section. The detailed implementation methods for these requirements are left up to each vendor. Examples of Transport Interface functions include the following:

- Network Layer functions: IP and IPSec.
- Transport Layer functions: TCP, UDP, Stream Control Transmission Protocol (SCTP), TLS.
- LAN protocols.

SCM-006420 [**Required**] The CCA shall support assignment of the following items to itself:

a. Only one CCA IP address (this one IP address shall be implemented in the CCA as either a single logical IP address or a single physical IP address).

b. A CCA FQDN that maps to that IP address.

c. A CCA SIP URI that uses that CCA FQDN as its domain name, and maps to the "SIP B2BUA" function within the CCA itself.

SCM-006430 [**Required**] The CCA shall support assignment of the following items to each SIP and AS-SIP PEI and AEI on the Appliance LAN:

a. Only one PEI or AEI IP address.

b. A PEI or AEI FQDN that maps to that IP address.

c. A PEI or AEI SIP URI that uses that PEI or AEI FQDN as its domain name, and maps to the "SIP User Agent" function within the PEI or AEI.

SCM-006440 [**Required**] The CCA shall support assignment of the following items to each MG on the Appliance LAN:

a. Only one MG IP address (this one IP address shall be implemented in the MG as either a single logical IP address or a single physical IP address).

b. An MG FQDN that maps to that IP address.

c. An MG SIP URI that uses that MG FQDN as its domain name, and maps to the "UC Signaling and Media End Point" function within the MG.

SCM-006450 [**Required**] The CCA shall support assignment of the following items to the SBC:

a. Only one SBC IP address (this one IP address shall be implemented in the SBC as either a single logical IP address or a single physical IP address).

b. An SBC FQDN that maps to that IP address.

c. An SBC SIP URI that uses that SBC FQDN as its domain name, and maps to the "SIP B2BUA" function within the SBC.

2.15.2 CCA Interactions With the SBC

High-level CCA requirements for interacting with an SBC are as follows:

SCM-006460 [**Required**] When directing VoIP sessions to other network appliances providing voice and video services across the DISN, the CCA shall direct these VoIP sessions to the SBC, so that the SBC can process them before directing them to the network appliances on the DISN WAN.

SCM-006470 [**Required**] The CCA shall direct VoIP sessions to other network appliances through the SBC in the following cases:

a. When the CCA is part of an SC and is directing VoIP sessions to an SS on the DISN WAN, which is the "primary" or "backup" SS for that SC.

b. When the CCA is part of an SS and is directing VoIP sessions to an SC on the DISN WAN, which is a "subtended" SC for that SS.

c. When the CCA is part of an SS and is directing VoIP sessions to another SS on the DISN WAN.

SCM-006480 [**Required**] When accepting VoIP sessions from other network appliances on the DISN, the CCA shall accept these VoIP sessions from the SBC, because the SBC relays them from the network appliances on the DISN WAN.

SCM-006490 [**Required**] The CCA shall accept VoIP sessions from other network appliances through the SBC in the following cases:

a. When the CCA is part of an SC and is accepting VoIP sessions from an SS on the DISN WAN, which is the "primary" or "backup" SS for that SC.

b. When the CCA is part of an SS and is accepting VoIP sessions from an SC on the DISN WAN, which is a "subtended" SC for that SS.

c. When the CCA is part of an SS and is accepting VoIP sessions from another SS on the DISN WAN.

2.15.3 CCA Support for Admission Control

The CCA interacts with the ASAC component of the SC and SS to perform specific functions related to ASAC, such as counting internal, outgoing, and incoming calls; managing separate call budgets for VoIP and Video over IP calls; and providing preemption.

SCM-006500 [**Required**] The SC and SS CCA shall meet all the requirements in Section 2.3, ASAC.

SCM-006510 [**Required**] The SC and SS CCA shall meet all the requirements in Section 2.25.1, Multilevel Precedence and Preemption.

SCM-006520 [**Required**] The SC and SS CCA shall meet all the requirements in AS-SIP 2013, Section 7, Policing of Call Count Thresholds.

2.15.4 CCA Support for User Features and Services

The User Features and Services (UFS) Server is responsible for providing features and services to VoIP and Video PEIs/AEIs on an SC or SS, where the CCA alone cannot provide the feature or service.

SCM-006530 [**Required**] The CCA within a network appliance shall support the operation of the following features and capabilities, as listed in Table 2.2-1, Assured Services Product Features and Capabilities:

a. The CCA shall generate a redirecting number each time it forwards a VoIP or Video session request as part of a CF feature.

b. The CCA supports the ability to direct VoIP and Video sessions and session requests to the UFS Server, so that the UFS Server can apply an Appliance VoIP or Video feature, when use of that feature is required by the calling party, the called party, or the appliance itself.

The interface and protocols used to interconnect the CCA with the UFS Server are internal to the network appliance and, therefore, are supplier-specific.

2.15.5 CCA Support for Information Assurance

The Information Assurance function within the appliance ensures that end users, PEIs, AEIs, MGs, and SBCs that use the appliance are all properly authenticated and authorized by the appliance. The Information Assurance function ensures that Voice and Video signaling streams that traverse the appliance and its ASLAN are properly encrypted SIP/TLS.

SCM-006540 [**Required**] The CCA shall relay received SIP and TLS authentication credentials and encryption key information from sending end systems (i.e., users, PEIs, AEIs, and SBCs) to the Information Assurance function to support the Information Assurance function's user, PEI, AEI, and SBC authentication capabilities, and its PEI, AEI, and SBC signaling stream encryption capabilities.

SCM-006550 [**Required: MG**] The CCA MGC shall relay received H.248 and IPSec (or proprietary-protocol-equivalent) authentication credentials and encryption key information from MGs to the Information Assurance function to support the Information Assurance function's MG authentication capabilities, and its MG signaling stream encryption capabilities.

SCM-006560 [**Required**] The CCA shall relay authentication credentials received in a SIP or AS-SIP REGISTER message from a PEI, AEI, or SBC to the Information Assurance function so the Information Assurance function can validate those credentials and allow that PEI, AEI, or SBC to register with the appliance.

SCM-006570 [**Optional**] The CCA MGC shall relay authentication credentials received with an H.248 message in an IPSec packet from an MG to the Information Assurance function so the Information Assurance function can validate those credentials and allow that MG to register with the appliance.

SCM-006580 [**Required**] The CCA shall relay TLS encryption key information received from a PEI or AEI to the Information Assurance function so the Information Assurance function can verify that this encryption key information can be used on the signaling streams for voice or video sessions to/from that PEI or AEI.

SCM-006590 [**Required**] The CCA shall relay TLS encryption key information received from an SBC to the Information Assurance function so the Information Assurance function can verify that this encryption key information can be used on the signaling streams for the Voice or Video sessions to/from that SBC.

SCM-006600 [**Required**] The CCA within the appliance shall support all Information Assurance Appliance requirements in Section 4, Information Assurance, which involve the appliance's SCS functions and the appliance's MGC.

The interface and protocols used to interconnect the CCA with the Information Assurance function are internal to the appliance and therefore, are supplier specific.

2.15.6 CCA Interactions With Session Controller Location Service

The Session Controller Location Service (SCLS) provides information on called address translation in response to call routing queries from the CCA.

The interface and protocols used to interconnect the CCA with the SCLS are internal to the appliance and therefore, are supplier specific.

2.15.7 CCA Interactions With Softswitch Location Service

The Softswitch Location Service (SSLS) provides information on call routing in response to call routing queries from the CCA where the CCA determines that the call's destination lies outside the SS.

The interface and protocols used to interconnect the CCA with the SSLS are internal to the appliance and therefore, are supplier specific.

2.15.8 CCA Interactions With End Instrument(s)

The CCA in the SS or SC needs to interact with VoIP PEIs and AEIs served by that SS or SC. The VoIP interface between the PEI and the SS or SC is left up to the network appliance supplier. The VoIP interface between the AEI and the SS or SC is AS-SIP.

The following requirements on VoIP EIs are part of the CCA requirements for the SS or SC:

SCM-006610 [**Required**] The CCA shall support vendor-proprietary Voice and Video EIs, using EI-CCA protocols that are proprietary to the SC or SS supplier.

SCM-006620 [**Required**] The CCA shall support the following Voice and Video EIs and their associated EI signaling protocols:

SCM-006620.a [**Optional**] SIP Voice and Video EIs.

SCM-006620.b [**Optional**] H.323 Voice and Video EIs.

SCM-006620.c [**Required**] AS-SIP Voice and Video EIs.

SCM-006630 [**Conditional**] If the CCA IWF supports H.323 Voice and Video EIs, the IWF shall support these EIs using ITU-T Recommendation H.323.

NOTE: An SC or SS ASLAN may support two different types of H.323 EIs:

a. "H.323 Overlay Network": H.323 EIs that are served by an H.323 Gatekeeper that is completely separate from the CCA.
b. "H.323/AS-SIP Interworking": H.323 EIs that are served by the CCA (where the CCA is effectively an H.323 Gatekeeper for these EIs).

The first case is outside the scope of this section.

SCM-006640 [**Required**] When the CCA IWF supports AS-SIP Voice and Video AEIs, the IWF shall support these AEIs using the set of AS-SIP protocol requirements in Section 2.9.6, Operational Framework for AEIs and Video Codecs, and AS-SIP 2013.

2.15.9 CCA Support for Assured Services Voice and Video

SCM-006650 [**Required**] The Appliance CCA shall support both assured Voice and Video services. The CCA shall support both assured Voice and assured Video sessions, and shall support these sessions from both, VoIP EIs and Video EIs, as described in Section 2.15.8, CCA Interactions With End Instrument(s).

SCM-006660 [**Required**] The Appliance CCA shall support common procedures and protocol for VoIP and Video session control, with the following clarifications and exceptions:

a. The CCA is required to be able to support "single-rate" TDM video (i.e., 64-Kbps TDM video calls) at MG trunk groups that are controlled by the CCA.
b. The CCA is not required to be able to support "multi-rate" TDM video (i.e., Nx64-Kbps TDM video calls, where N runs from 2 to 24) at MG trunk groups that are controlled by the CCA.

SCM-006670 [**Required**] The CCA is not required to support protocol interworking between TDM video calls and the following:

- IP video sessions that originate from or terminate on local Video EIs that are served by the CCA.
- IP video sessions that originate from or terminate on remote Video EIs, that reach the CCA via the SBC, the DISN WAN, and remote appliances.

SCM-006680 [**Required**] The Appliance CCA shall support common procedures and protocol for feature control, for the features and capabilities given in Table 2.2-1, Assured Services Product Features and Capabilities.

SCM-006690 [**Required**] On calls to and from Proprietary VoIP and Proprietary Video EIs, the CCA shall use the appropriate parameters within the appliance supplier's Proprietary protocol messages to differentiate Proprietary VoIP sessions from Proprietary Video sessions.

SCM-006700 [**Conditional**] If H.323 EIs are supported on calls to and from H.323 EIs, the CCA shall use the appropriate parameters within the H.323 protocol messages to differentiate H.323 VoIP sessions from H.323 Video sessions.

SCM-006710 [**Required**] When AS-SIP EIs are supported on calls to and from AS-SIP EIs, the CCA shall use the SDP message bodies in AS-SIP INVITE, UPDATE, REFER, and Acknowledgement (ACK) messages, as well as the SDP message bodies in AS-SIP 200 (OK) responses and earlier 1xx provisional responses, to differentiate AS-SIP Voice sessions from AS-SIP Video sessions.

SCM-006720 [**Required**] The CCA's use of these SDP bodies for VoIP and Video differentiation shall follow the detailed SDP requirements for VoIP and Video in AS-SIP 2013.

SCM-006730 [**Required**] The CCA shall track VoIP sessions against corresponding Appliance VoIP budgets, and shall separately track Video sessions against corresponding Video budgets. The CCA shall maintain the Appliance's VoIP budgets separate from the Appliance's Video budget. The CCA shall perform this separate tracking of Appliance VoIP and Video calls and budgets consistent with the CAC/SAC requirements in Section 2.15.3, CCA Support for Admission Control.

SCM-006740 [**Required**] As part of SC-Level ASAC and WAN-Level ASAC Policing, the CCA shall support PBAS/ASAC for both VoIP sessions and Video sessions, consistent with the ASAC requirements in Section 2.15.3, CCA Support for Admission Control.

SCM-006750 [**Required**] The CCA shall allow an individual PEI to support both VoIP and Video sessions and to have VoIP and Video sessions active at the same time.

SCM-006760 [**Required**] The CCA shall allow an individual AEI to support both VoIP and Video sessions and to have VoIP and Video sessions active at the same time.

SCM-006770 [**Required**] The CCA shall support the routing of both VoIP and Video session requests from SCs to SSs, from SSs to SCs, and from SSs to SSs, using AS-SIP. The CCA shall direct outgoing VoIP and Video session requests to SBCs, and shall accept incoming VoIP and

Video session requests from SBCs, consistent with this SC-to-SS routing, SS-to-SC routing, and SS-to-SS routing.

2.15.10 CCA Interactions With Service Control Functions

SCM-006780 [**Required**] The CCA shall support the ability to remove VoIP and Video sessions and session requests from the media server so the CCA can continue with necessary session processing once the media server has completed its functions. Examples include the following:

a. Removing a calling VoIP PEI or AEI from the media server after in-band audible ringing has been applied and then removed (for a local PEI-to-PEI or AEI-to-AEI call).

b. Removing a called VoIP PEI or AEI from the media server after a Call Preemption tone or announcement has been applied and then removed.

The interface and protocols used to interconnect the CCA with the media server are internal to the SC and SS and, therefore, supplier specific.

2.16 MEDIA GATEWAY

This section provides requirements for the MG function in the SC and SS network appliances. These appliances have defined designs that include a Media Gateway Controller (MGC) function and one or more MGs.

SCM-006790 The MG supports interconnection of VoIP, FoIP, and MoIP media streams with the following SC functions and end-user devices:

> **SCM-006790.a** [**Required: SC MG**] The SC media server, which provides tones and announcements for SC calls and SC features.
>
> **SCM-006790.b** [**Optional: SC MG**] Proprietary VoIP, FoIP, and MoIP EIs on the SC (when these EIs are supported on the SC).
>
> **SCM-006790.c** [**Optional: SC MG**] Proprietary SIP EIs on the SC (when these EIs are supported on the SC).
>
> **SCM-006790.d** [**Optional: SC MG**] Proprietary H.323 EIs on the SC (when these EIs are supported on the SC).
>
> **SCM-006790.e** [**Required: SC MG**] AS-SIP VoIP, FoIP, and MoIP AEIs on the SC.

SCM-006800 [**Optional – Deployable: SC MG**] Deployable SC shall include an MGC and MG.

SCM-006810 [**Conditional – Deployable: SC MG**] If a Deployable SC includes an MG, then the MG shall meet the MG requirements defined in UCR 2013.

The MG in the SS supports ISDN PRI and, optionally, CAS trunks.

NOTE: When an SC is included within an SS, it will serve a set of (SS-internal) SC EIs and MGs. These SC EIs and MGs will exchange media streams with EIs and MGs on other SCs located elsewhere on the DISN WAN. In addition, the SS SBC controls these media streams between the (SS-internal) SC EIs and MGs connected to the SS ASLAN, and EIs and MGs on other SCs, where separate ASLANs are connected to the DISN WAN.

2.16.1 MG Call Denial Treatments to Support CAC

When the CCA determines that a VoIP session request should be blocked because an Appliance CAC restriction applies (e.g., the VoIP session count equals the VoIP session limit for the type of session being requested), the CCA will deny the session request and apply a Call Denial treatment (i.e., a busy signal or call denial announcement) to the calling party on that request. If the calling party is a TDM calling party whose call enters the appliance at an MG trunk group, the MG is responsible for applying the Call Denial treatment also.

SCM-006820 [**Required**] On incoming call requests to a TDM trunk group, where the CCA/MGC applies a CAC Call Denial treatment to that call request, the MG shall connect the TDM called party on the incoming call request to the appropriate CAC Call Denial tone or announcement when instructed to do so by the MGC.

2.16.1.1 MG Call Preemption Treatments to Support ASAC

When the CCA determines that an existing VoIP session or VoIP session request should be cleared because an Appliance ASAC preemption applies (e.g., a CAC limit applies and a call of a higher precedence level needs to complete within the appliance), the CCA will clear the existing session or session request and apply a Call Preemption treatment (i.e., a Call Preemption tone or announcement) to both the calling and called parties on that request. If the calling party is a TDM calling party whose call entered the appliance at an MG trunk group, or the called party is a TDM called party whose call left the appliance at an MG trunk group, the MG is responsible for applying the Call Preemption treatment also.

SCM-006830 [**Required**] On incoming calls or call requests to a TDM trunk group, where the CCA/MGC applies an ASAC Call Preemption treatment to that call or call request, the MG shall connect the TDM calling party on the incoming call or call request to the appropriate ASAC Call Preemption tone or announcement when instructed to do so by the MGC.

SCM-006840 [**Required**] On outgoing calls or call requests from a TDM trunk group, where the CCA/MGC applies an ASAC Call Preemption treatment to that call or call request, the MG shall connect the TDM called party on the outgoing call or call request to the appropriate ASAC Call Preemption tone or announcement when instructed to do so by the MGC.

2.16.1.2 MG and Information Assurance Functions

The MG interaction with Information Assurance function is consistent with the DoD Information Assurance requirements in Section 4, Information Assurance.

The Information Assurance function within the appliance ensures that end users, PEIs, AEIs, MGs, and SBCs that interact with the appliance are all properly authenticated by the appliance. The Information Assurance function also ensures that VoIP signaling streams and media streams that traverse the appliance and its ASLAN are properly encrypted, using SIP/TLS and SRTP, respectively.

Requirements for CCA and MGC interaction with the Information Assurance server are found in Section 2.15.5, CCA Support for Information Assurance. These requirements, therefore, apply to the MG.

SCM-006850 [**Required**] Each MG within an appliance shall support all the appliance requirements in Section 4, Information Assurance, that involve an Appliance MG.

SCM-006860 [**Required**] The MG shall perform the following authentication and encryption functions in conjunction with the CCA and Information Assurance:

- When the MG registers with the MGC in the CCA, the MG exchanges authentication credentials with the CCA and, through the CCA, with Information Assurance.
- The MG exchanges encryption keys with the CCA and, through the CCA, with Information Assurance, before exchanging H.248 messages and encapsulated PRI messages with the MGC in the CCA.
- The MG uses the exchanged encryption keys to (1) encrypt H.248 messages and encapsulated PRI messages sent in the MG => CCA => Information Assurance direction, and (2) decrypt H.248 messages and encapsulated PRI messages sent in the Information Assurance => CCA => MG direction. The encryption and decryption are performed at the IP layer using IPSec packets, instead of being done at the message layer using H.248 messages or PRI messages.
- The MG also performs the following encryption functions in conjunction with PEIs or AEIs, and the media server in the SC (NOTE: These functions may or may not use Information Assurance, depending on the internal design of the SC.):
  - The MG exchanges encryption keys with local PEIs or AEIs and local MGs, remote PEIs or AEIs and remote MGs, and the media server, before exchanging encrypted VoIP media streams with these devices.
  - The MG uses the exchanged encryption keys to (1) encrypt VoIP SRTP media streams sent in the MG => PEI/AEI/other MG/media server direction, and (2) decrypt VoIP SRTP media streams received in the PEI/AEI/other MG/media server => MG direction.

The encryption and decryption are performed above the UDP Transport Layer using SRTP packets.

2.16.1.3 MG Interaction With Service Control Functions

The media server is responsible for playing tones and announcements to calling and called parties on VoIP calls, and for playing audio/video clips (similar to tones and announcements) to calling and called parties on video calls. In addition, the media server may provide "play announcement and collect digits" functionality to calling and called parties on VoIP and video calls when this functionality is required by certain features that the CCA supports. Depending on the complexity of those features, the media server may act as a full Interactive Voice Response (IVR) system for Appliance PEIs/AEIs and other Assured Services end users, providing IVR-like features to local and remote VoIP callers, and providing video-enhanced IVR-like features to local and remote video callers.

The MG is responsible for routing individual VoIP, FoIP, and MoIP media streams to the media server when instructed to do so by the CCA/MGC. When instructed to do so by the CCA/MGC, the MG is responsible for removing individual VoIP, FoIP, and MoIP media streams from the media server, and for either disconnecting them entirely, or routing them on to other SC end users (e.g., VoIP or video EIs).

SCM-006870 [**Required**] When instructed to do so by the MGC, the MG shall direct TDM calls and call requests to the media server, so that the media server can do the following:

a. Play tones and announcements to TDM parties on TDM calls and call requests (e.g., busy tone or announcement; call preemption tone or announcement).

b. Provide "play announcement and collect digits" functionality when required by an Appliance VoIP feature.

c. Provide full IVR-like functionality when required by an Appliance VoIP feature.

The interface and protocols used to interconnect the MG with the media server are internal to the appliance and are, therefore, supplier-specific.

2.16.1.4 Interactions With IP Transport Interface Functions

The Transport Interface functions in the SC provide interface and connectivity functions with the ASLAN and its IP packet transport network. This section outlines high-level requirements for MG interaction with the SC Transport Interface functions. The detailed implementation methods for these requirements are left up to the vendor.

SCM-006880 [**Required**] Since each Appliance MG is an IP endpoint on the Appliance LAN, each MG shall support assignment of the following items to itself:

SCM-006880.a [**Required**] Only one MG IP address (This one IP address shall be implemented in the CCA as either a single logical IP address or a single physical IP address).

SCM-006880.b [**Required**] An MG FQDN that maps to that IP address.

SCM-006880.c [**Required**] An MG SIP URI that uses that MG FQDN as its domain name, and maps to a "SIP User Agent" function within the MG.

SCM-006890 [**Required**] The MG shall interact with the Transport Interface functions in the appliances in the following cases:

SCM-006890.a [**Required**] When the MG uses the native LAN protocols, IP, and UDP to exchange SRTP media streams with PEIs, AEIs, other MGs, and the SBC over the Appliance LAN.

SCM-006890.b [**Optional**] When the MG uses the native LAN protocols, IPSec, and UDP, TCP, or SCTP to exchange H.248 signaling messages with the MGC over the Appliance LAN.

SCM-006890.c [**Optional**] When the MG uses the native LAN protocols, IPSec, and UDP, TCP, or SCTP to exchange encapsulated PRI messages with the MGC over the Appliance LAN.

2.16.1.5 MG–SBC Interaction

The MG interacts with the SBC by sending SRTP media streams to it (for call media destined for a PEI, AEI, or MG that is served by another appliance outside the SC), or by accepting SRTP media streams from it (for call media arriving from a PEI, AEI, or MG that is served by another appliance outside the SC).

SCM-006900 [**Required**] The SRTP media streams exchanged between the SC MG and a remote PEI, AEI, or MG shall pass through the SBC. (The SBC modifies these SRTP media streams by doing NAT/Network Address Port Translation [NAPT] on them.)

The VoIP MG in the SS or SC needs to interact with VoIP Media Transfer functions in the SBC. The SBC does the following:

- Transfers media streams between the PEIs or AEIs and MGs on the appliance, and PEIs or AEIs and MGs on remote appliances, located elsewhere on the DISN WAN.
- Supports commercial SBC functions, such as NAT and NAPT.
- Supports IP firewall functions.

High-level MG requirements for interacting with an SBC are as follows:

SCM-006910 [**Required**] When sending VoIP media streams to PEIs or AEIs and MGs served by other network appliances, the MG shall direct these VoIP media streams to the SBC so the SBC can process them before sending them on to the remote PEIs or AEIs and MGs via the DISN WAN. The MG shall use IP address of the local SBC, when directing the VoIP media streams via the local SBC to the DISN WAN and the remote PEIs or AEIs and MGs.

SCM-006920 [**Required**] The MG shall direct VoIP media streams to remote PEIs or AEIs and MGs through the SBC in the following cases:

a. When the MG is part of an SC and is directing VoIP media streams to PEIs or AEIs and MGs on another SC on the DISN WAN.

b. When the MG is part of an SC and is directing VoIP media streams to PEIs or AEIs and MGs on an SS on the DISN WAN.

c. When the MG is part of an SS and is directing VoIP media streams to PEIs or AEIs and MGs on an SC on the DISN WAN.

d. When the MG is part of an SS and is directing VoIP media streams to PEIs or AEIs and MGs on another SS on the DISN WAN.

SCM-006930 [**Required**] When accepting VoIP media streams from PEIs or AEIs and MGs served by other network appliances, the MG shall accept these VoIP media streams from the appliance SBC, because the SBC relays them from the DISN WAN and the remote PEIs or AEIs and MGs on the DISN WAN. The MG shall recognize and act on the network-level IP addresses of the remote PEIs or AEIs and MGs, when accepting the VoIP sessions through the SBC from the DISN WAN and the remote PEIs or AEIs and MGs.

SCM-006940 [**Required**] The MG shall accept VoIP media streams from remote PEIs or AEIs and MGs through the SBC in the following cases:

a. When the MG is part of an SC and is accepting VoIP media streams from PEIs or AEIs and MGs on another SC on the DISN WAN.

b. When the MG is part of an SC and is accepting VoIP media streams from PEIs or AEIs and MGs on an SS on the DISN WAN.

c. When the MG is part of an SS, and is accepting VoIP media streams from PEIs or AEIs and MGs on an SC on the DISN WAN.

d. When the MG is part of an SS, and is accepting VoIP media streams from PEIs or AEIs and MGs on another SS on the DISN WAN.

2.16.1.6 MG Support for Appliance Management Functions

The Management function in the SBC, SC, and SS supports functions for SBC/SC/SS FCAPS management and audit logs.

SCM-006950 [**Required**] The MG shall interact with the Appliance Management function by doing the following:

- Making changes to its configuration and to its trunks' configuration in response to commands from the Management function that request these changes.
- Returning information to the Management function on its FCAPS in response to commands from the Management function that request this information.
- Sending information to the Management function on a periodic basis (e.g., on a set schedule), keeping the Management function up-to-date on MG activity. An example of this update would be a periodic transfer of trunk media error logs from the MG to the Management function so that the Management function could either store the records locally or transfer them to a remote EMS for remote storage and processing.

2.16.1.7 IP-Based PSTN Interface

Voice and Video over IP interfaces from the UC network to the PSTN are pending.

2.16.1.8 MG Requirements: Interactions With VoIP EIs

The MG in the SS or SC needs to interact with VoIP EIs served by that SS or SC, and with VoIP EIs served by other SSs or SCs. The VoIP signaling interface between the PEI and the SS or SC is left up to the network appliance supplier. The VoIP signaling interface between the AEI and the SS or SC is AS-SIP per Section 2.9.6, Operational Framework for AEIs and Video EIs, of this document. Detailed requirements for this VoIP interface are beyond the scope of this section.

However, the following high-level requirements on VoIP EIs do apply and are part of the MG requirements for the SS and SC:

SCM-006960 [**Required**] The MG shall support the exchange of VoIP media streams with the following voice PEIs and AEIs both on the local appliance and on remote network appliances:

a. Vendor proprietary Voice PEIs.

b. Voice SIP EIs, when the appliance supplier supports these EIs.

c. Voice H.323 EIs, when the appliance supplier supports these EIs.

d. Voice AS-SIP EIs.

SCM-006970 [**Optional**] When the MG supports the exchange of voice media streams with voice H.323 EIs (both on the local network appliance and on remote network appliances), the MG shall support a mechanism for interworking the G.7xx/SRTP/UDP/IP-based VoIP media streams that the MG uses with the H.323-based VoIP media streams that the H.323 EI uses.

2.16.1.9 MG Support for User Features and Services

SCM-006980 [**Required**] The MG shall support the operation of the following features for VoIP and Video end users, consistent with the operation of this feature on analog and ISDN lines in DoD TDM switches:

a. Call Hold.
b. Music on Hold.
c. Call Waiting.
d. Precedence Call Waiting.
e. Call Forwarding Variable.
f. Call Forwarding Busy Line.
g. Call Forwarding No Answer.
h. Call Transfer.
i. Three-way calling.
j. Hotline Service.
k. Calling Number Delivery
l. Call Pickup.

2.16.2 MG Interfaces to TDM NEs in DoD Networks: PBXs, EOs, and MFSs

SCM-006990 [**Required**] Each appliance MG shall support TDM trunk groups that can interconnect with the following NEs in DoD networks, in the United States and worldwide:

a. PBXs.
b. SMEOs.
c. EOs.
d. MFSs.

SCM-007000 [**Required**] Each appliance MG shall support TDM trunk groups that can interconnect with DISN and DoD NEs in the United States and worldwide using the following types of trunk groups:

SCM-007000.a [**Required: SC, SS**] U.S. National ISDN PRI, where the MG handles both the media channels and the signaling channel.

(1) ANSI T1.619 and T1.619a support is required for PRI MLPP signaling.

(2) Facility Associated Signaling is required for T1.619A and commercial PSTN PRIs, and NFAS is optional for T1.619A and commercial PSTN PRIs.

SCM-007000.b [**Optional: SC, SS**] U.S. CAS trunks, where the MG handles both media and signaling on the same channel.

SCM-007000.b.1 [**Conditional: SC, SS**] If a U.S. CAS trunk is supported, then CAS MLPP signaling shall be required.

SCM-007010 [**Required**] MG support for these TDM trunk groups shall be identical to the support for these trunk groups in DoD TDM PBXs, EOs, Tandem switches, and MFSs.

2.16.3 MG Interfaces to TDM NEs in Allied and Coalition Partner Networks

The appliance suppliers should support TDM trunk groups on their MG product that can interconnect with NEs in U.S. Allied and Coalition partner networks worldwide.

SCM-007020 [**Required**] The MG shall support foreign country ISDN PRI trunk groups where the MG handles both the media channels and the signaling channel as follows:

a. For interconnection with an allied or coalition partner network, using foreign ISDN PRI from the network of the allied or coalition partner.

b. Support for MLPP using ISDN PRI, per ITU-T Recommendation Q.955.3, is required on SC trunk groups when these trunk groups are used to connect to an allied or coalition partner from a U.S. OCONUS ETSI-compliant country.

c. Support for MLPP using ISDN PRI, per ITU-T Recommendation Q.955.3, is required on SS trunk groups when these trunk groups are used to connect to an allied or coalition partner from a U.S. OCONUS ETSI-compliant country.

SCM-007030 [**Optional**] The MG shall support foreign country CAS trunk groups where the MG handles both media and signaling on the same channel as follows:

a. For interconnection with an allied or coalition partner network, using foreign CAS trunk groups from the network of the allied or coalition partner.

b. Support for MLPP using CAS trunk signaling is not required on these trunk groups.

SCM-007040 [**Conditional**] If appliance suppliers support allied and coalition partner network TDM trunk groups on their MG, then MG support for these trunk groups shall be identical to the support for these trunk groups in DoD TDM PBXs, EOs, Tandem Switches, and MFSs.

2.16.4 MG Interfaces to TDM NEs in the PSTN in the United States

SCM-007050 [**Required**] Each appliance MG shall support TDM trunk groups that can interconnect with NEs in the PSTN in the United States, including CONUS, Alaska, Hawaii, and U.S. Caribbean and Pacific Territories.

SCM-007060 [**Required**] Each appliance MG shall support TDM trunk groups that can interconnect with the U.S. PSTN, using the following types of trunk groups:

SCM-007060.a [**Required**] U.S. National ISDN PRI, where the MG handles both the media channels and the signaling channel:

(1) This is required for U.S. PSTN NEs nationwide.

(2) Support for MLPP using ISDN PRI is not required on these trunk groups.

(3) Support for FAS is required on these trunk groups.

(4) Support for NFAS is optional on these trunk groups.

SCM-007060.b [**Optional**] U.S. CAS trunks, where the MG handles both media and signaling on the same channel:

(1) This is optional for U.S. PSTN NEs nationwide.

(2) Support for MLPP using CAS trunk signaling is not required on these trunk groups.

SCM-007070 [**Required**] MG support for these TDM trunk groups to the U.S. PSTN shall be identical to the support for these trunk groups in DoD TDM PBXs, EOs, Tandem Switches, and MFSs.

2.16.5 MG Interfaces to TDM NEs in OCONUS PSTN Networks

The appliance supplier (i.e., SC or SS supplier) should support TDM trunk groups on its MG product that can interconnect with NEs in foreign country PSTN networks (OCONUS) worldwide.

SCM-007080 [**Required**] The MG shall support foreign country ISDN PRI, where the MG handles both the media channels and the signaling channel:

a. For interconnection with a foreign country PSTN, using foreign country ISDN PRI, from the country where the DoD user's B/P/C/S is located.

b. Support for ETSI PRI is required on SC trunk groups when the SC is used in OCONUS ETSI-compliant countries.

c. Support for ETSI PRI is required on SS trunk groups when the SS is used in OCONUS ETSI-compliant countries.

d. Support for MLPP using ISDN PRI is not required on the above trunk groups.

SCM-007090 [**Optional**] The MG shall support foreign country CAS trunks, where the MG handles both media and signaling on the same channel:

a. For interconnection with a foreign country PSTN, using foreign country CAS trunk groups from the country where the DoD user's B/P/C/S is located.

b. Support for MLPP using CAS trunk signaling is not required on foreign country CAS trunk groups.

SCM-007100 [**Conditional**] If an appliance supplier supports foreign country PSTN TDM trunk groups on its MG, then MG support for these trunk groups shall be identical to the support for these trunk groups in DoD TDM PBXs, EOs, Tandem Switches, and MFSs.

2.16.6 MG Support for ISDN PRI Trunks

SCM-007110 [**Required**] The MG shall support ISDN PRI trunk groups that carry the U.S./National ISDN version of the ISDN PRI protocol. The MG shall support these U.S. PRI trunk groups conformant with the detailed U.S. ISDN PRI requirements in the following DoD and ANSI documents:

a. Section 2.25.3, ISDN, including Table 2.25-12, PRI Access, Call Control, and Signaling, and Table 2.25-13, PRI Features.

   (1) The "MFS" column in these tables shall apply to the SS.

   (2) The "PBX1" column in these tables shall apply to the SC.

b. Section 2.25.1, Multilevel Precedence and Preemption, including

   (1) Section 2.25.1.4.2, (MLPP Preempt Signaling for) Primary Rate Interface.

   (2) Section 2.25.1.7, ISDN MLPP PRI.

   (3) ANSI T1.619-1992 (R2005).

   (4) ANSI T1.619a-1994 (R1999).

   (5) FAS is required for T1.619 and commercial PSTN PRIs, and NFAS is optional for T1.619 and commercial PSTN PRIs.

SCM-007120 [**Required: SS, SC for ETSI PRI – Optional: SS, SC for Other Foreign PRI**] The appliance supplier (i.e., SC or SS supplier) has the option of supporting one or more foreign versions of the ISDN PRI protocol on its product. As used here, the term "foreign version of ISDN PRI protocol" means the version of the PRI protocol that is used in the PSTN of a foreign country.

SCM-007130 [**Conditional**] If an appliance supplier supports a foreign version of the ISDN PRI protocol on its product, the MG shall support ISDN PRI trunk groups that support the version of the PRI protocol that is used in the PSTN of a foreign country. The MG shall support these foreign PRI trunk groups conformant with the PRI protocol standards that are used in the PSTN of that foreign country. Examples of these standards include ETSI standards and ITU-T standards.

SCM-007140 [**Required**] When used in OCONUS ETSI-compliant countries, the MG shall support ISDN PRI trunk groups that support ITU-T Recommendation Q.955.3 for MLPP.

SCM-007150 [**Required**] The MG shall support multiple U.S. PRI trunk groups based on the needs of the DoD user deploying the appliance. The MG shall allow each U.S. PRI trunk group at the MG to connect to: TDM EO and tandem components of the local MFS; a different U.S.

PSTN TDM Network Element (NE) (e.g., PBX, TDM switch); a different DoD TDM NE (e.g., PBX, TDM switch); or a different DoD IP NE (e.g., SC, SS), based on the interconnection needs of the DoD user.

The MG shall have knowledge of which U.S. PSTN TDM, DoD TDM, and DoD IP NE each U.S. PRI trunk group is connected.

SCM-007160 [**Required: SS, SC for ETSI PRI – Optional: SS, SC for Other Foreign PRI**] When the appliance supplier supports foreign ISDN PRIs, the MG shall support multiple foreign PRI trunk groups based on the needs of the DoD user deploying the appliance. The MG shall allow each foreign PRI trunk group at the MG to connect to a different foreign PSTN TDM, a different allied network element, or a coalition partner TDM network element (e.g., PBX, switch), based on the interconnection needs of the DoD user.

SCM-007170 [**Required**] The MG shall have knowledge of which foreign PSTN TDM, or allied or coalition partner TDM NE each foreign PRI trunk group is connected.

SCM-007180 [**Required**] The MG shall support reception of ISDN PRI messages from the CCA MGC and transmission of ISDN PRI messages to the CCA MGC.

2.16.7 MG Support for CAS Trunks

SCM-007190 [**Optional: SC, SS**] The MG shall support CAS trunk groups that carry the U.S. version of the CAS protocol.

SCM-007200 [**Conditional: SC, SS**] If supported, then the MG shall support these U.S. CAS trunk groups conformant with the detailed CAS trunk and CAS trunk signaling requirements in the following DoD documents:

a. Section 2.25.2, Signaling, including the following:
   (1) Section 2.25.2.4, Trunk Supervisory Signaling.
   (2) Section 2.25.2.5, Control Signaling.
   (3) Section 2.25.2.6, Alerting Signals and Tones.
b. Section 2.25.1, Multilevel Precedence and Preemption, including:
   (1) Section 2.25.1.4.1, Channel-Associated Signaling.

SCM-007210 [**Optional: SC, SS**] The MG shall support foreign versions of CAS trunks and trunk signaling. As used here, the term “foreign version of CAS trunks and trunk signaling” means the version of CAS trunks and trunk signaling that is used in the PSTN of a foreign country.

SCM-007220 [**Conditional: SC, SS**] If the MG supports a foreign version of CAS trunks and trunk signaling, then the CCA IWF shall support the version of CAS trunks and CAS trunk signaling that is used in the PSTN of a foreign country, conformant with the CAS trunk

standards that are used in the PSTN of that foreign country. Examples of these standards include ETSI CAS trunk standards and ITU-T CAS trunk standards.

SCM-007230 [**Conditional: SC, SS**] If the MG supports the U.S. version of CAS trunks and trunk signaling, then the MG shall support multiple U.S. CAS trunk groups based on the needs of the DoD user deploying the appliance. The MG shall allow each U.S. CAS trunk group at the MG to connect to: a TDM EO and Tandem components of the local SS; a different U.S. PSTN TDM NE (i.e., PBX, TDM Switch); a different DoD TDM NE (i.e., PBX, TDM switch); or a different DoD IP NE (i.e., SC, SS), based on the interconnection needs of the DoD user.

SCM-007240 [**Conditional: SC, SS**] If the MG supports a foreign version of CAS trunks and trunk signaling, then the MG shall have knowledge of which U.S. PSTN TDM, DoD TDM, or DoD IP NE (i.e., SC, SS) each U.S. CAS trunk group is connected.

SCM-007250 [**Conditional: SC, SS**] If the MG supports a foreign version of CAS trunks and trunk signaling, then the MG shall support multiple foreign CAS trunk groups based on the needs of the DoD user deploying the appliance. The MG shall allow each foreign CAS trunk group at the MG to connect to a different foreign PSTN, or allied or coalition partner TDM network element (e.g., PBX, TDM switch), based on the interconnection needs of the DoD user.

SCM-007260 [**Conditional: SC, SS**] If the MG supports a foreign version of CAS trunks and trunk signaling, then the MG shall have knowledge of which foreign PSTN TDM, or allied or coalition partner TDM network element each foreign CAS trunk group is connected.

SCM-007270 [**Optional: SC, SS**] The MG shall support reception of U.S. CAS trunk signaling sequences (i.e., Supervisory, Control, and Alerting) from the CCA MGC, and transmission of U.S. CAS trunk signaling sequences to the CCA MGC.

SCM-007280 [**Optional: SC, SS**] The MG shall support the requirements for MLPP Trunk Selection (Hunting) in Section 2.25.1.3.3, MLPP Trunk Selection (Hunting), on MG CAS trunk groups to DSN EOs, SSs, SMEOs, PBX1s, and PBX2s.

2.16.8 MG Requirements: VoIP Interfaces Internal to an Appliance

The requirements in the following section assume that a supplier-specific Gateway Control Protocol is used on the MGC-MG interface. In this case, these requirements assume that the protocol layers below the application layer that carries the supplier-specific Gateway Control Protocol either can be industry standard (in the following paragraph) or supplier specific, which is outside the scope of this document.

When the H.248 Gateway Control Protocol is used over the open interface between the MG and the MGC, this open interface supports industry-standard protocol layers (i.e., physical, data link, network, and transport) below the application layer that carries the Gateway Control Protocol. The support for these protocol layers is optional.

2.16.8.1 MG Support for VoIP Interconnection at the Physical and Data Link Layers

SCM-007290 [**Required**] The MG shall connect to the ASLAN of the appliance using the physical layer and data link layer protocols of the ASLAN. In this case, the MG shall appear to the MGC, SBC, and appliance PEIs/AEIs as a physical layer and data link layer endpoint on a LAN switch in the ASLAN.

2.16.8.2 MG Support for VoIP Interconnection at the Network Layer

SCM-007300 [**Required**] The MG shall connect to the ASLAN of the appliance using the IP as a Network Layer Protocol. In this case, the MG shall appear to the MGC, SBC, and appliance PEIs/AEIs as an IP endpoint on an IP router on the ASLAN.

SCM-007310 [**Required**] The MG shall support IPv4 as a Network Layer Protocol, conformant with RFC 791.

SCM-007320 [**Required**] The MG shall also support IPv6 as a Network Layer Protocol, conformant with RFC 2460.

SCM-007330 [**Required**] Conformant with Section 5, IPv6, the MG shall support dual IPv4 and IPv6 stacks (i.e., support both IPv4 and IPv6 in the same IP end point) as described in RFC 4213.

SCM-007340 [**Conditional**] If an open H.248 MGC-MG interface is used, then the MG shall support IPSec for use with securing IP packets containing H.248 signaling messages and encapsulated ISDN PRI signaling messages. The MG support for IPSec shall be conformant with the appliance IPSec requirements in Section 4, Information Assurance.

NOTE: The MG is not required to support IPSec for use in IP packets containing SRTP media streams for VoIP, FoIP, and MoIP calls.

2.16.8.3 MG Support for VoIP Interconnection at the Transport Layer

NOTE: Support for an open MGC-MG interface is optional.

SCM-007350 [**Conditional**] If an open MGC-MG interface is used, then the MG shall support transport of H.248 signaling messages and encapsulated ISDN PRI signaling messages using the TCP as a Transport Layer Protocol. In this case, the MG shall support TCP conformant with RFC 793.

SCM-007360 [**Conditional**] If an open MGC-MG interface is used, then the MG shall support transport of H.248 signaling messages and encapsulated ISDN PRI signaling messages using the UDP as a Transport Layer Protocol. In this case, the MG shall support UDP conformant with RFC 768.

SCM-007370 [**Conditional**] If an open MGC-MG interface is used, then the MG shall support transport of H.248 signaling messages and encapsulated ISDN PRI signaling messages using the SCTP as a Transport Layer Protocol. In this case, the MG shall support SCTP conformant with RFC 4960.

SCM-007380 [**Conditional**] If an open MGC-MG interface is used, then the MG shall support a per-MG parameter that controls which of the three Transport Layer Protocols (i.e., UDP, TCP, or SCTP) is used to exchange H.248 signaling messages and encapsulated PRI signaling messages with the MGC. This parameter shall support the following values:

a. When this parameter is set to "TCP," the MG shall exchange application layer messages with the MGC using TCP.

b. When this parameter is set to "UDP," the MG shall exchange application layer messages with the MGC using UDP.

c. When this parameter is set to "SCTP," the MG shall exchange application layer messages with the MGC using SCTP.

NOTE: The MG is not required to support TLS at the Transport Layer for securing H.248 signaling messages or encapsulated PRI signaling messages that are exchanged with the MGC using UDP, TCP, or SCTP. IPSec, which provides security at the Network Layer, is used in these cases instead of TLS, which provides security at the Transport Layer. Transport Layer Security is used elsewhere in the appliance to secure AS-SIP signaling messages on the appliance-to-AEI and appliance-to-appliance interfaces, but it is not used to secure H.248 or PRI signaling messages on the MG-to-MGC interface.

NOTE: The SCTP is used in other telecommunication industry documents as the Transport Layer Protocol for communication between VoIP SSs and their MGs.

2.16.8.4 MG Support for VoIP Interconnection for Media Stream Exchange Above the Transport Layer

SCM-007390 [**Required**] The MG shall support exchange of VoIP media streams with appliance PEIs/AEIs, other appliance MGs, and the appliance SBC (and through the appliance SBC, with other PEIs/AEIs and MGs on other network appliances) using the following IETF-defined Media Transfer Protocols:

a. SRTP, conformant with RFC 3711.

b. SRTCP, conformant with RFC 3711.

SCM-007400 [**Required**] The MG shall secure all VoIP media streams exchanged with appliance PEIs/AEIs, other appliance MGs, and the appliance SBC (and through the SBC, with PEIs/AEIs and MGs on other network appliances) using SRTP and SRTCP.

SCM-007410 [**Required**] The MG shall use UDP as the underlying Transport Layer Protocol, and IP as the underlying Network Layer Protocol, when SRTP is used for media stream exchange.

2.16.8.5 MG Support for VoIP Interconnection for Signaling Stream Exchange Above the Transport Layer

SCM-007420 [**Conditional**] If an open MGC-MG interface is used, then the MG shall support exchange of VoIP signaling streams with the appliance MGC. When the VoIP signaling streams contain ISDN PRI signaling messages at the Application Layer, the MG shall use the ISDN User Adaptation (IUA) Protocol between the Transport Layer and the Application Layer (the ISDN PRI signaling). The MG shall support the IUA Protocol consistent with RFC 4233.

NOTE: The IUA Protocol is used in other telecommunication industry documents as the ISDN Adaptation Layer Protocol above the SCTP Transport Layer Protocol for ISDN communication between VoIP SSs and their MGs.

SCM-007430 [**Conditional**] If the VoIP signaling streams contain vendor-proprietary protocol messages instead of H.248 or ISDN PRI messages, then the MG shall secure the proprietary protocol message exchange with the MGC using mechanisms that are as strong as, or stronger than, the use of IPSec to secure H.248 and PRI message exchange.

2.16.8.6 MG Support for VoIP Interworking for ISDN PRI Trunks

SCM-007440 [**Required**] When an MG interworks a TDM call from an ISDN PRI trunk group with a VoIP session within the network appliance, the MG shall perform the following:

SCM-007440.a [**Required**] Convert between the ISDN media stream on the ISDN PRI B-Channel and the VoIP SRTP/Transport Layer/IP media stream within the appliance.

SCM-007440.b [**Optional**] Convert between ISDN signaling messages (ITU-T Recommendation Q.931 messages in Q.921 frames) on the ISDN PRI D-Channel and encapsulated ISDN signaling messages (ITU-T Recommendation Q.931 messages in IUA frames) in a VoIP IUA/Transport Layer/IPSec signaling stream within the appliance.

NOTE: The method of converting PRI signaling into VoIP signaling and the method of conveying this information to and from the CCA are dependent on the MGC protocol used. Some protocols will not use encapsulation at all. If H.248 is used, signaling is encapsulated between the MG and CCA.

2.16.8.6.1 MG Support for VoIP Interworking for National ISDN PRI

SCM-007450 [**Optional**] For U.S. ISDN PRI trunks carrying National ISDN PRI signaling, the MG shall interwork the National ISDN PRI Data Link Layer Protocol (the National ISDN

version of ITU T Recommendation Q.921) with the IETF IUA Protocol and the underlying Transport Layer and IPSec protocols.

2.16.8.7 MG Support for VoIP Interworking for CAS Trunks

Support for CAS trunks is optional, but if they are supported the MG needs to read and understand incoming CAS signaling sequences before translating them into MGC messages and sending them to the MGC using IP. Similarly, the MG has to understand and generate outgoing CAS signaling sequences after receiving signaling messages from the MGC using IP and translating the signaling messages into the appropriate CAS signaling sequences. The method of converting CAS signaling into VoIP signaling and the method of conveying this information to and from the CCA are dependent on the MG control protocol used. The H.248 protocol provides a standard way of doing this.

2.16.8.7.1 MG Support for VoIP Interworking for U.S. CAS Trunks

SCM-007460 [**Conditional**] If the MG supplier supports U.S. CAS trunks, then the MG shall interwork a TDM call from a U.S. CAS trunk with a VoIP session within the appliance and shall perform the following:

a. Convert between the TDM media stream on the CAS trunk and the VoIP SRTP/Transport Layer/IP media stream within the appliance.

b. Convert between the CAS signaling sequences on the CAS trunk and the VoIP signaling sequences within the appliance.

2.16.8.7.2 MG Support for VoIP Interworking for Foreign CAS Trunks

SCM-007470 [**Conditional**] If the MG supplier supports foreign CAS trunks, then the MG shall interwork a TDM call from a foreign CAS trunk with a VoIP Session within the appliance and shall perform the following:

a. Convert between the TDM media stream on the foreign CAS Trunk and the VoIP SRTP/Transport Layer/IP media stream within the appliance.

b. Convert between the CAS signaling sequences on the foreign CAS trunk and the VoIP signaling sequences within the appliance.

2.16.8.8 MG Support for VoIP Codecs for Voice Calls

The MG must support a set of internationally standard and DISN-standard VoIP codecs for use in converting TDM media streams to VoIP media streams, and in converting VoIP media streams to TDM media streams.

SCM-007480 [**Required**] The MG shall support TDM voice streams using the following:

a. ITU-T 64 Kbps G.711 μ -law PCM over digital trunks.

b. ITU-T 64 Kbps G.711 A-law PCM over digital trunks.

c. North American 56 Kbps G.711 μ -law PCM over digital trunks.

SCM-007490 [**Optional**] The MG shall support voice streams using 2-wire and 4-wire North American analog voice circuit interfaces on the non-IP side of the MG, using the following signaling protocols:

a. Loop Start signaling.

b. Ground Start signaling.

c. E&M signaling.

SCM-007500 [**Required**] The MG shall convert between North American 56 Kbps G.711 μ-law PCM and ITU-T 64 Kbps G.711 μ -law PCM in cases where North American 56 Kbps TDM voice trunks are used on the TDM side of the MG.

SCM-007510 [**Required**] The MG shall convert between North American analog voice transmission and ITU T 64 Kbps G.711 μ -law PCM in cases where North American analog voice trunks are used on the TDM side of the MG.

SCM-007520 [**Conditional**] If the MG supplier supports analog foreign CAS trunks, then the MG shall support TDM voice streams using international (foreign) analog voice transmission over analog trunks on TDM trunk groups on the TDM side of the MG.

SCM-007530 [**Conditional**] If the MG supplier supports analog foreign CAS trunks, then the MG shall convert between international (foreign) analog voice transmission and ITU-T 64 Kbps G.711 A law PCM in cases where international (foreign) analog voice trunks are used on the TDM side of the MG.

2.16.8.8.1 Support for Uncompressed, Packetized VoIP per ITU-T Recommendation G.711

SCM-007540 [**Required**] The MG shall support uncompressed, packetized VoIP streams using ITU-T Recommendation G.711 μ law PCM and ITU-T Recommendation G.711 A-law PCM (ITU-T Recommendation G.711, November 1998, plus Appendix I, September 1999, and Appendix II, September 2000) over the IP network on the VoIP side of the MG.

SCM-007550 [**Required**] The MG shall packetize/depacketize G.711 media streams received or sent between its TDM side and its VoIP side.

SCM-007560 [**Required**] The MG shall transport each packetized G.711 VoIP stream to and from the destination local PEI, local AEI, local MG, remote PEI (via an SBC), remote AEI (via an SBC), or remote MG (via an SBC) using SRTP, UDP, and IP protocol layers on the VoIP side of the MG.

SCM-007570 [**Required**] The MG shall support the use of uncompressed, packetized G.711 μ-law and A-law VoIP media streams for both Fixed and Deployable applications.

2.16.8.8.2 Support for Compressed, Packetized VoIP per ITU-T Recommendation G.72x

SCM-007580 [**Required**] The MG shall support compressed, packetized VoIP streams over the IP network on the VoIP side of the MG, according to the following international standards:

a. ITU-T Recommendation G.723.1.

b. ITU-T Recommendation G.729, plus Erratum 1, and Annexes A through J, and Appendices I, II, and III.

SCM-007590 [**Required**] The MG shall use internal G.723.1 and G.729 codecs to perform this compression and decompression. These compressed VoIP codecs are referred to collectively as G.72x in this section. The MG shall use these internal codecs to 1) compress G.711 TDM media to G.72x VoIP media, for media transfer in the TDM-to-IP direction, and 2) decompress G.72x VoIP media to G.711 TDM media, for media transfer in the IP-to-TDM direction.

SCM-007600 [**Required**] The MG shall transport each packetized G.72x VoIP stream to and from the destination local PEI, local AEI, local MG, remote PEI (via an SBC), remote AEI (via an SBC), or remote MG (via an SBC) using SRTP, UDP, and IP protocol layers on the VoIP side of the MG.

SCM-007610 [**Required**] The MG shall support the use of packetized G.72x VoIP media streams for both Deployable and Fixed applications.

2.16.8.9 MG Support for Group 3 Fax Calls

SCM-007620 [**Required**] The MG shall support Group 3 Facsimile (G3 Fax) calls between TDM trunk-side interfaces on the MG, PEIs, AEIs, TAs, IADs, TDM line-side interfaces on the MG, and SBCs.

SCM-007630 [**Required**] The MG shall support G3 Fax calls on TDM trunks for the following TDM trunk types:

- U.S. ISDN PRI.
- U.S. CAS trunk (Conditional: when the MG supplier supports U.S. CAS trunks).
- Foreign ISDN PRI (Required: When the MG supplier supports ETSI PRI – Optional: when the MG supplier supports other foreign ISDN PRIs).

SCM-007640 [**Required**] The MG support for G3 Fax calls on the TDM trunk types listed in this section shall be identical to the support for G3 Fax calls on these trunk groups in DoD TDM PBXs, EOs, Tandem switches, and MFSs.

SCM-007650 [**Required**] The MG support for G3 Fax calls on the TDM trunk types listed in this section shall allow G3 Fax calls to:

a. Originate from a PEI, AEI, TA, IAD, or MG line card that supports G3 Fax, and terminate on a G3 Fax device in a TDM network (i.e., DoD; U.S. or foreign PSTN; allied or coalition partner), via an MG trunk card.

b. Originate from a G3 Fax device in a TDM network (i.e., DoD; U.S. or foreign PSTN; allied or coalition partner) via an MG trunk card, and terminate on a PEI, AEI, TA, IAD, or MG line card supporting G3 Fax.

c. Originate from a G3 Fax device in a TDM network, and terminate to a G3 Fax device in a TDM network, where either TDM network can be DoD, U.S. or foreign PSTN, or allied or coalition partner, when the VVoIP network is used as a tandem network in between the originating TDM network and the terminating TDM network.

SCM-007660 [**Required**] The MG shall support a mechanism to detect FoIP calls, to distinguish them from VoIP calls, and to treat them differently from VoIP calls. The MG shall support this FoIP detection mechanism on both TDM-to-FoIP calls (i.e., inbound from a TDM network to the IP appliance) and FoIP-to-TDM calls (i.e., outbound from the IP appliance to a TDM network).

SCM-007670 [**Required**] The MG shall not rely on called number screening or calling number screening for detecting inbound TDM-to-FoIP calls or outbound FoIP-to-TDM calls.

In other words, the IP appliance administrator are not be required to maintain a list of calling and called fax numbers that are local to the IP appliance (representing FoIP end points within the appliance), and a list of calling and called fax numbers that are outside the IP appliance (representing G3 Fax and FoIP end points outside of the appliance) to determine whether the call is an FoIP call.

SCM-007680 [**Required**] The MG, in conjunction with the MGC, shall support two separate options for "Handling of FoIP calls within the IP appliance:"

a. Handle FoIP calls as G.711 VoIP calls (Fax Passthrough Calls).

b. Handle FoIP calls as ITU-T Recommendation T.38 FoIP calls (Fax Relay Calls).

SCM-007690 [**Required**] The MG and the MGC shall allow the IP appliance administrator to set the value of this option on a per-MG basis. Compression of FoIP calls via ITU-T Recommendation G.723.1 or G.729 is not recommended.

SCM-007700 [**Required**] In the case where an FoIP call enters the IP appliance MG over one TDM trunk or line card, and then leaves the same IP appliance MG over another TDM trunk or line card, the MG shall support the ability to interconnect the two-way TDM media streams from the first trunk/line card directly with the two-way TDM media streams from the second trunk/ line card, without performing any TDM-to-FoIP and FoIP-to-TDM conversions on those two TDM media streams.

2.16.8.9.1 MG Option to "Handle FoIP Calls as G.711 VoIP Calls" (Fax Passthrough Calls)

SCM-007710 [**Required**] When the MG is configured to "Handle FoIP calls as G.711 VoIP Calls," the MG shall support the use of uncompressed, packetized G.711 μ -law and A-law FoIP media streams for both Fixed and Deployable applications.

SCM-007720 [**Required**] When the MG is configured to "Handle FoIP calls as G.711 VoIP Calls," the MG shall handle FoIP calls within the appliance in exactly the same way it handles G.711 VoIP calls within the appliance (e.g., the MG shall not allow compression of the media streams on these calls), with these clarifications:

a. The MG shall still disable ECs for a FoIP call being handled as a G.711 VoIP call, when the MG detects an "EC disabling" tone from either the TDM side or the FoIP side of the call (see Section 2.16.9, MG Requirements for Echo Cancellation).

b. The MG is allowed to disable silence suppression on the FoIP side of the call.

SCM-007730 [**Required**] When the MG is configured to "Handle FoIP calls as G.711 VoIP Calls," the MG shall support uncompressed, packetized FoIP streams using ITU-T Recommendation G.711 μ -law PCM and G.711 A-law PCM over the IP network on the FoIP side of the MG.

SCM-007740 [**Required**] When the MG is configured to "Handle FoIP calls as G.711 VoIP Calls," the MG shall transport each packetized G.711 FoIP stream to and from the local EI/IAD/TA, local MG, remote EI/IAD/TA (via an SBC), or remote MG (via an SBC) using SRTP, UDP, and IP protocol layers on the FoIP side of the MG.

NOTE: That end-to-end (E2E) synchronization of the calling and called fax machines (or fax-equipped devices) is not guaranteed on a fax passthrough call. Even though a fax passthrough call may complete between these two devices (i.e., a successful AS-SIP signaling INVITE/200 OK/ACK exchange can occur, and G.711 media can be exchanged over SRTP, UDP, and IP), there is no guarantee that the two devices will be able to synchronize and exchange fax data using the resulting G.711 media streams. Even if the two devices do synchronize and exchange fax data, there is no guarantee that this synchronization and exchange will be maintained over time, or that the synchronization and exchange will result in a data throughput that matches what would be provided by a Fax Relay call, or by an E2E TDM fax call in a TDM voice network.

Because of this, there are no requirements in this section for the reliability of fax synchronization, reliability of data exchange, or rate of data transfer on fax passthrough calls. It is expected that these calls will complete using AS-SIP signaling and SRTP media exchange like VoIP calls do. However, it is not expected that the resulting synchronization and data exchange

will be 100 percent reliable, or that the data rate provided will match what would be provided on a Fax Relay call or a TDM fax call under the same conditions.

2.16.8.9.2 MG Option To "Handle FoIP Calls as T.38 FoIP Calls" (Fax Relay Calls)

SCM-007750 [**Conditional**] If the MG is configured to "Handle FoIP Calls as T.38 FoIP Calls," then the MG shall not handle FoIP calls within the appliance in the same way it handles G.711 VoIP calls within the appliance. Instead, upon detection that a VoIP call request is actually a FoIP call request, the MG shall direct the FoIP call request to a "T.38 Fax Server" that is internal to the appliance.

NOTE: This "T.38 Fax Server" shall be part of the MG, part of the separate UFS Server in the appliance, or part of the separate media server in the appliance.

SCM-007760 [**Required**] The T.38 Fax Server shall support the full set of procedures and protocols for Fax Relay in ITU-T Recommendation T.38.

SCM-007770 [**Required**] The T.38 Fax Server shall support the full set of procedures and protocols for Group 3 Fax reception and transmission in ITU-T Recommendation T.4.

SCM-007780 [**Required**] The T.38 Fax Server shall support adequate T.38 Fax Relay resources so at least 10 percent of the total number of calls that pass through the trunk-side interfaces of the MG (from TDM end points to IP end points, or from IP end points to TDM end points) can receive Fax Relay treatment, instead of receiving Fax Passthrough treatment.

NOTE: The acquiring activity for the MG and T.38 Fax Server should also determine, based on traffic engineering and vendor prices, the required number of MG Fax Relay resources (e.g., Fax-Relay-equipped trunk cards, or Fax Relay Digital Signal Processing [DSP] cards) that will support T.38 Fax Relay. T.38 Fax Relay is needed to support IP fax devices on an SC or SS, and analog fax devices behind TAs, IADs, and MG line cards on an SC or SS.

2.16.8.10 MG Support for ISDN Over IP Calls and 64-Kbps Clear Channel Data Streams

SCM-007790 [**Required**] The MG shall support 64-Kbps Clear Channel Data on U.S. ISDN PRI TDM trunks.

SCM-007800 [**Required**] The MG shall support 64-Kbps Clear Channel Data on ETSI ISDN PRI TDM trunks.

SCM-007810 [**Optional**] The MG shall support 64-Kbps Clear Channel Data on non-U.S., non-ETSI ISDN PRI TDM trunks.

SCM-007820 [**Required**] MG support for 64-Kbps Clear Channel Data calls on the TDM trunk types listed in this section shall be identical to the support for 64-Kbps Clear Channel Data on these trunk groups in DoD TDM PBXs, EOs, Tandem Switches, and MFSs.

SCM-007830 [**Required**] MG support for 64-Kbps Clear Channel Data calls on the trunk types listed in this section shall allow 64-Kbps Clear Channel Data calls to originate or terminate between an EI supporting 64-Kbps Clear Channel Data and an ISDN terminal supporting 64-Kbps Clear Channel Data in a TDM network (i.e., DoD, U.S. or foreign PSTN, allied or coalition partner). This includes the case when both the calling and called ISDN terminals are on TDM networks, and the IP network is used as a tandem network in between the originating TDM network and the terminating TDM network.

SCM-007840 [**Required**] The MG shall support a mechanism to detect 64-Kbps Clear Channel Data calls; to distinguish them from VoIP, FoIP, MoIP, and SCIP over IP calls; and to treat them differently from VoIP, FoIP, MoIP, and SCIP over IP calls. The MG shall support this 64-Kbps Clear Channel Data detection mechanism on both TDM-to-IP calls (i.e., inbound from a TDM network to the IP appliance) and IP-to-TDM calls (i.e., outbound from the IP appliance to a TDM network).

SCM-007850 [**Required**] When a 64-Kbps Clear Channel Data call enters the IP appliance MG over one TDM trunk, and then leaves the same IP appliance MG over another TDM trunk, the MG shall support the ability to interconnect the two-way TDM media streams from the first trunk directly with the two-way TDM media streams from the second trunk, without performing any TDM-to-IP and IP-to-TDM conversions.

SCM-007860 [**Required**] The MG shall support the procedures and protocols for carrying 64-Kbps Clear Channel Data streams over IP, UDP, and RTP as described in RFC 4040. This shall include the coding of SDP MIME parameters in the following manner (as excerpted from RFC 4040):

a. MIME media type name: audio.

b. MIME subtype name: clearmode.

c. Optional parameters: ptime, maxptime.

   (1) “ptime” gives the length of time in milliseconds represented by the media in a packet, as described in RFC 4566.

   (2) “maxptime” represents the maximum amount of media that can be encapsulated in each packet, expressed as time in milliseconds, as described in RFC 4566.

d. Encoding considerations: This type is defined only for transfer via RTP.

e. Parameter mapping considerations:

   (1) The MIME type (audio) goes in the SDP “m=“ attribute as the media name.

(2) The MIME subtype (clearmode) goes in the SDP "a=rtpmap" attribute as the encoding name.

(3) The optional parameters "ptime" and "maxptime" go in the SDP "a=ptime" and "a=maxptime" attributes, respectively.

2.16.8.11 MG Support for "Hairpinned" MG Calls

SCM-007870 [**Required**] The MG shall support VoIP sessions between trunks on the same MG, including all combinations of TDM call legs and VoIP media end points.

SCM-007880 [**Required**] In the TDM-to-TDM sessions, the MG shall not establish any IP, UDP/TCP/SCTP, RTP, or VoIP codec communication between the "call-originating" and "call-terminating" side of the MG. In addition, the MG shall not establish any TDM-to-VoIP media conversion, or VoIP-to-TDM media conversion, on either side of the MG, for either direction of media transmission.

2.16.8.12 MG Support for Multiple Codecs for a Given Session

SCM-007890 [**Required**] Each MG shall support at least ten audio and voiceband data codecs, including the eight identified as follows:

f. ITU-T G.711 μ-law.

g. ITU-T G.711 A-law.

h. ITU-T G.722.1.

i. ITU-T G.723.1.

j. ITU-T G.729 or G.729A.

k. IETF RFC 4040 (G.711 clear mode).

l. ITU-T T.38 Fax Relay.

m. ITU-T V.150.1 Modem Relay.

SCM-007900 [Required] The MG shall be capable of simultaneously offering at least five codecs for a given session, except when RFC 4040 is used.

2.16.9 MG Requirements for Echo Cancellation

The following basic requirements for MG Echo Cancellation are based on the commercial VoIP network Echo Cancellation requirements in Telcordia Technologies GR-3055-CORE.

2.16.9.1 Trunk Gateway Echo Cancellation

SCM-007910 [**Required**] The MG shall provide an echo canceller (EC) capability with an echo path capacity (echo tail length) of at least 64 ms.

SCM-007920 [**Optional**] The MG shall provide an EC capability with an echo path capacity (echo tail length) of at least 128 ms.

According to ITU Recommendation G.168, ECs may remain active for several types of non-voice calls as well; in particular, for G3 Fax calls and VBD modem calls.

SCM-007930 [**Required**] The MG shall provide echo cancellation for voice, G3 Fax, and VBD modem fax calls. (In the G3 Fax and VBD modem call cases, the MG shall provide echo cancellation if an "echo canceller disabling signal" is not sent by any end user's equipment on the G3 Fax or modem call.) This echo cancellation shall conform to the echo cancellation requirements specified in ITU-T Recommendation G.168.

SCM-007940 [**Required**] Each MG EC shall be equipped with an "echo canceller disabling signal" tone detector. This tone detector shall detect and respond to an in-band EC disabling signal from an end user's G3 Fax or VBD modem device. The EC disabling signal detected shall consist of a 2100-Hz tone with periodic phase reversals inserted in that tone.

SCM-007950 [**Required**] The MG tone detector/EC disabler shall detect the "echo canceller disabling signal" and disable the MG EC when, and only when, that signal is present for G3 Fax or VBD modem.

SCM-007960 [**Required**] The MG shall support all DSN Echo Cancellation requirements in Section 2.25.5, Echo Canceller. In the case of a discrepancy between the DSN Echo Cancellation requirements in Section 2.25.5 and the VVoIP Echo Cancellation requirements here, the VVoIP Echo Cancellation requirements here shall take precedence.

2.16.10 MG Requirements for Clock Timing

SCM-007970 [**Required**] The MG shall derive its clock timing from a designated T1 or PRI interface.

SCM-007980 [**Required: MG**] The MG shall meet the external timing mode requirements specified in the Telcordia Technologies GR-518-CORE, Paragraph 18.1. Most SMEOs and PBX1s will support only line timing.

SCM-007990 [**Required: MG**] The MG shall support external timing modes as defined in Telcordia Technologies TR-NWT-001244.

SCM-008000 [**Required: MG**] The MG shall support line timing modes as defined in Telcordia Technologies TR-NW-001244.

SCM-008010 [**Required: MG**] The MG shall provide internal clock requirements as described in the Telcordia Technologies GR-518-CORE, Paragraph 18.2.

SCM-008020 [**Required: MG**] The MG shall provide a stratum 4 or better internal clock.

SCM-008030 [**Required: MG**] The MG shall meet the synchronization performance monitoring criteria as described in Telcordia Technologies GR-518-CORE, Paragraph 18.3.

SCM-008040 [**Required: MG**] The MG shall meet the DS1 traffic interfaces as described in the Telcordia Technologies GR 518-CORE, Paragraph 18.4.

SCM-008050 [**Required: MG**] The MG shall meet the DS0 traffic interconnects as described in the Telcordia Technologies GR 518-CORE, Paragraph 18.5.

2.16.11 MGC-MG CCA Functions

NOTE: An MGC and MG(s) are optional for Deployable SC locations.

SCM-008060 [**Required**] The MGC within the CCA shall be responsible for controlling all the MGs within the SC or SS.

SCM-008070 [**Required**] The MGC within the CCA shall be responsible for controlling all the trunks (i.e., PRI or CAS) within each MG within the SC or SS.

SCM-008080 [**Required**] The MGC within the CCA shall be responsible for controlling all media streams on each trunk within each MG.

SCM-008090 [**Required**] The MGC within the CCA shall accept IP signaling streams from an MG, conveying received PRI or CAS trunk signaling. The MGC shall return IP signaling streams to the MG accordingly, for conversion to transmitted PRI or CAS trunk signaling.

SCM-008100 [**Conditional**] If the appliance supplier supports non-U.S. PRI or CAS trunks on its product, the CCA shall know which national variant of PRI or CAS signaling (e.g., ETSI/TTC/TTA; Germany/Japan/South Korea) the non-U.S. PRI or CAS Trunk supports.

SCM-008110 [**Required**] Within the appliance (i.e., SC or SS), the MGC shall use either ITU-T Recommendation H.248 (Gateway Control Protocol Version 3) or a vendor-proprietary protocol to accomplish the MG, trunk, and media stream controls described previously.

2.16.11.1 MG Support for MGC-MG Signaling Interface

SCM-008120 [**Required**] The MGC shall use ITU-T Recommendation H.248, other open standards, or a vendor-proprietary protocol for MG control.

SCM-008130 [**Required**] The MGC protocol for MG control (MG Control Protocol) shall support the following:

a. Control message exchanges that are functionally equivalent to the control message exchanges used in ITU-T Recommendation H.248.

b. Transport Layer functionality, including message sequencing, detection of message loss, and recovery from message loss, which are functionally equivalent to the sequencing, loss detection, and loss recovery mechanisms in TCP and SCTP.

c. Strong security for the exchange of gateway control messages and their underlying Transport Layer packets and Network Layer packets, so security controls (i.e., MG and MGC authentication, encryption and decryption of exchanged messages down to the Network Layer) are at least as strong as the IPSec security protection used when ITU-T Recommendation H.248 is used as the MGC-MG protocol. This strong security shall be supported consistent with the H.248-over-IPSec requirements in Section 4, Information Assurance.

SCM-008140 [**Required**] The CCA and MGC shall be able to select the VoIP codec used by the MG to match the type of end point (i.e., PEI, AEI, SBC) and service requested (i.e., uncompressed VoIP; compressed VoIP, FoIP, MoIP, SCIP over IP; or video over IP).

SCM-008150 [**Required**] The CCA and MGC shall ensure that both endpoints of each VVoIP session use the same VVoIP codec for both directions of media stream transmission between the MG and the peer SBC, PEI, AEI, or other MG. ("VVoIP session," as used here, includes VoIP sessions, FoIP sessions, MoIP sessions, SCIP over IP sessions, and video over IP sessions.)

SCM-008160 [**Required**] If the VoIP codec requested by a calling or called PEI, AEI, or SBC end point does not match any of the VVoIP codecs supported by a called or calling MG end point (based on CCA signaling with the EI or SBC, and MGC signaling with the MG), the CCA shall reject the VVoIP media "offer" from this calling or called end point, and indicate to the calling or called end point which VVoIP codec(s) should be used to send compatible VVoIP media to that MG.

"SBC end point," as used here, means a remote PEI, AEI, or MG endpoint served by another appliance elsewhere on the DISN WAN, where signaling and media streams enter the Local Assured Services Domain from the DISN WAN via that domain's SBC.

"VVoIP codec," as used here, includes VoIP codecs, FoIP codecs, MoIP codecs, SCIP over IP codecs, and video over IP codecs.

"VVoIP media," as used here, includes VoIP media, FoIP media, MoIP media, SCIP over IP media, and video over IP media.

SCM-008170 [**Required**] Since the CCA and MGC support selection and negotiation of VoIP codecs on calls to and from MGs, the CCA and MGC shall support, at a minimum, the following set of ITU-T standard VoIP codecs:

a. ITU-T Recommendation G.711, both North American μ -law and international A-law variants.

b. ITU-T Recommendation G.723.1.

c. ITU-T Recommendation G.729.

2.16.11.2 MG Support for Encapsulated National ISDN PRI Signaling

SCM-008180 [**Required**] The MG and MGC shall support the transparent exchange of ISDN PRI signaling messages.

SCM-008190 [**Required**] The MG and MGC shall preserve the correct message sequence, in both directions of an ISDN PRI signaling message exchange.

SCM-008200 [**Required**] The MG and MGC shall support the detection of message loss and recovery from message loss (e.g., by retransmission of lost messages), in both directions of an ISDN PRI signaling message exchange.

SCM-008210 [**Required**] The MG and MGC shall support the detection of message errors and correction of message errors (e.g., by retransmission of errored messages), in both directions of transmission.

SCM-008220 [**Required**] ISDN PRI signaling messages exchanged between the MG and MGC shall be encrypted.

SCM-008230 [**Conditional**] If the MG uses a vendor-proprietary protocol for MG control, then MG support for the immediately preceding requirements within this subsection shall be such that the resulting exchange of ISDN PRI messages (and security of exchanged ISDN PRI messages) is functionally equivalent to what would occur if IUA, UDP/TCP/SCTP, and IPSec were used.

SCM-008240 [**Conditional**] If the MGC and MG use an open protocol to exchange ISDN PRI signaling messages, then the MG shall use the following protocol stack to support encapsulation of ISDN PRI signaling messages sent from the MG to the MGC, and de-encapsulation of ISDN PRI signaling messages sent from the MGC to the MG:

a. National ISDN PRI signaling messages, as described in Telcordia Technologies SR 4994.

b. IUA frames, where IUA shall be supported as defined in RFC 4233.

c. One of the following IETF-standard Transport Layer Protocols:

   (1) TCP.

   (2) UDP.

   (3) SCTP.

d. IPSec packets, secured using mutual MGC and MG encryption, at the IP Network Layer. This encryption shall be performed consistent with the MGC and MG encryption of encapsulated ISDN PRI messages described in Section 4, Information Assurance.

2.16.11.3 MG Support for Mapped CAS Trunk Signaling Using H.248 Packages for MF and DTMF Trunks

SCM-008250 [**Conditional**] If CAS trunks and trunk signaling are supported, then the MG shall transport the CAS trunk signaling between the MG and the MGC. In this case, the MG shall still support the following:

a. Transparent passing of CAS trunk signaling (or indications of CAS trunk signaling) using supplier-specific messages between the MG and MGC.

b. Preservation of correct message sequences, in both directions of transmission.

c. Detection of message loss and recovery from message loss (e.g., by retransmission of lost messages), in both directions of transmission.

d. Detection of message errors and correction of message errors (e.g., by retransmission of errored messages), in both directions of transmission.

e. Securing of supplier-specific messages using MGC and MG encryption, in both directions of transmission.

SCM-008260 [**Conditional**] If CAS trunks and trunk signaling are supported, then the MG shall support all these capabilities over the supplier-specific protocol so the resulting exchange of CAS trunk signaling (and security of the messages carrying the CAS trunk signaling) is identical to what would occur if H.248, UDP/TCP/SCTP, and IPSec were used.

SCM-008270 [**Conditional**] If CAS trunks and trunk signaling are supported and an open protocol is used to support the transport of CAS signaling messages between the MG and MGC, then the MGC shall use the following protocol stack to support encapsulation of CAS trunk signaling sent from the MG to the MGC, and de-encapsulation of CAS trunk signaling sent from the MGC to the MG:

a. ITU-T Recommendation H.248 signaling messages carrying indications of MGC-to-MG and MG-to-MGC signaling for Dual Tone Multifrequency (DTMF) trunks and MF trunks. This H.248 signaling message shall include DTMF, MF, and CAS information from the following H.248 packages:

   (1) Basic DTMF Generator Package (from ITU-T Recommendation H.248.1).

   (2) DTMF Detection Package (from ITU-T Recommendation H.248.1).

   (3) Multi-Frequency Tone Generation and Detection Packages (from ITU-T Recommendation H.248.24).

   (4) Basic CAS Packages (from ITU-T Recommendation H.248.25).

   (5) International CAS Packages (from ITU-T Recommendation H.248.28).

b. One of the following IETF-standard Transport Layer Protocols:

   (1) TCP.

(2) UDP.

(3) SCTP.

c. IPSec packets, secured using mutual MG and MGC encryption, at the IP Network Layer. This encryption shall be performed consistent with the MG and MGC encryption of H.248 messages described in Section 4, Information Assurance.

SCM-008280 [**Conditional**] If CAS trunks and trunk signaling are supported, then the MGC shall support the following set of CAS trunk signals, consistent with their use in Telcordia Technologies GR-3055-CORE (for the MG) and GR-3051-CORE (for the MGC):

a. Seizure Signal. A signal, sent from the originating switching system (or MGC/MG) to the terminating switching system (or MGC/MG), that defines the transition from the trunk idle state to the trunk seizure state.

b. Addressing Control Signal. A signal that marks the transition from the seizure state to the addressing state. Two addressing control methods of operation exist:

(1) Wink Start. After receiving a seizure signal, the terminating switching system (or MGC/MG) sends an off-hook signal with a defined duration (wink) to indicate that it is prepared to receive address information.

(2) Immediate-Dial. No addressing control signal is used. The originating switching system (or MGC/MG) waits for a specified time after sending a seizure signal before sending the first address digit.

c. Answer Signal. A signal that defines the transition from the call-processing state to the communications state, and persists for the duration of the communications state.

d. Transfer of address digits using DTMF signaling for DTMF trunk groups.

e. Transfer of address digits using MF signaling for MF trunk groups.

f. Disconnect Signal. A signal that defines the transition from the call-processing state or the communications state to the idle state.

2.16.11.4 MG Support for Glare Conditions on Trunks

In DSN switching systems, glare occurs when both interfaces of switching systems connected to the same inter-switching-system facility (trunk) apply a seizure signal at approximately the same time. In this section, at least one of the "switching systems connected to the same inter-switching-system facility (trunk)" is an SC or SS MG, as represented by a CAS trunk group.

NOTE: MG support for CAS trunks is optional.

SCM-008290 [**Conditional: SC, SS**] If CAS trunks and trunk signaling are supported, then the MG shall provide functions required to handle a glare situation on CAS trunks as specified in Telcordia Technologies GR-506-CORE, Section 11.5, Glare Resolution.

2.16.11.5 MGC and IWF Treatments for PRI-to-AS-SIP Mapping for TDM MLPP

SCM-008300 [**Required**] In conjunction with the IWF, the MGC shall support the following mapping of PRI-signaled MLPP information to AS-SIP-signaled Reservation Priority High (RPH) information on calls or sessions that involve TDM MLPP and PRI/AS-SIP interworking:

a. The four Network Infrastructure (NI) digits received in octets 5 and 6 of the ISDN PRI precedence level IE shall be mapped to the network-domain subfield of the Namespace field in the AS-SIP RPH.

b. The "MLPP Service domain" information received in octets 7, 8, and 9 of the ISDN PRI precedence level IE shall be mapped to the precedence-domain subfield of the Namespace field in the AS-SIP RPH.

c. The "Precedence level" information received in bits 4 through 1 of octet 4 of the ISDN PRI precedence level IE shall be mapped to the "Resource-Priority (r-priority)" field in the AS-SIP RPH.

In the absence of a received ISDN PRI precedence level IE, the following requirements apply:

SCM-008310 [**Required**] The MGC/IWF shall use a default network-domain value of "uc" in the Namespace field in the AS-SIP RPH.

SCM-008320 [**Required**] The MGC/IWF shall use a default precedence-domain value of "000000" in the Namespace field in the AS-SIP RPH.

SCM-008330 [**Required**] The MGC/IWF shall use a default Resource Priority value of "0 (Routine)" in the "r-priority" field in the AS-SIP RPH.

SCM-008340 [**Required**] The MGC/IWF shall support mapping of the four NI digits to the network-domain subfield of the Namespace field in the RPH as follows:

a. Until the 2012 timeframe, the MGC/IWF shall always use the value "uc" in the network-domain subfield, independent of the NI digits received.

b. For the 2012-and-onwards timeframe, the MGC/IWF shall first check the NI digits translation table that is configured in the CCA for the PRI on which the precedence level IE was received. Table 2.16-1, NI Digit Translation Table, contains a set of valid NI digit sequences (e.g., 0000, 0001, 0002) that the MGC/IWF will accept on that PRI, and the corresponding set of RPH network-domain values (e.g., "uc," "cuc," "dod," "nato") that the valid NI digit sequences map to.

Table 2.16-1. NI Digit Translation Table

LEVEL IE NI DIGITS	OUTPUT SIP RPH NETWORK DOMAIN
0000	uc
0001	cuc

LEVEL IE NI DIGITS	OUTPUT SIP RPH NETWORK DOMAIN
0002	dod
0003	nato
LEGEND	
IE: Information Element	RPH: Resource Priority Header
NI: Network Identifier	SIP: Session Initiation Protocol

c. For the 2012-and-onwards timeframe, the MGC/IWF shall set the value in the network-domain subfield to the network-domain value that is configured for the received NI digits in this translation table for the PRI in question.

SCM-008350 [**Conditional**] If the received NI digits are not included in the translation table for this PRI, the MGC/IWF shall use a default network-domain value of "uc" for this call.

SCM-008360 [**Required**] The MGC/IWF shall support mapping of the PRI "MLPP Service domain" field to the precedence-domain subfield of the Namespace field in the RPH as follows:

a. The MGC/IWF shall convert the three-octet hexadecimal values from the three-octet PRI MLPP service domain field into a text string consisting of six text characters. The MGC/IWF shall use this six-character string as the precedence-domain subfield of the Namespace field in the RPH. For example:

   (1) For the 2012-and-onwards timeframe, the MGC/IWF shall set the NI digits value to the NI digits value that is configured for the received network-domain value in this translation table for the PRI in question.

b. If the received network-domain value is not included in the translation table for this PRI, the MGC/IWF shall use a default NI digits value of "0000" for this call.

SCM-008370 [**Required**] The MGC/IWF shall support mapping of the precedence-domain subfield of the Namespace field in the RPH to the PRI MLPP service domain field as follows:

a. The MGC/IWF shall replace the six-character text string from the RPH precedence-domain with the hexadecimal-encoded number "000000" in the three-octet PRI MLPP service domain field. The MGC/IWF shall use this three-octet hexadecimal-encoded number, "000000," in the MLPP service domain field in the ISDN PRI precedence level IE.

SCM-008380 [**Required**] The MGC/IWF shall support mapping of the Resource-Priority field of the RPH to the PRI Precedence Level field (a semi-octet) as follows:

a. If the network-domain field in the RPH is "uc," then the MGC/IWF shall set the Precedence Level field in the ISDN PRI precedence level IE according to Table 2.16-2, Mapping of RPH r-priority Field to PRI Precedence Level Value.

Table 2.16-2. Mapping of RPH r-priority Field to PRI Precedence Level Value

MLPP PRECEDENCE LEVEL	PRI PRECEDENCE LEVEL VALUE (DECIMAL NUMBER, SEMI-OCTET)	RPH FIELD (SINGLE CHARACTER, TEXT)
ROUTINE	4	0
PRIORITY	3	2
IMMEDIATE	2	4
FLASH	1	6
FLASH OVERRIDE	0	8
Spare, not used	5 through 15	0
LEGEND MLPP: Multilevel Precedence and Preemption PRI: Proprietary End Instrument RPH: Resource Priority Header		

b. If the network-domain field in the RPH is any value other than "uc," then the MGC/IWF shall set the Precedence Level field in the ISDN PRI precedence level IE to the value of "0 1 0 0" (4, meaning Routine).

2.16.11.6 MGC Support for MG-to-MG Calls

SCM-008390 [**Required**] The MGC shall be able to support multiple MGs.

SCM-008400 [**Required**] The MGC shall support VoIP sessions between trunk/line cards on the same or different MGs of the MGC, without requiring them to route to a VoIP EI on the appliance, or requiring them to be routed through the appliance's SBC to the DISN WAN.

SCM-008410 [**Required**] For MG-to-MG sessions where a single MG is involved, the MGC shall handle MG-to-MG calls within a single MG as TDM-to-TDM calls that are local to the MG, rather than as TDM-to-VoIP-to-TDM calls that use VoIP resources within the MG and other appliance components. In this case, the MGC shall instruct the MG to connect the TDM media locally from the one TDM leg of the call, to the TDM media from the other TDM leg of the call, for both directions of TDM media transmission.

2.16.12 MGs Using the V.150.1 Protocol

SCM-008420 [**Conditional: MG**] If the MG uses ITU-T Recommendation V.150.1, then the following applies:

a. ITU-T Recommendation V.150.1 provides for three states: audio, VBD, and modem relay. After call setup, inband signaling may be used to transition from one state to another. In addition, V.150.1 provides for the transition to FoIP using Fax Relay per ITU-T Recommendation T.38.

b. When the MG uses V.150.1 inband signaling to transition between audio, FoIP, modem relay, or VBD states or modes, the MG shall continue to use the established session's

protocol (e.g., decimal 17 for UDP) and port numbers so that the transition is transparent to the SBC.

2.16.13 Remote Media Gateway

SCM-008430 [**Conditional: SC, SS, Remote MG, SBC**] If an MG is geographically separated from the MGC that controls it, then the following five specific conditional requirements address the SBC, the MG control protocol, the DSCP for the control packets, and the security aspects for that arrangement.

SCM-008440 [**Conditional: Remote MG, SBC**] The SRTP media stream and the H.248.1 control packets shall pass through an SBC deployed as part of the Remote MG SUT. The H.248.1 protocol uses well known UDP ports: MG port 2727 and MGC port 2427. Within the IPSec channel, these two ports shall be left open by the SBC, which shall allow only authenticated SCs and SSs to access these port numbers. The requirements for the SBC are given in Section 2.17.10, SBC Requirements to Support Remote MG.

SCM-008450 [**Conditional: SC, SS, Remote MG**] The signaling/control protocol between the SC/SS MGC and the remote MG shall be ITU-T Recommendation H.248.1, Media Gateway Control Protocol. Proprietary protocols for controlling remote MGs are not permitted. The MG VVoIP media stream protocol shall be SRTP.

SCM-008460 [**Conditional: SC, SS, Remote MG**] The precedence level information for each session shall be contained in the SDP part of H.248.1 messages, as specified in AS-SIP 2013, Section 6, Precedence and Preemption.

SCM-008470 [**Conditional: SC, SS, Remote MG**] The H.248.1 protocol packets are a form of signaling packets with respect to their placement in the CE-R QoS queues. Consequently, when transiting the IP CAN/MAN/WAN the H.248.1 packets shall be marked with DSCP 40, as described in Section 6.3.2, Differentiated Services Code Point Assignments.

SCM-008480 [**Conditional: SC, SS, Remote MG, SBC**] The IP Sec with H.248.1 shall be used on the MGC to MGC SBC channel, the MGC SBC to remote MG SBC channel, and on the remote MG SBC to Remote MG channel to secure the MG control protocol packets as specified in Section 4.2.5, Confidentiality [Internet Key Exchange (IKE) version 1, Advanced Encryption Standard (AES) 128, Oakley Group 2048 support, etc.]. Multiple Remote MGs can be controlled by a single MGC. A single IPSec channel shall be used between the MGC and the MGC SBC to encapsulate the multiple H.248.1 control streams. The MGC SBC shall establish separate IPSec channels to each of the Remote MG SBCs, and use the H.248.1 packet header IP address information to route the H.248.1 packets (modified by NAT if it is used) to the corresponding IPSec channel to each of the remote MG SBCs. The Remote MG SBC shall unencapsulate the IPSec channel, use the control information to open and close media stream pinholes, apply NAT if used, and reencapsulate the H.248.1 packets into the IPSec channel to the MG.

2.17 SBC

SCM-008490 [**Required: SBC**] The SBC shall present one or more signaling IP addresses to each network side (one to the LAN [red] side and one to the network [black] side). The SBC shall also present one or more media IP addresses to each network side (one to the LAN [red] side and one to the network [black] side). In both the signaling and media cases, each individual IP address shall be implemented in the SBC as either a single logical IP address or a single physical IP address.

SCM-008500 [**Required: SBC**] The SBC shall still meet all of the VVoIP Intrusion Detection System (IDS) monitoring requirements in this configuration (multiple signaling IP address and multiple media IP addresses on each network side). The SBC IDS monitoring requirements are in Section 4.2.3.4, Ancillary Equipment. The functionality that each VVoIP IDS/Intrusion Prevention System (IPS) shall provide is specified in Section 13.2.4, IPS Functionality, and Section 13.2.5, IPS VVoIP Signal and Media Inspection.

2.17.1 AS-SIP Back-to-Back User Agent

SCM-008510 [**Required: SBC**] The product shall act as an AS-SIP B2BUA for interpreting the AS-SIP messages to meet its functions.

NOTE: The requirements of the product to secure the AS-SIP messages properly are specified in Section 4, Information Assurance, and the proper processing of an AS-SIP message is found in this section and AS-SIP 2013.

SCM-008520 [**Required: SBC**] The product shall be capable of bidirectionally anchoring (NAT and NAPT) the media associated with a voice or video session that originates or terminates within its enclave.

SCM-008520.a [**Required: SBC**] The product shall assign a locally unique combination of “c” and “m” lines when anchoring the media stream.

SCM-008520.b [**Required: SBC**] If an INVITE request is forwarded to a product fronting an SS for which the INVITE request is not destined (i.e., the SS will forward the INVITE request downstream to another SS or SC), the product shall be capable of anchoring the media upon receipt of the INVITE request, but shall restore the original “c” and “m” lines upon receipt of the forwarded INVITE request from the SS.

NOTE: The SS will not modify the “c” and “m” lines. The reason why the anchoring occurs upon receipt of the message is that the product does not know at that point whether the session will terminate within the enclave.

SCM-008520.c [**Required: SBC**] If a session is forwarded or transferred so the session is external to the enclave (i.e., the session no longer terminates or originates within the enclave), then the product shall restore the original received “c” and “m” lines to the

forwarding/transfer message, as appropriate, to ensure that the media is no longer anchored to that product.

SCM-008530 [**Required: SBC**] The SBC shall be capable of processing Route headers IAW RFC 3261, Sections 20.34, 8.1.2, 16.4, and 16.12.

SCM-008540 [**Required: SS**] The SS will generate Route headers for the SBC to identify the next hop for the AS-SIP message.

SCM-008550 [**Optional: SC**] The SC should generate Route headers for the SBC.

SCM-008560 [**Required: SBC**] The product shall preserve/pass the CCA-ID field in the Contact header.

SCM-008570 [**Required: SBC**] The product shall always decrement the Max-Forward header.

SCM-008580 [**Required: SBC**] The product shall modify the Contact header to reflect its IP address to ensure it is in the return routing path.

SCM-008590 [**Required: SBC**] The product fronting an SC shall be capable of maintaining a persistent TLS session between the SBC fronting the primary SS and the SBC fronting the secondary SS. Persistent means the TLS session is established when the product joins the signaling network, and it is not established on a session-by-session basis.

SCM-008590.a [**Required: SBC**] The SBC shall be capable of distinguishing between the primary (associated with the primary SS) and a secondary (associated with the secondary SS) TLS path for the purposes of forwarding AS-SIP messages.

SCM-008590.b [**Required: SBC**] The SBC initiates a session toward its fronted SC/SS (arriving from the WAN) when receiving an incoming INVITE AS-SIP message from the WAN.

2.17.2 Call Processing Load

SCM-008600 [**Required: SBC**] The product shall be capable of handling the aggregated WAN call processing load associated with its SCs and SSs.

NOTE: For instance, if the B/P/C/S has three SCs within the B/P/C/S and each SC is expected to handle 50 WAN calls per minute, then the SBC shall handle 150 calls per minute.

2.17.3 Network Management

SCM-008610 [**Required: SBC**] The product shall support FCAPS Network Management functions as defined in Section 2.19, Management of Network Appliances, of this document.

2.17.4 DSCP Policing

Every ASLAN, whether Fixed (Strategic) or Deployable (Tactical), has an associated SBC. All outgoing VVoIP media packets within the ASLAN that are marked for Assured Services and destined for points outside the ASLAN must be delivered to this SBC. All incoming VVoIP media packets on the WAN Access Circuit serving the ASLAN that are marked for Assured Services and destined for points within the ASLAN must be delivered to the SBC.

SCM-008620 [**Optional: SBC**] The SBC shall ensure that media streams associated with a particular session use the appropriate DSCP based on the information in the AS-SIP RPH.

SCM-008630 [**Optional: SBC**] Packets that are not marked with the appropriate DSCP shall be dropped.

SCM-008640 [**Optional: SBC**] The SBC shall perform this policing for media packets received from the ASLAN that are destined for points outside of the ASLAN, and for media packets received from the WAN that are destined for points within the ASLAN.

NOTE: This requires that the product maintain a table of the appropriate DSCP for an RPH marking. The mapping between precedence and DSCP is found in Section 6, Network Infrastructure End-to-End Performance.

2.17.5 Codec Bandwidth Policing

SCM-008650 [**Optional: SBC**] The SBC shall be capable of ensuring that the media streams associated with a particular session use the appropriate codec (bandwidth) based on the SDP information in the AS-SIP message. The SBC is allowed to drop any session with an associated media stream that exceeds the negotiated bandwidth, or it may perform traffic shaping on the offending media stream.

2.17.6 Availability

There are two types of SBCs: High Availability and Medium Availability. High Availability SBCs support No Loss of Active Sessions and are recommended for locations that serve F/FO users, I/P users, and R users with PRIORITY and above precedence service. It is also noted that Medium Availability SBCs provide a cost-effective solution for locations that serve R users.

SCM-008660 [**Required: High Availability SBC**] The product shall have an availability of 99.999 percent (non-availability of no more than 5 minutes per year). The product shall meet the requirements specified in Section 2.8.2, Product Quality Factors, of this document.

SCM-008670 [**Required: Medium Availability SBC**] The product shall have an availability of 99.99 percent. The product shall meet the requirements specified in Section 2.8.2.1, Product Availability, except for Item i, No Loss of Active Sessions.

NOTE: The vendor will provide a reliability model for the product showing all calculations for how the availability was met.

2.17.7 IEEE 802.1Q Support

SCM-008680 [**Required: SBC**] The product shall be capable of supporting the IEEE 802.1Q 2-byte TCI Field 12-bit Virtual Local Area Network Identification (VID).

NOTE: The VID field has 12 bits and allows the identification of 4096 (212) VLANs. Of the 4096 possible VIDs, a VID value of 0 and 4095 (Hexadecimal FFF) are reserved, so the maximum possible VIDs are 4094. The component shall be capable of distinctly tagging each media (i.e., voice, video, data, signaling, and NM) with any of the 4094 VIDs.

2.17.8 Packet Transit Time

SCM-008690 [**Required: SBC**] The product shall be capable of receiving, processing, and transmitting a UC packet within 2 ms to include executing all internal functions.

NOTE: Internal functions do not include Domain Name Service (DNS) lookups and other external actions or processes.

2.17.9 H.323 Support

SCM-008700 [**Conditional: SBC**] If the SBC supports H.323 video, then the product shall be capable of processing and forwarding H.323 messages IAW Section 4, Information Assurance.

2.17.10 SBC Requirements to Support Remote MG

SCM-008710 [**Conditional: SBC**] If an MG is geographically separated from the MGC that controls it, then the media stream encapsulated in SRTP, and the H.248.1 control packets encapsulated with IPSec shall pass through an SBC deployed as part of the Remote MG SUT. Within the IPSec channel, the H.248.1 protocol uses well-known UDP ports: MG port 2727 and MGC port 2427. The MG SBC shall act as an Application Layer Gateway on H.248.1 sessions, in the same manner as it acts as a B2BUA on AS-SIP sessions, to open and close pinholes for authorized and authenticated bearer sessions.

2.17.11 SBC Support for Multiple SCs

SCM-008720 [**Optional: SBC**] The product shall support more than one SC.

NOTE: A physical SBC may house two or more logical SBCs supporting two or more SCs. Each logical SBC is a software based partition of the single physical SBC asset. Each logical SBC will have its own IP address. Virtual machine middleware may be employed for the partitioning of the physical SBC into two or more logical SBCs.

2.18 WORLDWIDE NUMBERING AND DIALING PLAN

NOTE: PEIs and AEIs are allowed to support the use of a softkey or other method for the user to indicate that a call is Routine or Precedence in lieu of the user explicitly dialing a 9P prefix (where P = 0, 1, 2, 3, or 4).

NOTE: In this Worlwide Number and Dialing Plan section, "intra-SC" means both "within the same SC" and "between an SC and an EO/PBX on the same B/P/C/S." "Inter-SC" means both "from one SC on one B/P/C/S to another SC on another B/P/C/S" and "from one SC on one B/P/C/S to an EO/PBX on another B/P/C/S." These definitions are for Fixed cases. For Deployed cases, the term "enclave" replaces the term "B/P/C/S."

SCM-008730 [**Required: PEI, AEI, SC, SS**] Seven-digit intra-SC dialing options as well as 7- and 10-digit inter-SC dialing shall be supported by UC EIs and signaling appliances.

SCM-008740 [**Required: PEI, AEI, SC, SS**] Seven-digit dialing shall consist of using the seven digits of the SC code and line number to establish either inter-SC or intra-SC calls within the same numbering plan area.

SCM-008750 [**Required: PEI, AEI, SC, SS**] Number assignments for this plan shall be of the form KXX-XXXX, where X is any digit 0–9 and K is any digit 2–8. The specific KXX of each SC will be assigned by DISA to preclude conflicts with other SC codes.

SCM-008760 [**Required: PEI, AEI, SC, SS**] Access to the local attendant shall be obtained by dialing zero.

SCM-008770 [**Required: PEI, AEI, SC, SS**] UC ROUTINE precedence 7-digit inter-SC or intra-SC calls are initiated by dialing the appropriate sequence of (1X) KXX-XXXX or 94 (1X) KXX-XXXX.

SCM-008780 [**Required: PEI, AEI, SC, SS**] UC calls above the ROUTINE precedence are initiated by the appropriate sequence of 9P (1X) KXX-XXXX, where P is the precedence digit (0, 1, 2, or 3).

SCM-008790 [**Required: PEI, AEI, SC, SS**] Ten-digit dialing shall consist of using ten digits comprising the area code, SC code, and line number to establish inter-SC calls where the number plan area of the calling party is different from the number plan area of the called party.

SCM-008800 [**Required: PEI, AEI, SC, SS**] Number assignments for this plan shall be of the form KXX-KXX-XXXX, where K is any digit 2–8, and X is any digit 0–9.

SCM-008810 [**Required: PEI, AEI, SC, SS**] UC ROUTINE precedence 10-digit interswitch calls are initiated by dialing the appropriate sequence of (1X) KXX-KXX-XXXX or 94 (1X) KXX-KXX-XXXX.

SCM-008820 [**Required: PEI, AEI, SC, SS**] The calls above the ROUTINE precedence are initiated by the appropriate sequence of 9P (1X) KXX- KXX-XXXX, where P is the precedence digit (0, 1, 2, or 3).

NOTE: Access to other Government and/or commercial services is obtained by dialing 9 followed by the appropriate service digit(s).

2.18.1 DSN Worldwide Numbering and Dialing Plan

SCM-008830 [**Required: SC, SS**] The DSN Worldwide Numbering and Dialing Plan will be used as the addressing schema within the current DSN and its migration into the SIP environment. The highlights of the DSN Worldwide Numbering and Dialing Plan are summarized in the following paragraphs. The SC shall operate with the dialing format illustrated in Table 2.18-1, DSN User Dialing Format. The digits shown in parentheses may not be dialed by the DSN user on all calls.

Table 2.18-1. DSN User Dialing Format

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

Table 2.18-2, Mapping of DSN tel Numbers to SIP URIs, provides examples of DSN numbers using SIP URIs that use the syntax defined in RFC 3966 and referenced in RFC 3261, Section 19.1.6.

Table 2.18-2. Mapping of DSN tel Numbers to SIP URIs

ALIAS TYPE	SIP URI
7-digit intradomain (SC enclave) call	sip:4305335;phone-context=uc.mil@uc.mil;user=phone
7-digit interdomain (SC enclave) call within same area code	sip:4801235;phone-context=uc.mil@uc.mil;user=phone
10-digit interdomain (SC enclave) call to another area code	sip:3157261135;phone-context=uc.mil@uc.mil;user=phone

SCM-008840 [**Required: SC, SS**] The CCA shall allow session requests from SC, SS EIs, other appliances, and SS MGs to contain the following:

a. Called addresses including DSN numbers from the DSN numbering plan.

b. Called addresses including E.164 numbers from the E.164 numbering plan.

NOTE: The SC and SS may require the use of a DSN escape code, such as "98" or "8," as a prefix to a DSN number from the DSN numbering plan.

NOTE: The SC and SS may require the use of a PSTN escape code, such as "99" or "9," as a prefix to an E.164 number from the E.164 numbering plan.

SCM-008850 [**Required: SC, SS**] When a session request's called address includes a DSN number from the DSN numbering plan, the CCA shall determine whether the called DSN number is local to the SC or SS, or external to the SC or SS.

SCM-008860 [**Conditional: SC, SS**] If the called DSN number is local to the SC or SS, the CCA shall complete the session request within the SC or SS.

SCM-008870 [**Conditional: SC, SS**] If the called DSN number is external to the SC or SS, the CCA shall route the session request outside of the SC or SS, using one of the following:

- The external IP address of the next appliance (i.e., SC or SS) that should handle the session request.
- The local IP address of the SC or SS MG and MG trunk group that should handle the session request.

SCM-008880 [**Required: SC, SS**] When a session request's called address includes an E.164 number from the E.164 numbering plan, the CCA shall determine whether the called E.164 number is local to the SC or SS, or external to the SC or SS.

SCM-008890 [**Conditional: SC, SS**] If the called E.164 number is local to the SC or SS, the CCA shall complete the session request within the SC or SS.

SCM-008900 [**Conditional: SC, SS**] If the called E.164 number is external to the SC or SS, the CCA shall route the session request outside of the SC or SS, using one of the following:

- The external IP address of the next signaling appliance that should handle the session request.
- The local IP address of the SC or SS MG and MG trunk group that should handle the session request.

SCM-008910 [**Required: SC, SS**] The access code shall include the access digit, followed by the precedence digit or the service digit.

SCM-008920 [**Required: SC, SS**] The access digit (e.g., 9) shall provide the indication to the SC/SS that the following digits will indicate either UC call precedence, selected egress to the services of other systems or networks, or selected access to special UC features, such as individual trunk tests.

SCM-008930 [**Required: SC, SS**] The precedence digit (0, 1, 2, 3, or 4) shall permit a UC user to dial an authorized UC precedence level from properly classmarked 12-button telephone instruments. When the 7-digit intraSC dialing option is used, it is not necessary to dial or key the precedence access digit for ROUTINE precedence calls. The assignment of precedence digits is shown in Table 2.18-3, Precedence and Service Access.

Table 2.18-3. Precedence and Service Access

ASSIGNMENTS FOR TELEPHONE KEYSETS		
Access Digit	Precedence Digit	Precedence
e.g., 9	0	UC FLASH OVERRIDE
e.g., 9	1	UC FLASH
e.g., 9	2	UC IMMEDIATE
e.g., 9	3	UC PRIORITY
e.g., 9	4	UC ROUTINE
ASSIGNMENTS FOR SERVICE ACCESS CODES		
Access Digit	Service Digit	Precedence
e.g., 9	5	Off-Net 700 Services
e.g., 9	6	Not Assigned
e.g., 9	7	DSN CONUS ~~FTS~~Networx
e.g., 9	8	Not Assigned
e.g., 9	9	Local PTN

SCM-008940 [**Required: SC, SS**] The service digits, 5 through 9, shall provide information to the SC/SS to connect calls to Government or public telephone services or networks that are not part of the UC. The UC SC/SS will collect the access code and all routing and address digits before attempting to route a call to prevent numbering ambiguities between the access codes and the 2-digit abbreviated dial codes. The assignment of service access codes is shown in Table 2.18-3, Precedence and Service Access.

2.18.1.1 CCA and SSLS Support for Dual Assignment of DSN and E.164 Numbers to SS EIs

SCM-008950 [**Required: SC, SS**] The CCA shall allow each VoIP and Video PEI and AEI served by an SC or SS to have both a DSN number assigned and an E.164 number assigned.

SCM-008960 [**Required: SC, SS**] For VoIP and Video PEIs or AEIs that have both a DSN number and an E.164 number assigned, the CCA shall be able to match each PEI's or AEI's DSN number with its E.164 number, and to match each PEI's or AEI's E.164 number with its DSN number.

2.18.1.2 CCA Differentiation Between DSN Numbers and E.164 Numbers

SCM-008970 [**Required: SC, SS**] The CCA shall be able to distinguish DSN called numbers from E.164 called numbers when processing VoIP and Video session requests from PEIs, AEIs, SBCs, MG line cards, and MG trunk groups.

SCM-008980 [**Required: SC, SS**] The CCA shall be able to distinguish local DSN called numbers from external DSN called numbers when processing VoIP and Video session requests from PEIs, AEIs, SBCs, MG line cards, and MG trunk groups.

SCM-008990 [**Required: SC, SS**] The CCA shall be able to distinguish local E.164 called numbers from external E.164 called numbers when processing VoIP and Video session requests from PEIs, AEIs, SBCs, MG line cards, and MG trunk groups.

SCM-009000 [**Optional: SC, SS**] On SIP and AS-SIP calls from PEIs or AEIs and the SBC, the CCA (and its SCLS and SSLS Servers) shall use the contents of the phone-context parameter in the called SIP URI to determine the following:

a. Whether the session request is intended for a DSN number or an E.164 number.

b. In the E.164 case, whether the E.164 number is locally significant, nationally significant, or internationally significant.

SCM-009010 [**Required: SC, SS**] On ISDN PRI calls from an MG, the CCA shall use the contents of the Type of Number and Numbering Plan Identification fields in the ISDN Called Party Number IE in the SETUP message to determine the following:

a. Whether the call request is intended for a DSN number or an E.164 number.

b. In the E.164 case, whether the E.164 number is locally significant, nationally significant, or internationally significant.

SCM-009020 [**Conditional: SC, SS**] If CAS trunks and trunk signaling are supported, then the CCA shall use the identity of the trunk group that the call was received on (and the presence or absence of prefix digits in the received Called Party Number) to determine the following for CAS trunk calls from an MG:

a. Whether the call request is intended for a DSN number or an E.164 number.

b. In the E.164 case, whether the E.164 number is locally significant, nationally significant, or internationally significant.

2.18.1.3 CCA Use of SIP "phone-context" to Differentiate Between DSN and E.164 Numbers

SCM-009030 [**Optional: SC, SS**] On SIP and AS-SIP calls from PEIs or AEIs and other appliances, the CCA shall use the contents of the "phone-context" parameter in the called SIP URI to distinguish DSN numbers from E.164 numbers as follows:

a. If the "phone-context" parameter in the "User" portion of the called SIP URI indicates "uc.mil" (or a subordinate domain name built on "uc.mil"), then the CCA shall treat the 10-digit number that precedes the "phone-context" parameter as a DSN number.

b. If the "phone-context" parameter in the "User" portion of the called SIP URI indicates a sequence of digits, possibly prefixed with a "+" character, then the CCA shall treat the variable length number that precedes the "phone-context" parameter as an E.164 number.

SCM-009040 [**Optional: SC, SS**] On SIP and AS-SIP calls from SS PEIs or AEIs and other appliances, the CCA shall use the contents of the "phone-context" parameter in the called SIP URI to distinguish local, national, and international E.164 numbers from one another as follows:

a. If there is no "phone-context" parameter in the "User" portion of the called SIP URI, then the CCA shall treat the variable length number in the "User" portion of this URI as an international E.164 number.

b. If the "phone-context" parameter in the "User" portion of the called SIP URI contains a "+" character followed by an E.164 country code, but no area code or city code, then the CCA shall treat the variable length number that precedes the "phone-context" parameter as a national E.164 number (for the country identified by the country code).

c. If the "phone-context" parameter in the "User" portion of the called SIP URI contains a "+" character followed by an E.164 country code and an area code or city code, then the CCA shall treat the variable length number that precedes the "phone-context" parameter as a local E.164 number (for the country identified by the country code, and the area or city identified by the area code or city code).

2.18.1.4 Use of SIP URI Domain Name With DSN Numbers and E.164 Numbers

The SIP URIs used for VVoIP calls contain both a username (with a numeric Called Party Number and an optional "phone-context" parameter) and the domain name "uc.mil." Signaling appliances need some mechanism to accept, reject, or overwrite the domain name values received as part of Called SIP URIs in each VoIP and Video session request.

NOTE: Support for IETF Domain Names implies that UC also supports IETF DNS, which uses domain name servers and allows Domain Names to be resolved to IP addresses (and vice versa). The UC support for DNS is optional.

SCM-009050 [**Optional: SC, SS**] Each signaling appliance shall support a configurable per-appliance parameter, named "Domain Name Treatment for Session Requests," that indicates how the appliance handles domain names received in VoIP and Video session requests.

SCM-009060 [**Conditional: SC, SS**] If a signaling appliance supports the "Domain Name Treatment for Session Requests" parameter, then this parameter shall be set to one of the following values:

- Overwrite with Network Domain Name.
- Overwrite with Appliance FQDN.
- Passthrough.

The default value shall be Overwrite with Network Domain Name.

SCM-009070 [**Conditional: SC, SS**] If a signaling appliance supports the "Domain Name Treatment for Session Requests" parameter, then it shall meet all of the following conditional requirements:

> **SCM-009070.a** [**Conditional: SC, SS**] The appliance shall support all three options noted above, and shall support the default parameter value of "Overwrite with Network Domain Name." The appliance shall allow the option selected to be software-configurable.
>
> **SCM-009070.b** [**Conditional: SC, SS**] When the value of the Domain Name Treatment for Session Requests parameter for the signaling appliance is Overwrite with Network Domain Name, the appliance CCA shall discard all domain names received in called SIP URIs in session requests, and overwrite them with the Domain Name of the DoD network that the appliance belongs to.
>
> **SCM-009070.c** [**Conditional: SC, SS**] The appliance shall support a per-appliance parameter called the "UC Network Domain Name," to be used in overwriting the received domain names in this case. (Support for this additional parameter is not a requirement for UC Spiral 1.) The value of this parameter shall be a text string that identifies the Domain Name of the DoD network that the appliance belongs to, for domain name overwriting purposes. At a minimum, the following FQDNs for DoD networks (i.e., UC, Classified UC[CUC]) shall be supported: "uc.mil" and "cuc.mil."
>
> **SCM-009070.d** [**Conditional: SC, SS**] When the value of the Domain Name Treatment for Session Requests parameter for the appliance is Overwrite with Appliance FQDN, the appliance CCA shall discard all domain names received in called SIP URIs in session requests, and overwrite them with the FQDN of the appliance.
>
> **SCM-009070.e** [**Conditional: SC, SS**] The appliance shall support a per-appliance parameter called the "Appliance FQDN," to be used in overwriting the received domain names in this case. The value of this parameter shall be a text string that identifies the FQDN of the appliance, for domain name overwriting purposes.
>
> **SCM-009070.f** [**Conditional: SC, SS**] When the value of the Domain Name Treatment for Session Requests parameter for the appliance is "Passthrough," the appliance CCA shall transparently passthrough all domain names received in called SIP URIs in session requests, without altering them.

2.18.1.4.1 SIP URI Domain Names in UC Spiral 1

SCM-009080 [**Required: SC, SS**] The SS or SC is required to support only one network FQDN for use with SIP URI domain names: "uc.mil" if that appliance is used for Sensitive but Unclassified (SBU) traffic, and "cuc.mil" if that appliance is used for classified traffic.

SCM-009090 [**Required: SC, SS**] The SS or SC is required to ensure that all AS-SIP session requests entering or leaving that appliance use the network FQDN of that appliance (i.e., "uc.mil" for SBU traffic, or "cuc.mil" for Classified traffic) as the domain name in called SIP URIs.

SCM-009100 [**Conditional: SC, SS**] In cases where a received called SIP URI in a received AS-SIP message has a domain name other than "uc.mil" (for SBU traffic) or "cuc.mil" (for Classified traffic), the SS or SC shall do either of the following:

- Reject the AS-SIP session request that contained the unexpected domain name.
- Accept the AS-SIP session request that contained the unexpected domain name, but overwrite the received domain name with "uc.mil" (for SBU traffic) or "cuc.mil" (for Classified traffic).

2.18.1.5 Domain Directory

SCM-009110 [**Required: SC, SS**] SC and SS shall maintain subscriber assignment information in the form of a domain directory. A domain directory shall support the following functions:

> **SCM-009110.a** [**Required: SC, SS**] A Directory Look-Up function that shall allow a user assigned to an SC to look up the telephone numbers of other users assigned to (i.e., served by) that common SC. This function is referred to as "white pages" services, and it should not be confused with call routing tables used for forwarding SIP call requests.
>
> **SCM-009110.b** [**Required: SC, SS**] For security reasons, the Directory Look-Up function shall be available only from a user's IP telephone instrument, not via the Internet. The IP telephone instrument will contain a small display and function keys that facilitate the Directory Look-Up function.
>
> **SCM-009110.c** [**Required: SC, SS**] Access to the Directory Look-Up function shall be controlled by assigned attributes. There may be specific reasons for denying this privilege to certain users.
>
> **SCM-009110.d** [**Required: SC, SS**] The SC shall allow the system administrator to update the directory database in response to service order activity (i.e., subscriber adds, moves, changes, or removals). The SC shall update the white pages data automatically as well as subscriber line information contained as part of the Directory Look-Up function.

SCM-009110.e [**Optional: SC, SS**] When automatic instrument registration is supported, a service order "flag" shall be sent to the system administrator terminal so the administrator can update the subscriber's location information as necessary.

SCM-009110.f [**Required: SC, SS**] The data elements shown in Table 2.18-4, White Pages Directory Data Elements, shall be incorporated as part of the white pages directory portion of the SC subscriber database.

Table 2.18-4. White Pages Directory Data Elements

DATA ITEM	EXAMPLE
USER 10-DIGIT DSN TELEPHONE NUMBER	315-454-1192
USER ORGANIZATION CODE	SCX
ORGANIZATION NAME	1st Comm Squadron
USER GEOGRAPHIC LOCATION	Langley AFB
USER NAME	Civ Bill Smith

SCM-009110.g [**Optional: SC, SS**] The SC shall support a periodic update of a "global directory" database via an automated electronic transfer of directory data. Any such transfer will be under the control of a system administrator responsible for the global directory.

SCM-009110.h The user shall be offered the following ways of searching for local (domain) directory information:

SCM-009110.h.1 [**Required: SC, SS**] User access to the local domain directory is provided by a "directory" feature available on the VoIP instrument. Directory search will be limited to information contained within the SC subscriber information.

SCM-009110.h.2 [**Required: SC, SS**] The basic search shall be made based on Last Name, First Name.

SCM-009110.h.3 [**Optional: SC, SS**] The search utilitymay allow users to specifiy Boolean expressions for search criteria, such as using OR with multiple entries in a single field, or using AND across multiple fields to identify the desired directory entries.

2.19 MANAGEMENT OF NETWORK APPLIANCES

2.19.1 General Management

SCM-009120 [**Required: SC, SS, SBC**] There shall be a local craftsperson interface [Craft Input Terminal (CIT)] for OAM&P for all VVoIP appliances. The CIT is a supplier-provided input/output device that is locally connected to a network component. The CIT may be connected to the local EMS, which is in turn connected to the VVoIP appliance using the local

EMS Ethernet management interface. The CIT may be connected directly to the VVoIP appliance also, using the Ethernet management interface on the component that would otherwise be used by the local EMS (when there is no local EMS). The CIT may be connected directly to the VVoIP appliance using a separate serial interface.

SCM-009130 [**Required: SC, SS, SBC**] Communications between VVoIP EMS and the VVoIP appliances shall be via IP.

SCM-009140 [**Required: SC, SS and SBC Local EMS**] Where an EMS is the interface with a VVoIP component, the TCP/IP-based communications between the VVoIP EMS and the local EMS shall be via the following:

SCM-009150 [**Required: SC, SS, SBC**] A network appliance shall issue state change notifications for changes in the states of replaceable components, including changes in operational state or service status, and detection of new components.

SCM-009160 [**Required: SC, SS, SBC**] A network appliance shall be provisioned by the VVoIP EMS with the address and Transport Layer port information associated with its Core Network interfaces.

SCM-009170 [**Required: SC, SS, SBC**] A network appliance shall be capable of maintaining and responding to VVoIP EMS requests for resource inventory, configuration, and status information concerning Core Network interface resources (e.g., IP or MAC addresses) that have been installed and placed into service.

SCM-009180 [**Required: SC, SS, SBC**] A network appliance shall be capable of setting the Administrative state and maintaining the Operational state of each Core Network interface, and maintaining the time of the last state change.

SCM-009190 [**Required: SC, SS, SBC**] A network appliance shall generate an alarm condition upon the occurrence of any of the following failure conditions, as defined in ITU-T Recommendation M.3100:

> **SCM-009190.a** [**Required: SC, SS, SBC**] A network appliance shall generate an alarm condition upon the occurrence of power loss.
>
> **SCM-009190.b** [**Required: SC, SS, SBC**] Environmental condition not conductive to normal operation.
>
> **SCM-009190.c** [**Required: SC, SS, SBC**] Loss of data integrity.

SCM-009200 [**Required: SC, SS, SBC**] A network appliance shall generate an alarm condition when the number of received packets that fail encoding integrity checks exceeds a configurable threshold.

SCM-009210 [**Required: SC, SS, SBC**] A network appliance shall generate an alarm condition when the number of received packets that fail decryption exceeds a configurable threshold.

SCM-009220 [**Required: SC, SS, SBC**] A network appliance shall be capable of maintaining and responding to requests for physical resource capacity information for installed components. This information includes the following:

a. Component type and model.

b. Shelf location.

c. Rack location.

d. Bay location.

2.19.2 Requirements for FCAPS Management

General requirements for the five management functional areas are defined in the following sections.

2.19.2.1 Fault Management

SCM-009230 [**Required: SC, SS, SBC**] Faults shall be reported IAW IETF RFC 3418.

2.19.2.1.1 Alarm Messages

SCM-009240 [**Required: SC, SS, SBC**] Alarm messages shall be distinguishable from administrative log messages.

2.19.2.1.2 Self-Detection of Fault Conditions

SCM-009250 [**Required: SC, SS, SBC**] The appliances shall detect their own fault (alarm) conditions.

2.19.2.1.3 Alarm Notifications

SCM-009260 [**Required: SC, SS, SBC**] The NEs shall generate alarm notifications.

2.19.2.1.4 Near-Real-Time Alarm Messages

SCM-009270 [**Required: SC, SS, SBC**] The network elements shall send the alarm messages in near-real time (NRT). More than 99.95 percent of alarms shall be detected and reported in NRT. NRT is defined as event detection and alarm reporting within 5 seconds of the event, excluding transport time.

2.19.2.1.5 SNMP Version 3 Format Alarm Messages

SCM-009280 [**Required: NM**] The network components shall send alarm messages in Simple Network Management Protocol (SNMP) version 3 (SNMPv3) format.

2.19.2.2 Configuration Management

SCM-009290 [**Optional: SC, SS, SBC**] All Configuration Management (CM) information shall be presented IAW RFC 3418.

2.19.2.2.1 Read-Write Access to CM Data by the VVoIP EMS

SCM-009300 [**Required: SC, SS, SBC**] Capability to access and modify configuration data by the VVoIP EMS shall be controllable by using an access privileges function within the network appliance.

2.19.2.3 Accounting Management

SCM-009310 [**Required: SC, SS**] Call Detail Records (CDRs) shall be created and maintained for each session processed and shall include the following items:

a. Host Name of the CCA controlling the call processing.

b. Start Date of call (In Julian or Calendar).

c. Start Time of Call (Hour + Minute + Second).

d. Elapsed Time of Call and/or Stop Time of call.

e. Calling Number.

f. Called Number (included all dialed digits).

g. Precedence level of call.

NOTE: The precedence level of a call shall be maintained in a specific precedence level designation field in the call record, or by providing the dialed precedence level access digits in the called number field.

SCM-009320 [**Optional: SC, SS**] The CDR for each session shall include:

a. Call Answered/Unanswered Indicator.

b. Indication of either a VoIP or Video over IP call.

c. Indication of the assigned bandwidth for Video over IP call.

d. Conference Call Indicator.

e. Customer/Business Group Identification.

The following subsections describe the types of VoIP calls (e.g., PSTN to IP, IP to PSTN), and provide additional call information that shall be captured in the CDR.

2.19.2.3.1 VoIP to PSTN

The term VoIP to PSTN calls refer to calls routed to the PSTN from a VoIP network.

SCM-~~008460~~ 009325 [**Required: SC, SS**] In addition to the call data specified previously, the following call data shall be provided in the CDR for calls that are routed to the PSTN from the VoIP network:

a. IP address of originating subscriber (if the call originated from the subscriber on the VoIP network).

b. IP address of the gateway connecting to the PSTN.

c. Outgoing trunk group of the call.

d. Outgoing trunk group member of the call.

2.19.2.3.2 PSTN to VoIP

PSTN to VoIP refers to the type of call where the call that originates in the PSTN network enters the VoIP network for completion.

SCM-009330 [**Required: SC, SS**] In addition to the call data specified previously, the following call data shall be provided in the CDR for calls that are routed from the PSTN to the VoIP network:

a. IP address of terminating subscriber (if the call terminates to a subscriber on the VoIP network).

b. IP address of the gateway connecting to the PSTN.

c. Incoming trunk group of the call.

d. Incoming trunk group member of the call.

2.19.2.3.3 VoIP to VoIP

A VoIP to VoIP call can be one of the following three basic scenarios:

1. Subscriber in the UC VoIP network originates a call and the call terminates in the UC VoIP network.
2. Subscriber in the UC VoIP network originates a call to the call terminates in another VoIP network.
3. Call from another VoIP network terminates a call to a UC VoIP subscriber.

SCM-009340 [**Required: SC, SS**] In addition to the call data specified previously, the following call data shall be provided in the CDR (that captures both the originating and terminating information) for calls that originate and terminate within the UC VoIP network:

a. IP address of originating subscriber.

b. IP address of terminating subscriber.

SCM-009350 [**Required: SC, SS**] In addition to the call data specified previously, the following call data shall be provided in the CDR for calls that originate from the UC VoIP network and terminate to another VoIP network:

a. IP address of originating subscriber.

b. IP address of the gateway connecting to the other VoIP network (if applicable).

SCM-009360 [**Required: SC, SS**] In addition to the call data specified previously, the following call data shall be provided in the CDR for calls that originate in another VoIP network and terminate in the UC VoIP network:

a. IP address of terminating subscriber.

b. IP address of the gateway connecting to the other VoIP network (if applicable).

2.19.2.3.4 Quality of Service

The "product" for the following requirements is the combination of the Enterprise SC and the set of PEIs and AEIs that it serves.

NOTE: The requirement to provide a voice quality record is optional for SCs in other than the Enterprise Services application.

SCM-009370 [**Required: ESC, PEI, AEI**] The product shall provide a voice quality record at the completion of each voice session. The voice quality record shall be included in the CDR that the ESC generates for that session, and shall conform to the E-Model, as described in TIA TSB-116-A and ITU-T Recommendation G.107. The voice quality record shall contain the calculated R-Factor for the voice session per TIA TSB-116-A. The allowable error for the voice quality calculations shall be ±3 IAW TIA TSB-116-A.

NOTE: This requirement is related only to VoIP EIs and is not applicable to MGs.

SCM-009380 [**Required: ESC, PEI, AEI**] As part of the voice quality record, the product shall provide the raw voice session statistics that are used to make the R-Factor calculation to include, as a minimum, the latency, packet loss, Equipment Impairment Factor (Ie), and the Weighted Terminal Coupling Loss (TCLw).

SCM-009390 [**Required: ESC, PEI, AEI**] As part of the voice quality record, the product shall provide the jitter for the session.

SCM-009400 [**Required: ESC, AEI**] For AEIs, the voice quality record shall be transmitted at the completion of a session to the CCA, in an AS-SIP BYE message if the AEI ends the call, or an AS-SIP 200 (OK) response to a BYE message if the ESC ends the call.

SCM-009410 [**Optional: ESC, PEI, AEI**] The EI shall use one of the following SIP Quality of Service Statistics (QoS Stats) headers to convey the loss, latency, and jitter information in the AS-SIP BYE message or the AS-SIP 200 (OK) response.

a. X-RTP-Stat.

b. P-RTP-Stat.

Note that these QoS Stats headers do not currently include the Ie or TCLw values.

SCM-009420 [**Optional: ESC**] The product shall generate an alarm to the VVoIP EMS when the session R-Factor calculation in the CDR fails to meet a configurable threshold. By default, the threshold shall be an R-Factor value of 80, which is equivalent to an MOS value of 4.0.

2.19.2.4 Performance Management

SCM-009430 [**Optional: SC, SS, SBC**] Performance Management (PM) information shall be presented IAW RFC 3418.

2.19.2.4.1 Near-Real-Time Network Performance Monitoring

Near-real-time network performance monitoring is a subset of PM. The VVoIP EMS collects alarm messages in real time and selected performance data from the appliances on a NRT basis in 5- or 15-minute intervals. Network control personnel evaluate the alarm and performance data and, to minimize the effect on network traffic caused by a network anomaly, the control personnel implement traffic flow (NM) controls. The appliances must be capable of receiving and responding to NM controls from the VVoIP EMS.

2.19.2.4.2 Remote Network Management Commands

2.19.2.4.2.1 Automatic Congestion Controls

SCM-009440 [**Required: SC, SS**] When ASAC budgets are reduced, by NM action, below the current budget allocation, any previous sessions (regardless of precedence level) in excess of the new budget shall be one of the following:

a. Allowed to terminate naturally.

b. Deterministically preempted starting with those of lowest precedence until the number of sessions in progress equals the new budget allocation.

2.19.2.4.2.2 Destination Code Controls

Destination Code Control (DCC) is applied to reduce calls to a specific area or location that has been temporarily designated as “difficult to reach” due to circumstances.

SCM-009450 [**Required: SC, SS**] The SC and SS shall support DCC implemented based on specifying:

a. An entire Numbering Plan Area (NPA).

b. A group of specific NNX codes within an NPA. (The following is an example of when this control becomes necessary: when a large military base having multiple NNX codes becomes isolated.)

c. A single NNX.

d. An NNX-D (hundred group within an NNX. Reason: There are locations within CONUS that share an NNX.)

SCM-009460 [**Optional: SC, SS**] The SC and SS shall have the capability of setting the percentage of calls to be blocked to the designated destination(s).

SCM-009470 [**Required: SC, SS**] FLASH and FLASH OVERRIDE calls shall not be affected by DCC.

SCM-009480 [**Required: SC, SS**] The SC and SS shall play the "No Circuit Available" (NCA) announcement back towards the calling party on call attempts where the calling party is on the UC IP network, and DCC causes call blocking. The content of the NCA announcement shall be as follows: "Network service disruption has prevented the completion of your call. Please hang-up and try your call later. In case of emergency, please contact your Attendant or Operator."

SCM-009490 [**Required: SC, SS**] On SC or SS calls where the calling party is on the DISA TDM network, and the SC or SS MG is located in the session path between the IP called party and the TDM calling party, the MG shall return the Q.850 Cause Code Number 27, Destination out of order, in the DCC call rejection message sent towards the calling party on the T1.619A PRI between the MG and the DISA TDM network.

This cause code indicates that the destination indicated by the calling user cannot be reached because the interface to the destination is not functioning correctly.

2.19.2.4.2.3 Total Office Manual Control Removal

The ability to remove all controls that were put in place is equally applicable to TDM- and IP-based voice systems.

2.19.2.4.2.4 Call Budget Control

SCM-009500 [**Required: SS**] The SS shall be able to set ASAC call budgets for each SC under its control.

SCM-009510 [**Required: SS**] The SS shall be able to set ASAC call budgets for an SC while there are active calls to/from that SC.

SCM-009520 [**Conditional: SC, SS**] If directionalization is supported, then the SS and SC shall be able to swap between directionalization and no directionalization on an AS-SIP trunk group while there are active calls on the trunk group.

SCM-009530 [**Required: SC**] The SC shall be able to set ASAC call budgets for the PEI/AEIs under its control.

SCM-009540 [**Required: SC**] The SC shall be able to set ASAC call budgets for the PEI/AEIs while there are active calls to/from the SC.

SCM-009550 [**Required: SC, SS**] ASAC shall maintain the separate counts for voice and video, in 5-minute intervals. SS ASAC shall provide these counts for each of the SCs under its control and the SC shall provide these counts for the PEIs/AEIs that it controls.

The SS WAN-level ASAC and the SC-level ASAC session budgets and counts are as follows:

SCM-009550.a VoIP Session Budgets:

SCM-009550.a.1 [**Required**] IPB. The total budget of VoIP sessions plus session attempts in the session setup phase that are allowed on the IP access link.

SCM-009550.a.2 [**Optional**] IPBo. The budget for outbound VoIP sessions plus session attempts in the session setup phase that are allowed on the IP access link.

SCM-009550.a.3 [**Optional**] IPBi. The budget for inbound VoIP sessions plus session attempts in the session setup phase that are allowed on the IP access link.

SCM-009550.b TDM Session Budget:

SCM-009550.b.1 [**Required**] TDMB. The overall number of TDM sessions plus sessions in the session setup phase on the TDM link. This equals the number of DS0s on the trunk between the SC MG and the EO/SMEO/PBX1/PBX2.

SCM-009550.c VSU Budgets:

SCM-009550.c.1 [**Required**] VDB. The total number of inbound and outbound VSUs plus the in-progress VSUs connection attempts that an SC is allowed to have over the IP access link.

SCM-009550.c.2 [**Optional**] VDBi. The total number of inbound VSUs plus the in-progress inbound VSUs connection attempts that an SC is allowed to have over the IP access link.

SCM-009550.c.3 [**Optional**] VDBo. The total number of outbound VSUs plus the in-progress outbound VSUs connection attempts that an SC is allowed to have over the IP access link.

SCM-009550.d VoIP Session Counts:

SCM-009550.d.1 [**Required**] IPC. The total number of interbase IP sessions in progress plus the number of session attempts in the session setup phase.

SCM-009550.d.2 [**Optional**] IPCo. The number of outbound IP sessions in progress plus the number of outbound session attempts in the session setup phase.

SCM-009550.d.3 [**Optional**] IPCi. The number of inbound IP sessions in progress plus the number of inbound session attempts in the session setup phase.

SCM-009550.e TDM Session Counts:

SCM-009550.e.1 [**Required**] TDMC. The total number of sessions in progress between the TDM switch and the MG plus the total number of session attempts in the session setup phase.

SCM-009550.f VSU Counts:

SCM-009550.f.1 [**Required**] VBC. The total number of interbase VSU sessions in progress plus the number of session attempts in the session setup phase.

SCM-009550.f.2 [**Optional**] VBCo. The number of outbound VSU sessions in progress plus the number of outbound session attempts in the session setup phase.

SCM-009550.f.3 [**Optional**] VBCi. The number of inbound VSU sessions in progress plus the number of inbound session attempts in the session setup phase.

2.19.2.4.2.5 PEI/AEI Origination Capability Control

Setting the PEI and AEI origination capability involves setting the parameters for the precedence and destinations of a call that may be originated from a PEI or AEI.

SCM-009560 [**Required: SC**] The product shall have the capability of setting a PEI/AEI's maximum allowed precedence level for originating a call. This is a "subscriber class mark feature," which is controlled by the SC system administrator.

SCM-009570 [**Required: SC**] The product shall have the capability of controlling the destination(s) that a PEI or AEI is restricted from calling. This is a subscriber class mark feature that is controlled by the SC system administrator. This action or function can be performed by:

SCM-009570.a [**Required**] Setting the destinations to which calls are to be blocked by:

SCM-009570.a.1 [**Required**] NPA/NNX.

SCM-009570.a.2 [**Optional**] Blocked by a specific 7-digit directory number (NPA-NNX Dxxx).

2.19.2.5 Security Management

SCM-009580 [**Required: SC, SS**, SBC] All network management interactions shall meet the access control, confidentiality, integrity, availability, and non-repudiation requirements in Section 4, Information Assurance.

2.20 V.150.1 MODEM RELAY SECURE PHONE SUPPORT

This section identifies requirements for "V.150.1 Modem Relay Secure Phone Support," to ensure that UC MGs can support SCIP-based secure phones for all scenarios required by the National Security Agency (NSA).

V.150.1 Secure Phone Support relies on the following:

- SCIP-216 Modem Relay capabilities in UC MGs, ATAs, and IADs.
- SCIP-215 Modem Relay capabilities in UC SEI.

2.20.1 SCIP/V.150.1 Gateway

This section contains the SCIP/V.150.1 Gateway requirements for the UCR, based on the NSA document, SCIP-216. All references to "SCIP-216" that follow are references to SCIP-216, Revision 2.1.

2.20.1.1 Basic Minimum Essential Requirements

The following requirements are based on the Basic Minimum Essential Requirements in SCIP-216 Section 3.

2.20.1.1.1 IP Transport Layer Protocol

SCM-009590 [**Required: MG-TS – Optional: MG-LS, TA, IAD**] The SCIP/V.150.1 Gateway shall meet all the requirements for "IP Transport Layer Protocol" in SCIP-216, Section 3.1.

SCM-009600 [**Required: MG-TS – Optional: MG-LS, TA, IAD**] The SCIP/V.150.1 Gateway shall support V.150.1 Simple Packet Relay Transport (SPRT) for reliable IP transport of the demodulated modem signals, per SCIP-216, Section 3.1.

2.20.1.1.2 Operational Mode

SCM-009610 [**Required: MG-TS – Optional: MG-LS, TA, IAD**] The SCIP/V.150.1 Gateway shall meet all the requirements for "V.150.1 Operational Mode" in SCIP-216, Section 3.2.

SCM-009620 [**Required: MG-TS – Optional: MG-LS, TA, IAD**] The SCIP/V.150.1 Gateway shall support the V.150.1 Audio and Modem Relay (MR) modes, per SCIP-216, Section 3.2.

2.20.1.1.3 Modem Relay Gateway Type

SCM-009630 [**Required: MG-TS – Optional: MG-LS, TA, IAD**] The SCIP/V.150.1 Gateway shall meet all the requirements for "Modem-Relay Gateway Type" in SCIP-216, Section 3.3.

SCM-009640 [**Required: MG-TS – Optional: MG-LS, TA, IAD**] The SCIP/V.150.1 Gateway shall support the V.32 and V.34 duplex modulation types in the MR mode, per SCIP-216, Section 3.3.

SCM-009650 [**Required: MG-TS – Optional: MG-LS, TA, IAD**] The SCIP/V.150.1 Gateway shall also support the V.90 digital and V.92 digital modulation types in the MR mode, per SCIP-216, Section 3.3 (where they are optional) and ITU-T Recommendation V.150.1, Section 9.1, where they are required.

SCM-009660 [**Optional: MG-TS, MG-LS, TA, IAD**] The SCIP/V.150.1 Gateway shall also support the V.90 Analog and V.92 analog modulation types in the MR mode, per SCIP-216, Section 3.3 (where they are optional) and ITU-T Recommendation V.150.1, Section 9.1 (where they are also optional).

2.20.1.1.4 Simple Packet Relay Transport

The following requirements are based on the SPRT requirements in SCIP-216, Section 3.4.

SCM-009670 [**Required: MG-TS – Optional: MG-LS, TA, IAD**] The SCIP/V.150.1 Gateway shall meet all the requirements for "Transport Channel" in SCIP-216, Section 3.4.1.

SCM-009680 [**Required: MG-TS – Optional: MG-LS, TA, IAD**] The SCIP/V.150.1 Gateway shall support SPRT Transport Channels TC0, TC2, and TC3 for the exchange of ACKs and control messages, per SCIP-216, Section 3.4.1.

SCM-009690 [**Required: MG-TS – Optional: MG-LS, TA, IAD**] The SCIP/V.150.1 Gateway shall support the "Suggested values for SPRT timers" for Timers TA01, TA02, and TR03, and for Transport Channel TC2, per Table B.3 in Section B.2.3.6 of ITU-T Recommendation V.150.1.

SCM-009700 [**Required: MG-TS – Optional: MG-LS, TA, IAD**] The SCIP/V.150.1 Gateway shall meet all the requirements for "SPRT Modem Relay Messages" in SCIP-216, Section 3.4.2.

SCM-009710 [**Required: MG-TS – Optional: MG-LS, TA, IAD**] In the MR mode, the SCIP/V.150.1 Gateway shall meet all the requirements for the INIT, JM-INFO, CONNECT, MR_EVENT, I_OCTET, and I_OCTET-CS MR messages, as described in Table 3-3 in SCIP-216, Section 3.4.2.

SCM-009720 [**Required: MG-TS – Optional: MG-LS, TA, IAD**] The SCIP/V.150.1 Gateway shall meet all the requirements for "SPRT Timers" in Section 3.4.3 of SCIP-216.

2.20.1.1.5 State Signaling Event

The following requirements are based on the "State Signaling Event (SSE)" requirements in Section 3.5 of SCIP-216.

SCM-009730 [**Required: MG-TS – Optional: MG-LS, TA, IAD**] The SCIP/V.150.1 Gateway shall use the SSE protocol to transition between the Audio (native state) and MR modes of operation, per Section 3.5 of SCIP-216.

SCM-009740 [**Required: MG-TS – Optional: MG-LS, TA, IAD**] The SCIP/V.150.1 Gateway shall meet all the requirements for "SSE Call Discrimination Messages" in Section 3.5.1 of SCIP-216.

SCM-009750 [**Required: MG-TS – Optional: MG-LS, TA, IAD**] The SCIP/V.150.1 Gateway shall meet all the requirements for "SSE Reliability" in Section 3.5.2 of SCIP-216.

SCM-009760 [**Required: MG-TS – Optional: MG-LS, TA, IAD**] The SCIP/V.150.1 Gateway shall meet all the requirements for "SSE Reason Identifier Codes" in Section 3.5.3 of SCIP-216.

SCM-009770 [**Required: MG-TS – Optional: MG-LS, TA, IAD**] The SCIP/V.150.1 Gateway shall meet all the requirements for "SSE Timers" in Section 3.5.4 of SCIP-216.

2.20.1.1.6 Call Setup Protocol

The following requirements are based on the "Call Setup Protocol Requirements for Negotiating Specific V.150.1 Capabilities" in Section 3.6 of SCIP-216.

SCM-009780 [**Required: MG-TS – Optional: MG-LS, TA, IAD**] The SCIP/V.150.1 Gateway shall meet all the requirements for "V.150.1 Version Declaration" in Section 3.6.1 of SCIP-216.

SCM-009790 [**Required: MG-TS – Optional: MG-LS, TA, IAD**] The SCIP/V.150.1 Gateway shall advertise a V.150.1 version number of "1" or higher, per Section 3.6.1 of SCIP-216.

SCM-009800 [**Required: MG-TS – Optional: MG-LS, TA, IAD**] The SCIP/V.150.1 Gateway shall meet all the requirements for "Transcompression Capability" in Section 3.6.2 of SCIP-216.

SCM-009810 [**Required: MG-TS – Optional: MG-LS, TA, IAD**] The SCIP/V.150.1 Gateway shall meet all the requirements for "Modem Relay Type Declaration" in Section 3.6.3 of SCIP-216.

SCM-009820 [**Required: MG-TS – Optional: MG-LS, TA, IAD**] The SCIP/V.150.1 Gateway shall meet all the requirements for "Modulation Support Indication" in Section 3.6.4 of SCIP-216.

SCM-009830 [**Required: MG-TS; Optional: MG-LS, TA, IAD**] The SCIP/V.150.1 Gateway shall meet all the requirements for "RFC 2833 Events" in Section 3.6.5 of SCIP-216.

SCM-009840 [**Required: MG-TS – Optional: MG-LS, TA, IAD**] In the Audio state, the SCIP/V.150.1 Gateway shall declare support for the four Answer events listed in Table 3-8 of Section 3.6.5 in SCIP-216, using the procedures defined in RFC 2833 (RTP Payload for DTMF Digits, Telephony Tones and Telephony Signals).

NOTE: "Support" means that the SCIP/V.150.1 Gateway shall be able to:

a. Transmit the RFC 2833 Event over its IP interface after detecting the corresponding Answer event on its Data Communications Equipment (DCE) interface.

b. Transmit the Answer event on its DCE interface after detecting the corresponding RFC 2833 Event on its IP interface.

SCM-009850 [**Optional: MG-TS, MG-LS, TA, IAD**] The SCIP/V.150.1 Gateway shall meet all the requirements for "SPRT Payload and Window Size Parameter" in Section 3.6.6 of SCIP-216.

SCM-009860 [**Required: MG-TS – Optional: MG-LS, TA, IAD**] The SCIP/V.150.1 Gateway shall meet all the requirements for "JM Delay Support" in Section 3.6.7 of SCIP-216.

SCM-009870 [**Required: MG-TS – Optional: MG-LS, TA, IAD**] The SCIP/V.150.1 Gateway shall meet all the requirements for "Call Discrimination Mode Parameters" in Section 3.6.8 of SCIP-216.

SCM-009880 [**Required: MG-TS – Optional: MG-LS, TA, IAD**] The SCIP/V.150.1 Gateway shall meet all the requirements for "SSE Capability Indications" in Section 3.6.9 of SCIP-216.

SCM-009890 [**Required: MG-TS – Optional: MG-LS, TA, IAD**] The SCIP/V.150.1 Gateway shall meet all the requirements for "SPRT Protocol Support Parameters" in Section 3.6.10 of SCIP-216.

SCM-009900 [**Required: MG-TS – Optional: MG-LS, TA, IAD**] The SCIP/V.150.1 Gateway shall meet all the requirements for "NoAudio Support" in Section 3.6.11 of SCIP-216.

2.20.1.1.7 Data Communications Equipment (DCE) Interface

The following requirements are based on the "DCE Interface Requirements" in Section 3.7 of SCIP-216.

SCM-009910 [**Optional: MG-TS, MG-LS, TA, IAD**] The SCIP/V.150.1 Gateway shall meet all the requirements for "V.14" in Section 3.7.1 of SCIP-216. The I_RAW-OCTET requirements in this section are optional.

SCM-009920 [**Required: MG-TS – Optional: MG-LS, TA, IAD**] The SCIP/V.150.1 Gateway shall meet all the requirements for "Answer Tone Generation" in Section 3.7.2 of SCIP-216.

SCM-009930 [**Required: MG-TS – Optional: MG-LS, TA, IAD**] The SCIP/V.150.1 Gateway shall meet all the requirements for "Absence of V.42" in Section 3.7.3 of SCIP-216.

2.20.1.2 Procedural Minimum Essential Requirements

The following requirements are based on the "Procedural Minimum Essential Requirements" in Section 4 of SCIP-216.

2.20.1.2.1 SSE State Transition

SCM-009940 [**Required: MG-TS – Optional: MG-LS, TA, IAD**] The SCIP/V.150.1 Gateway shall meet all the requirements for SSE State Transition in Section 4.1 of SCIP-216.

SCM-009950 [**Required: MG-TS – Optional: MG-LS, TA, IAD**] The SCIP/V.150.1 Gateway shall meet all the requirements for SSE State Transitions defined in ITU-T Recommendation V.150.1, Annex C, to coordinate the transition between media states.

2.20.1.2.2 SPRT Procedures

The following requirements are based on the "SPRT Procedures Requirements" in Section 4.2 of SCIP-216.

SCM-009960 [**Optional: MG-TS – Optional: MG-LS, TA, IAD**] The SCIP/V.150.1 Gateway shall meet all the requirements for Modem Relay Data Type Selection in Section 4.2.1 of SCIP-216. The I_RAW-OCTET requirements in this section are also Optional.

SCM-009970 [**Required: MG-TS; Optional: MG-LS, TA, IAD**] The SCIP/V.150.1 Gateway shall meet all the requirements for "SPRT Message Ordering" in Section 4.2.2 of SCIP-216.

SCM-009980 [**Required: MG-TS – Optional: MG-LS, TA, IAD**] In the MR mode, the SCIP/V.150.1 Gateway shall transmit the INIT message first, followed by the MR_EVENT message and/or the CONNECT message, as described in Section 4.2.2 of SCIP-216.

SCM-009990 [**Optional: MG-TS, MG-LS, TA, IAD**] The SCIP/V.150.1 Gateway shall meet all the requirements for "SPRT Window and Payload Size Negotiation" in Section 4.2.3 of SCIP-216.

SCM-010000 [**Required: MG-TS – Optional: MG-LS, TA, IAD**] The SCIP/V.150.1 Gateway shall use the MR_EVENT and CONNECT messages to indicate the data rate in bps, as described in Section 4.2.3 of SCIP-216 (which follows the Data Matching Rule defined in ITU-T Recommendation V.150.1).

SCM-010010 [**Required: MG-TS – Optional: MG-LS, TA, IAD**] The SCIP/V.150.1 Gateway shall meet all the requirements for SPRT Data Signaling Rate Indication in Section 4.2.4 of SCIP-216.

SCM-010020 [**Required: MG-TS – Optional: MG-LS, TA, IAD**] The SCIP/V.150.1 Gateway shall use the MR_EVENT and CONNECT messages to indicate the data rate negotiated on its DCE interface in bits per second (bps), per Section 4.2.4 of SCIP-216. The SCIP/V.150.1 Gateway shall also adhere to the Rate Matching Rule defined in Section 12.3.2.1 of ITU-T Recommendation V.150.1.

2.20.1.2.3 RFC 2833 Event Transmission Procedures

SCM-010030 [**Required: MG-TS – Optional: MG-LS, TA, IAD**] The SCIP/V.150.1 Gateway shall meet all the requirements for RFC 2833 Event Transmission Procedures in Section 4.3 of SCIP-216.

2.20.1.2.4 Native Session to Modem-Based Session Transition Procedures

The following requirements are based on the "Native Session to Modem-Based Session Transition Procedures" in Section 4.4 of SCIP-216.

SCM-010040 [**Required: MG-TS – Optional: MG-LS, TA, IAD**] The SCIP/V.150.1 Gateway shall use the SSE protocol to transition between the Audio (native state) and MR modes of operation, per Section 4.4 of SCIP-216.

SCM-010050 [**Required: MG-TS – Optional: MG-LS, TA, IAD**] The SCIP/V.150.1 Gateway SSE state shall always start in the Audio mode, per Section 4.4.1 of SCIP-216.

SCM-010060 [**Required: MG-TS – Optional: MG-LS, TA, IAD**] The SCIP/V.150.1 Gateway shall meet all the requirements for "SSE Audio to Modem Relay Transitions" in Section 4.4.1 of SCIP-216.

SCM-010070 [**Required: MG-TS – Optional: MG-LS, TA, IAD**] The SCIP/V.150.1 Gateway shall meet all the requirements for "Procedures for SPRT Modem Relay Setup" in Section 4.4.2 of SCIP-216.

2.20.1.2.5 Modem-Based Session to Native Session Transition (Cleardown) Procedures

The following requirements are based on the "Modem-Based Session to Native Session Transition (Cleardown) Procedures" in Section 4.5 of SCIP-216.

SCM-010080 [**Required: MG-TS – Optional: MG-LS, TA, IAD**] The SCIP/V.150.1 Gateway shall meet all the requirements for "Procedures for PSTN Initiated Cleardown" in Section 4.5.1 of SCIP-216.

SCM-010090 [**Required: MG-TS – Optional: MG-LS, TA, IAD**] The SCIP/V.150.1 Gateway shall meet all the requirements for "Procedures for IP Initiated Cleardown" in Section 4.5.2 of SCIP-216.

2.20.1.2.6 Transition to On-Hook While in a Modem-Based Session

The following requirements are based on the "Transition to On-Hook While in a Modem-Based Session" in Section 4.6 of SCIP-216.

SCM-010100 [**Required: MG-TS – Optional: MG-LS, TA, IAD**] The SCIP/V.150.1 Gateway shall meet all the requirements for "Procedures for IP Initiated On-Hook" in Section 4.6.1 of SCIP-216.

SCM-010110 [**Required: MG-TS – Optional: MG-LS, TA, IAD**] The SCIP/V.150.1 Gateway shall meet all the requirements for "Procedures for PSTN Initiated On-Hook" in Section 4.6.2 of SCIP-216.

2.20.1.2.7 SPRT CLEARDOWN Procedures

SCM-010120 [**Optional: MG-TS, MG-LS, TA, IAD**] The SCIP/V.150.1 Gateway shall meet all the requirements for "SPRT CLEARDOWN Procedures" in Section 4.7 of SCIP-216.

2.20.1.2.8 Call Menu – Joint Menu Procedures

SCM-010130 [**Required: MG-TS – Optional: MG-LS, TA, IAD**] The SCIP/V.150.1 Gateway shall meet all the requirements for "Call Menu (CM) – Joint Menu (JM)" Procedures in Section 4.8 of SCIP-216.

2.20.1.2.9 NoAudio Payload Type Requirements for SCIP-216 Compliant Gateways

SCM-010140 [**Required: MG-TS – Optional: MG-LS, TA, IAD**] The SCIP/V.150.1 Gateway shall meet all the requirements for NoAudio Payload Type in Section 4.9 of SCIP-216.

SCM-010150 [**Required: MG-TS – Optional: MG-LS, TA, IAD**] The SCIP/V.150.1 Gateway shall support a NoAudio payload type for "Modem-Relay-Preferred" end points, per Section 4.9 of SCIP-216.

The SCIP-216 defines a "Modem-Relay-Preferred" end point as an SCIP-216 end point that immediately transitions to the Modem Relay state without transmitting information in the Audio state.

2.20.1.2.10 Transfer of Application Data Between the IP and DCE Interfaces

The following requirements are based on the "Transfer of Application Data between the IP and DCE Interfaces" requirements in Section 4.10 of SCIP-216.

SCM-010160 [**Optional: MG-TS, MG-LS, TA, IAD**] The SCIP/V.150.1 Gateway shall meet all the requirements for "Processing of Data Received on the DCE Interface" in Section 4.10.1 of SCIP-216. I_RAW-OCTET requirements in this section are optional.

SCM-010170 [**Required: MG-TS – Optional: MG-LS, TA, IAD**] The SCIP/V.150.1 Gateway shall support the formatting of data received from the DCE (modem) interface into the I_OCTET and I_OCTET-CS Modem Relay data types sent on the IP interface, according to Section 4.10.1 of SCIP-216.

SCM-010180 [**Optional: MG-TS – MG-LS, TA, IAD**] The SCIP/V.150.1 Gateway shall meet all the requirements for "Processing of Data Received on the IP Interface" in Section 4.10.2 of SCIP-216. I_RAW-OCTET requirements in this section are optional.

SCM-010190 [**Required: MG-TS – Optional: MG-LS, TA, IAD**] The SCIP/V.150.1 Gateway shall support the conversion of data received in the I_OCTET and I_OCTET-CS Modem Relay data types on the IP interface into asynchronous V.14 data characters sent on the DCE (modem) interface, according to Section 4.10.2 of SCIP-216.

SCM-010200 [**Required: MG-TS – Optional: MG-LS, TA, IAD**] The SCIP/V.150.1 Gateway shall meet all the requirements for "Lost Packet Processing with I_OCTET-CS" in Section 4.10.3 of SCIP-216.

2.20.1.3 SSE and SPRT Message Content

The following requirements are based on the "SSE and SPRT Message Content" requirements in Section 5 of SCIP-216.

2.20.1.3.1 SSE Messages

The following requirements are based on the "SSE Messages" requirements in Section 5.1 of SCIP-216.

SCM-010210 [**Required: MG-TS – Optional: MG-LS, TA, IAD**] The SCIP/V.150.1 Gateway shall meet all the requirements for the SSE Audio Message in Section 5.1.1 of SCIP-216.

SCM-010220 [**Required: MG-TS – Optional: MG-LS, TA, IAD**] The SCIP/V.150.1 Gateway shall meet all the requirements for the "SSE Modem Relay Message" in Section 5.1.2 of SCIP-216.

2.20.1.3.2 SPRT Messages

The following requirements are based on the "SPRT Messages" requirements in Section 5.2 of SCIP-216.

SCM-010230 [**Required: MG-TS – Optional: MG-LS, TA, IAD**] The SCIP/V.150.1 Gateway shall meet all the requirements for the "SPRT INIT Message" in Section 5.2.1 of SCIP-216.

SCM-010240 [**Required: MG-TS – Optional: MG-LS, TA, IAD**] The SCIP/V.150.1 Gateway shall meet all the requirements for the "SPRT JM_INFO Message" in Section 5.2.2 of SCIP-216.

SCM-010250 [**Required: MG-TS – Optional: MG-LS, TA, IAD**] The SCIP/V.150.1 Gateway shall meet all the requirements for the "SPRT CONNECT Message" in Section 5.2.3 of SCIP-216.

SCM-010260 [**Required: MG-TS – Optional: MG-LS, TA, IAD**] The SCIP/V.150.1 Gateway shall meet all the requirements for the "SPRT MR_EVENT Message" in Section 5.2.4 of SCIP-216.

SCM-010270 [**Required: MG-TS – Optional: MG-LS, TA, IAD**] The SCIP/V.150.1 Gateway shall meet all the requirements for the "SPRT CLEARDOWN Message" in Section 5.2.5 of SCIP-216.

NOTE: Transmission of this message is optional in SCIP-216, but reception of this message is required.

SCM-010280 [**Conditional: MG-TS, MG-LS, TA, IAD**] If the SPRT I_RAW-OCTET Message is supported, the SCIP/V.150.1 Gateway shall meet all the requirements for that Message in Section 5.2.6 of SCIP-216. (Support for the I_RAW-OCTET data type is currently optional in SCIP-216, but may become a requirement later.)

SCM-010290 [**Required: MG-TS – Optional: MG-LS, TA, IAD**] The SCIP/V.150.1 Gateway shall meet all the requirements for the SPRT I_OCTET Message in Section 5.2.7 of SCIP-216.

SCM-010300 [**Required: MG-TS – Optional: MG-LS, TA, IAD**] The SCIP/V.150.1 Gateway shall meet all the requirements for the SPRT I_OCTET-CS Message in Section 5.2.8 of SCIP-216.

2.20.1.4 Use of Common UDP Port Numbers for SRTP, SSE, and SPRT Messages

SCM-010310 [**Required: MG-TS – Optional: MG-LS, TA, IAD**] The SCIP/V.150.1 Gateway shall use the same UDP port numbers and protocol numbers for the following:

a. The SRTP media packets sent and received during the Audio mode (when the call is "in the clear").

b. The SSE media packets sent and received during transitions between the Audio and Modem Relay modes (when the call is moving between "in the clear" and "secure").

c. The SPRT media packets sent and received during the Modem Relay mode (when the call is "secure").

SCM-010320 [**Required: MG-TS – Optional: MG-LS, TA, IAD**] The UDP port numbers shall be the UDP port numbers negotiated by the SCIP/V.150.1 Gateway and the remote party (SCIP/V.150.1 EI or remote SCIP/V.150.1 Gateway) using SDP during AS-SIP session establishment.

SCM-010330 [**Required: MG-TS – Optional: MG-LS, TA, IAD**] The UDP protocol number (the protocol number used in IP packets to indicate that the UDP protocol is being transported) shall be protocol number 17, as registered with the Internet Assigned Numbers Authority

(IANA). Per the IANA Web site page on Assigned Internet Protocol Numbers (http://www.iana.org/assignments/protocol-numbers/):

"In the Internet Protocol version 4 (IPv4) [RFC 791] there is a field called "Protocol" to identify the next level protocol. This is an 8-bit field. In Internet Protocol version 6 (IPv6) [RFC 2460], this field is called the "Next Header" field."

SCM-010340 [**Required: MG-TS – Optional: MG-LS, TA, IAD**] When an SCIP/V.150.1 Gateway transitions the media stream between a normal session using SRTP and a secure session using SPRT, the SCIP/V.150.1 Gateway shall use the same UDP port numbers and UDP protocol number (17) for both the normal session and the secure session, so that the media stream transition is transparent to the SBC (when the SBC is located in the media stream for those sessions).

SCM-010350 [**Required: MG-TS – Optional: MG-LS, TA, IAD**] The SCIP/V.150.1 Gateway shall not use AS-SIP and SDP to negotiate a new UDP port number when the call is changing from audio mode (SRTP) and modem relay mode (SPRT), or from modem relay mode back to audio mode.

SCM-010360 [**Required: MG-TS – Optional: MG-LS, TA, IAD**] The SCIP/V.150.1 Gateway shall not use AS-SIP and SDP to negotiate multiple UDP port numbers (one for Audio (SRTP), another for mode transitions (SSE), and yet another for modem relay (SPRT)) during AS-SIP session establishment.

The SCIP-216 allows this multiple UDP port number approach, but the SCIP/V.150.1 Gateway shall not use this approach because it adds complexity to session establishment and has a negative effect on SBCs.

2.20.1.5 UDP Port Number for SRTCP Media Control Packets

SCM-010370 [**Required: MG-TS – Optional: MG-LS, TA, IAD**] The SCIP/V.150.1 Gateway shall maintain, for the duration of a call, the UDP port number used for the SRTCP media control packets that are sent and received during the Audio mode (when the call is "in the clear").

SCM-010380 [**Required: MG-TS – Optional: MG-LS, TA, IAD**] This UDP port number shall be the UDP port number negotiated for SRTCP media control packets by the SCIP/V.150.1 Gateway and the remote party (SCIP/V.150.1 EI or remote SCIP/V.150.1 Gateway) using SDP during AS-SIP session establishment.

SCM-010390 [**Required: MG-TS – Optional: MG-LS, TA, IAD**] When a call transitions from Audio mode to Modem Relay mode, the SCIP/V.150.1 Gateway shall stop sending SRTCP packets, but shall maintain the UDP port number that had been used for exchanging SRTCP packets.

SCM-010400 [**Required: MG-TS – Optional: MG-LS, TA, IAD**] If a call transitions from Audio mode to Modem Relay mode, and then later back to Audio mode, the SCIP/V.150.1 Gateway shall resume sending and receiving SRTCP packets using the same UDP port number that was previously used in Audio mode for those packets.

2.20.1.6 Use of V.150.1 SSE Messages for Media Transitions Between Audio and Modem Relay

SCM-010410 [**Required: MG-TS – Optional: MG-LS, TA, IAD**] Per Section 4, Information Assurance, SCIP/V.150.1 Gateways shall protect audio and video media streams using SRTP, when exchanging these media streams with SCIP/V.150.1 Phones and other SCIP/V.150.1 Gateways.

(When SCIP/V.150.1 Gateways exchange modem relay media streams with SCIP/V.150.1 Phones and other gateways, the modem relay media streams are sent over SPRT, and not sent over SRTP. As a result, these modem relay media streams are not protected by SRTP.)

SCM-010420 [**Required: MG-TS – Optional: MG-LS, TA, IAD**] When SCIP/V.150.1 Gateways exchange RFC 2833 Events and V.150.1 SSE messages with SCIP/V.150.1 Phones and other Gateways, these RFC 2833 Events and SSE messages shall also be protected using SRTP. These messages and events shall not be exchanged using SPRT, and they shall not be exchanged using RTP without SRTP.

SCM-010430 [**Required: MG-TS – Optional: MG-LS, TA, IAD**] For all IP-TDM and TDM-IP interworking calls, SCIP/V.150.1 Gateways shall declare that they support audio, modem relay, SRTP, SSE, and SPRT in the original SDP offer (AS-SIP INVITE message) and SDP answer (200 OK response) for each call. SCIP/V.150.1 Gateways shall not reserve or allocate a modem relay resource at this point because the call will typically begin as an audio call, which does not require a modem relay resource.

SCM-010440 [**Required: MG-TS – Optional: MG-LS, TA, IAD**] After one end of the call (the TDM SCIP phone or IP SCIP phone) decides to go secure, the SCIP/V.150.1 Gateway shall begin the process of changing the established media stream from audio media to modem relay media. On the IP portion of this call, the SCIP/V.150.1 Gateway shall begin this processing by exchanging SSE messages with the SCIP/V.150.1 Phone, SBC, or other SCIP/V.150.1 Gateway, per ITU-T Recommendation V.150.1 and SCIP-216.

SCM-010450 [**Required: MG-TS – Optional: MG-LS, TA, IAD**] As part of the Audio-media-to-Modem-Relay-media conversion process, the SCIP/V.150.1 Gateway shall not send an outgoing AS-SIP re-INVITE message that requests Audio-to-Modem-Relay media conversion.

SCM-010460 [**Required: MG-TS – Optional: MG-LS, TA, IAD**] As part of the Audio-media-to-Modem-Relay-media conversion process, the SCIP/V.150.1 Gateway shall not require the receipt of an incoming AS-SIP re-INVITE message that requests Audio-to-Modem-Relay media conversion.

SCM-010470 [**Required: MG-TS – Optional: MG-LS, TA, IAD**] The SCIP/V.150.1 Gateway shall not reserve and allocate one of its modem relay resources for the media stream for this call, until the SSE message exchange for Audio-to-Modem-Relay media conversion has begun.

SCM-010480 [**Required: MG-TS – Optional: MG-LS, TA, IAD**] After one end of the call (the TDM SCIP phone or IP SCIP phone) decides to return to "voice in the clear," the SCIP/V.150.1 Gateway shall begin the process of changing the established media stream from modem relay media to Audio media. On the IP portion of this call, the SCIP/V.150.1 Gateway shall begin this processing by exchanging SSE messages with the SCIP/V.150.1 Phone, SBC, or other SCIP/V.150.1 Gateway, per ITU-T Recommendation V.150.1 and SCIP-216.

SCM-010490 [**Required: MG-TS – Optional: MG-LS, TA, IAD**] As part of the Modem-Relay-media-to-Audio-media conversion process, the SCIP/V.150.1 Gateway shall not send an outgoing AS-SIP re-INVITE message that requests Modem-Relay-to-Audio media conversion.

SCM-010500 [**Required: MG-TS – Optional: MG-LS, TA, IAD**] As part of the Modem-Relay-media-to-Audio-media conversion process, the SCIP/V.150.1 Gateway shall not require the receipt of an incoming AS-SIP re-INVITE message that requests Modem-Relay-to-Audio-media conversion.

SCM-010510 [**Required: MG-TS – Optional: MG-LS, TA, IAD**] The SCIP/V.150.1 Gateway shall not release and de-allocate its modem relay resource for the media stream for this call until the SSE message exchange for Modem-Relay-to-Audio media conversion has begun.

SCM-010520 [**Required: MG-TS – Optional: MG-LS, TA, IAD**] The SCIP/V.150.1 Gateways shall still be able to send and receive AS-SIP re-INVITE messages during an audio call. (For example, the gateway can use the AS-SIP re-INVITE message to request an Audio codec change during the audio/clear voice portion of a call, when the Gateway is using G.711 for audio media but then asks the far end to use G.729 for Audio media instead.) When the Gateway includes modem relay media information in an AS-SIP re-INVITE message, the Gateway shall make sure that this is the same modem relay information that was present in the initial AS-SIP INVITE message or 200 OK response that established the call. In this way, the AS-SIP re-INVITE message is not used to request an Audio-to-Modem-Relay transition.

2.20.1.7 Modem Relay and VoIP for SCIP/V.150.1 Gateways

SCM-010530 [**Required: MG-TS – Optional: MG-LS, TA, IAD**] When an SCIP/V.150.1 Gateway is unable to provide modem relay on an MoIP call (e.g., because the remote end is not modem relay capable, or the remote end is modem relay capable but does not currently have any modem relay resources available), then the SCIP/V.150.1 Gateway shall instead provide VoIP treatment for that call. In this case, the SCIP/V.150.1 Gateway shall handle the MoIP call in the SC or SS in the same way that it would handle a G.711 VoIP call in the SC or SS, with these clarifications:

a. The Gateway shall still disable EC for the MoIP call being handled as a G.711 VoIP call, when the Gateway detects an "EC disabling" tone from either the TDM side or the MoIP side of the call (see Section 2.16.9, MG Requirements for Echo Cancellation).

b. The Gateway may disable silence suppression on the MoIP side of the call.

SCM-010540 [**Conditional: MG-TS – Optional: MG-LS, TA, IAD**] If the Gateway also supports Voiceband Data codecs (proprietary and/or V.152) then the Gateway is allowed to provide VBD treatment for the MoIP call instead of providing VoIP treatment for that call.

NOTE: End-to-end synchronization of the calling and called modems (or modem-equipped SCIP phones) is not guaranteed on a VoIP call. Even though a VoIP call may complete between these two modems (i.e., a successful AS-SIP signaling INVITE/200 OK/ACK exchange can occur, and G.711 media can be exchanged over SRTP, UDP, and IP), there is no guarantee that the two modems will be able to synchronize and exchange data using the resulting G.711 media streams. Even if the two modems do synchronize and exchange data, there is no guarantee that this synchronization and exchange will be maintained over time, or that the synchronization and exchange will result in a data throughput that matches what would be provided by a modem relay call, or by an E2E TDM call in a TDM voice network.

Because of this, there are no requirements in this section for the reliability of modem synchronization, reliability of data exchange, or rate of data transfer on VoIP calls. It is expected that these calls will complete using AS-SIP signaling and SRTP media exchange like VoIP calls do. But it is not expected that the resulting synchronization and data exchange will be 100 percent reliable, or that the data rate provided will match what would be provided on a modem relay call or TDM modem call under the same conditions.

SCM-010550 [**Required: MG-TS**] The SCIP/V.150.1 Gateway shall support adequate V.150.1/SCIP-216 modem relay resources so that 10 percent of the maximum number of calls that can pass through the trunk-side interfaces of the MG (from TDM end points to IP end points, and from IP end points to TDM end points) can receive modem relay treatment, instead of receiving VoIP treatment.

NOTE: The acquiring activity for the SCIP/V.150.1 Gateway should also determine, based on traffic engineering and vendor prices, the required number of MG modem relay resources (e.g., Modem-Relay-equipped trunk cards, or modem relay DSP cards) that will support V.150.1/SCIP-216 modem relay. V.150.1/SCIP-216 modem relay is needed to support IP SCIP phones (SCIP-215 phones) on an SC or SS, and analog SCIP phones behind TAs, IADs, and MG line cards on an SC or SS.

2.20.1.8 Modem Relay Support for V.92 and V.90 Modulation Types

SCM-010560 [**Required: MG-TS**] On SCIP-216 modem relay calls where the V.92 Digital modulation type (UCR Required) is used, the TDM side of the MG-TS shall act as the digital interface to the remote V.92 Server modem.

SCM-010570 [**Conditional: MG-LS, TA, IAD**] If V.92 Analog modulation type (UCR Optional) is used on an SCIP-216 modem relay call, then the TDM side of the MG-LS, TA, or IAD shall act as the analog interface to the local V.92 client modem (e.g., a V.92 modem on an RJ-11 port on a DoD laptop computer).

SCM-010580 [**Required: MG-TS – Optional: MG-LS, TA, IAD**] The SCIP-216 modem relay communication between the MG-TS and the MG-LS, TA, or IAD shall support V.92-Server-modem-to-V.92-Client-modem communication in the MG-TS-to-MG-LS/IAD/TA direction, and V.92-Client-modem-to-V.92-Server-modem communication in the MG-LS/IAD/TA-to-MG-TS direction.

SCM-010590 [**Required: MG-TS – Optional: MG-LS, TA, IAD**] The data rate supported in the V.92-Server-modem-to-V.92-Client-modem direction shall be greater than 33.6 Kbps and less than 53.3 Kbps (the U.S. PSTN limit on 56 Kbps data communication). The data rate supported in the V.92-Client-modem-to-V.92-Server-modem direction shall be greater than 33.6 Kbps and less than 53.3 Kbps also.

SCM-010600 [**Required: MG-TS**] On SCIP-216 modem relay calls where the V.90 digital modulation type (UCR Required) is used, the TDM side of the MG-TS shall act as the digital interface to the remote V.90 server modem.

SCM-010610 [**Conditional: MG-LS, TA, IAD**] On SCIP-216 modem relay calls where the V.90 analog modulation type (UCR Optional) is used, the TDM side of the MG-LS, TA, or IAD shall act as the analog interface to the local V.90 client modem (e.g., a V.90 modem on an RJ-11 port on a DoD laptop computer).

SCM-010620 [**Required: MG-TS – Optional: MG-LS, TA, IAD**] The SCIP-216 modem relay communication between the MG-TS and the MG-LS, TA, or IAD shall support V.90-Server-modem-to-V.90-Client-modem communication in the MG-TS-to-MG-LS/IAD/TA direction, and V.90-Client-modem-to-V.90-Server-modem communication in the MG-LS/IAD/TA-to-MG-TS direction.

SCM-010630 [**Required: MG-TS – Optional: MG-LS, TA, IAD**] The data rate supported in the V.90-Server-modem-to-V.90-Client-modem direction shall be greater than 33.6 Kbps and less than 53.3 Kbps (the U.S. PSTN limit on 56 Kbps data communication). The data rate supported in the V.90-Client-modem-to-V.90-Server-modem direction shall be greater than 28.8 Kbps and less than or equal to 33.6 Kbps.

2.20.1.9 Going Secure, Glare Conditions, and Modem Relay Preferred Devices

SCM-010640 [**Required: MG-TS – Optional: MG-LS, TA, IAD**] The calling or called SCIP/V.150.1 Gateway shall be able to initiate going secure. The calling or called SCIP/V.150.1 Gateway shall be able to send an answer message (ANS) signal toward the far-end SCIP endpoint (MG or EI).

SCM-010650 [**Required: MG-TS – Optional: MG-LS, TA, IAD**] If a glare condition results from an SCIP/V.150.1 Gateway initiating going secure and sending an ANS signal toward the far-end SCIP endpoint (MG or EI) at the same time that the far endpoint initiates going secure and sends an ANS signal to the SCIP/V.150.1 Gateway, then the SCIP/V.150.1 Gateway and the far end SCIP endpoint both shall back off their request and try again later.

SCM-010660 [**Required: MG-TS – Optional: MG-LS, TA, IAD**] An SCIP/V.150.1 Gateway operating as an SCIP Modem Relay Preferred (MRP) device shall transition automatically from the audio state to the modem relay state upon the SCIP call being answered. This means that the first media stream packet sent by the MRP device shall be a Secure RTP (SRTP) packet containing an IETF RFC 2833 message indicating that an ANS, /ANS, ANSam, or /ANSam Event is being signaled.

2.20.2 SCIP/V.150.1 EI

This section contains the SCIP/V.150.1 EI requirements for UCR, based on the NSA document: SCIP-215, Revision 2.1. All references to "SCIP-215" in the following paragraphs are references to SCIP-215, Revision 2.1.

A "SCIP/V.150.1 EI" is a Secure IP Phone that conforms to SCIP-215, conforms to the requirements in this section, and is served by an SC.

A SCIP/V.150.1 EI also communicates with the SC using one of the following:

- Vendor-proprietary signaling and transport protocols.
- AS-SIP signaling over TLS.

A SCIP/V.150.1 EI also exchanges media with other EIs, MGs, ATAs, and IADs using SRTP over UDP during the audio part of the call ("talking in the clear"), and using SSE and SPRT over UDP during the modem relay part of the call ("talking secure").

The following SCIP/V.150.1 EI requirements apply to both SCIP/V.150.1 EIs in Strategic (Fixed) Networks, and to SCIP/V.150.1 EIs in Tactical (Deployable) networks.

2.20.2.1 Basic Minimum Essential Requirements (MERs)

The following requirements are based on the basic MER in Section 4 of SCIP-215.

2.20.2.1.1 IP Transport Layer Protocol

SCM-010670 [**Required: SCIP/V.150.1 EI**] The SCIP/V.150.1 EI shall meet all the requirements for "IP Transport Layer Protocol" in Section 4.1 of SCIP-215.

2.20.2.1.2 V.150.1 Operational Mode

SCM-010680 [**Required: SCIP/V.150.1 EI**] The SCIP/V.150.1 EI shall meet all the requirements for "V.150.1 Operational Mode" in Section 4.2 of SCIP-215.

2.20.2.1.3 Modem-Relay Gateway Type

SCM-010690 [**Required: SCIP/V.150.1 EI**] The SCIP/V.150.1 EI shall meet all the requirements for "Modem-Relay Gateway Type" in Section 4.3 of SCIP-215.

2.20.2.1.4 Simple Packet Relay Transport

The following requirements are based on the SPRT requirements in Section 4.4 of SCIP-215.

SCM-010700 [**Required: SCIP/V.150.1 EI**] The SCIP/V.150.1 EI shall meet all the requirements for "Transport Channel" in Section 4.4.1 of SCIP-215.

SCM-010710 [**Required: SCIP/V.150.1 EI**] The SCIP/V.150.1 EI shall meet all the requirements for "SPRT Modem Relay Messages" in Section 4.4.2 of SCIP-215.

SCM-010720 [**Required: SCIP/V.150.1 EI**] The SCIP/V.150.1 EI shall meet all the requirements for "SPRT Timer" in Section 4.4.3 of SCIP-215.

2.20.2.1.5 SSE

The following requirements are based on the SSE requirements in Section 4.5 of SCIP-215.

SCM-010730 [**Required: SCIP/V.150.1 EI**] The SCIP/V.150.1 EI shall meet all the requirements for "SSE Call Discrimination Messages" in Section 4.5.1 of SCIP-215.

SCM-010740 [**Required: SCIP/V.150.1 EI**] The SCIP/V.150.1 EI shall meet all the requirements for "SSE Reliability" in Section 4.5.2 of SCIP-215.

SCM-010750 [**Required: SCIP/V.150.1 EI**] The SCIP/V.150.1 EI shall meet all the requirements for "SSE Reason Identifier Code" in Section 4.5.3 of SCIP-215.

SCM-010760 [**Required: SCIP/V.150.1 EI**] The SCIP/V.150.1 EI shall meet all the requirements for "SSE Timer" in Section 4.5.4 of SCIP-215.

2.20.2.1.6 Call Setup Protocol

The following requirements are based on the "Call Setup Protocol Requirements for Negotiating Specific V.150.1 Capabilities" in Section 4.6 of SCIP-215.

SCM-010770 [**Required: SCIP/V.150.1 EI**] The SCIP/V.150.1 EI shall meet all the requirements for "V.150.1 Version Declaration" in Section 4.6.1 of SCIP-215.

SCM-010780 [**Required: SCIP/V.150.1 EI**] The SCIP/V.150.1 EI shall meet all the requirements for "Transcompression Capability" in Section 4.6.2 of SCIP-215.

SCM-010790 [**Required: SCIP/V.150.1 EI**] The SCIP/V.150.1 EI shall meet all the requirements for "Modem Relay Type Declaration" in Section 4.6.3 of SCIP-215.

SCM-010800 [**Required: SCIP/V.150.1 EI**] The SCIP/V.150.1 EI shall meet all the requirements for "Modulation Support Indication" in Section 4.6.4 of SCIP-215.

SCM-010810 [**Required: SCIP/V.150.1 EI**] The SCIP/V.150.1 EI shall meet all the requirements for "RFC 2833 Events" in Section 4.6.5 of SCIP-215.

SCM-010820 [**Optional: SCIP/V.150.1 EI**] The SCIP/V.150.1 EI shall meet all the requirements for "SPRT Payload and Window Size Parameter" in Section 4.6.6 of SCIP-215.

SCM-010830 [**Required: SCIP/V.150.1 EI**] The SCIP/V.150.1 EI shall meet all the requirements for "JM Delay Support" in Section 4.6.7 of SCIP-215.

SCM-010840 [**Required: SCIP/V.150.1 EI**] The SCIP/V.150.1 EI shall meet all the requirements for "Call Discrimination Mode Parameter" in Section 4.6.8 of SCIP-215.

SCM-010850 [**Required: SCIP/V.150.1 EI**] The SCIP/V.150.1 EI shall meet all the requirements for "SSE Capability Indication" in Section 4.6.9 of SCIP-215.

SCM-010860 [**Required: SCIP/V.150.1 EI**] The SCIP/V.150.1 EI shall meet all the requirements for "SPRT Protocol Support Parameters" in Section 4.6.10 of SCIP-215.

SCM-010870 [**Required: SCIP/V.150.1 EI**] The SCIP/V.150.1 EI shall meet all the requirements for "NoAudio Support" in Section 4.6.11 of SCIP-215.

2.20.2.1.7 SCIP Operational Mode

SCM-010880 [**Required: SCIP/V.150.1 EI**] The SCIP/V.150.1 EI shall meet all the requirements for "SCIP Operational Mode" in Section 4.7 of SCIP-215.

2.20.2.1.8 V.14

SCM-010890 [**Optional: SCIP/V.150.1 EI**] The SCIP/V.150.1 EI shall meet all the requirements for "V.14" in Section 4.8 of SCIP-215.

2.20.2.2 Procedural MER

The following requirements are based on the Procedural MER in Section 5 of SCIP-215.

2.20.2.2.1 SSE State Transition

SCM-010900 [**Required: SCIP/V.150.1 EI**] The SCIP/V.150.1 EI shall meet all the requirements for "SSE State Transition" in Section 5.1 of SCIP-215.

2.20.2.2.2 SPRT Procedures

The following requirements are based on the "SPRT Procedures Requirements" in Section 5.2 of SCIP-215.

SCM-010910 [**Optional: SCIP/V.150.1 EI**] The SCIP/V.150.1 EI shall meet all the requirements for modem relay "Data Type Selection" in Section 5.2.1 of SCIP-215. The I_RAW-OCTET requirements in this section are conditional.

SCM-010920 [**Required: SCIP/V.150.1 EI**] The SCIP/V.150.1 EI shall meet all the requirements for "SPRT Message Ordering" in Section 5.2.2 of SCIP-215.

SCM-010930 [**Optional: SCIP/V.150.1 EI**] The SCIP/V.150.1 EI shall meet all the requirements for "SPRT Window and Payload Size Negotiation" in Section 5.2.3 of SCIP-215.

SCM-010940 [**Required: SCIP/V.150.1 EI**] The SCIP/V.150.1 EI shall meet all the requirements for "SPRT Data Signaling Rate Indication" in Section 5.2.4 of SCIP-215.

2.20.2.2.3 RFC 2833 Event Transmission Procedures

SCM-010950 [**Required: SCIP/V.150.1 EI**] The SCIP/V.150.1 EI shall meet all the requirements for "RFC 2833 Event Transmission Procedures" in Section 5.3 of SCIP-215.

2.20.2.2.4 Clear-to-SCIP Traffic Transition Procedures

The following requirements are based on the "Clear-to-SCIP Traffic Transition Procedures" in Section 5.4 of SCIP-215.

SCM-010960 [**Required: SCIP/V.150.1 EI**] The SCIP/V.150.1 EI shall meet all the requirements for SSE Audio to modem relay Transitions in Section 5.4.1 of SCIP-215.

SCM-010970 [**Required: SCIP/V.150.1 EI**] The SCIP/V.150.1 EI shall meet all the requirements for Procedures for SPRT modem relay Setup in Section 5.4.2 of SCIP-215.

2.20.2.2.5 SCIP Traffic-to-Clear Transition (Cleardown) Procedures

The following requirements are based on the "SCIP Traffic-to-Clear Transition (Cleardown) Procedures" in Section 5.5 of SCIP-215.

SCM-010980 [**Required: SC**IP/V.150.1 EI] The SCIP/V.150.1 EI shall meet all the requirements for "Procedures for PSTN Initiated Cleardown" in Section 5.5.1 of SCIP-215.

SCM-010990 [**Required: SC**IP/V.150.1 EI] The SCIP/V.150.1 EI shall meet all the requirements for "Procedures for IP Initiated Cleardown" in Section 5.5.2 of SCIP-215.

2.20.2.2.6 Transition to On-Hook While in a Modem-Based Session

The following requirements are based on the "Transition to On-Hook While Exchanging SCIP Information" requirements in Section 5.6 of SCIP-215.

SCM-011000 [**Required: SCIP/V.150.1 EI**] The SCIP/V.150.1 EI shall meet all the requirements for Procedures for IP Initiated On-hook in Section 5.6.1 of SCIP-215.

SCM-011010 [**Required: SCIP/V.150.1 EI**] The SCIP/V.150.1 EI shall meet all the requirements for "Procedures for PSTN Initiated On-Hook" in Section 5.6.2 of SCIP-215.

2.20.2.2.7 SPRT CLEARDOWN Procedures

SCM-011020 [**Optional: SCIP/V.150.1 EI**] The SCIP/V.150.1 EI shall meet all the requirements for "SPRT CLEARDOWN Procedures" in Section 5.7 of SCIP-215.

2.20.2.2.8 Call Menu (CM) – Joint Menu (JM) Procedures

SCM-011030 [**Required: SCIP/V.150.1 EI**] The SCIP/V.150.1 EI shall meet all the requirements for "Call Menu (CM) – Joint Menu (JM) Procedures" in Section 5.8 of SCIP-215.

2.20.2.2.9 Use of the NoAudio Payload Type by "Modem Relay-Preferred" Terminals

SCM-011040 [**Required: SCIP/V.150.1 EI**] The SCIP/V.150.1 EI shall meet all the requirements for "Use of the NoAudio Payload Type By 'Modem Relay-Preferred' Terminals" in Section 5.9 of SCIP-215.

2.20.2.2.10 Bandwidth Negotiation

SCM-011050 [**Required: SCIP/V.150.1 EI**] The SCIP/V.150.1 EI shall meet all the requirements for "Bandwidth Negotiation" in Section 5.10 of SCIP-215.

2.20.2.3 SSE and SPRT Message Content

The following requirements are based on the "SSE and SPRT Message Content" requirements in Section 6 of SCIP-215.

2.20.2.3.1 SSE Messages

The following requirements are based on the "SSE Messages" requirements in Section 6.1 of SCIP-215.

SCM-011060 [**Required: SCIP/V.150.1 EI**] The SCIP/V.150.1 EI shall meet all the requirements for the "SSE Audio Message" in Section 6.1.1 of SCIP-215.

SCM-011070 [**Required: SCIP/V.150.1 EI**] The SCIP/V.150.1 EI shall meet all the requirements for the "SSE modem relay Message" in Section 6.1.2 of SCIP-215.

2.20.2.3.2 SPRT Messages

The following requirements are based on the "SPRT Messages" requirements in Section 6.2 of SCIP-215.

SCM-011080 [**Required: SCIP/V.150.1 EI**] The SCIP/V.150.1 EI shall meet all the requirements for the "SPRT INIT Message" in Section 6.2.1 of SCIP-215.

SCM-011090 [**Required: SCIP/V.150.1 EI**] The SCIP/V.150.1 EI shall meet all the requirements for the "SPRT JM_INFO Message" in Section 6.2.2 of SCIP-215.

SCM-011100 [**Required: SCIP/V.150.1 EI**] The SCIP/V.150.1 EI shall meet all the requirements for the "SPRT CONNECT Message" in Section 6.2.3 of SCIP-215.

SCM-011110 [**Required: SCIP/V.150.1 EI**] The SCIP/V.150.1 EI shall meet all the requirements for the "SPRT MR_EVENT" message in Section 6.2.4 of SCIP-215.

SCM-011120 [**Required: SCIP/V.150.1 EI**] The SCIP/V.150.1 EI shall meet all the requirements for the "SPRT CLEARDOWN" message in Section 6.2.5 of SCIP-215.

NOTE: Transmission of this message is optional in SCIP-215, but reception of this message is required.

SCM-011130 [**Conditional: SCIP/V.150.1 EI**] If the SPRT I_RAW-OCTET message is supported (UCR Optional), the SCIP/V.150.1 EI shall meet all the requirements for that message in Section 6.2.6 of SCIP-215.

SCM-011140 [**Required: SCIP/V.150.1 EI**] The SCIP/V.150.1 EI shall meet all the requirements for the "SPRT I_OCTET" message in Section 6.2.7 of SCIP-215.

SCM-011150 [**Required: SCIP/V.150.1 EI**] The SCIP/V.150.1 EI shall meet all the requirements for the "SPRT I_OCTET-CS" message in Section 6.2.8 of SCIP-215.

2.20.2.4 Use of Common UDP Port Numbers for SRTP, SSE, and SPRT Messages

SCM-011160 [**Required: SCIP/V.150.1 EI**] The SCIP/V.150.1 EI shall use the same UDP port and protocol numbers for SRTP media packets sent and received during the Audio mode (when the call is "in the clear"), SSE media packets sent and received during transitions between the Audio and modem relay modes (when the call is moving between "in the clear" and "secure"), and SPRT media packets sent and received during the modem relay mode (when the call is "secure").

SCM-011170 [**Required: SCIP/V.150.1 EI**] The UDP port numbers shall be the UDP port numbers negotiated by the SCIP/V.150.1 EI and the remote party (SCIP/V.150.1 Gateway or other SCIP/V.150.1 EI) using SDP during AS-SIP session establishment.

SCM-011180 [**Required: SCIP/V.150.1 EI**] The UDP protocol number (the protocol number used in IP packets to indicate that UDP protocol is being transported) shall be protocol number 17, as registered with Internet Assigned Numbers Authority (IANA).

SCM-011190 [**Required: SCIP/V.150.1 EI**] When an SCIP/V.150.1 EI transitions the media stream between a normal session using SRTP and a secure session using SPRT, the SCIP/V.150.1 EI shall use the same UDP port numbers and UDP protocol number (17) for both the normal session and the secure session, so that the media stream transition is transparent to the SBC (when the SBC is located in the media stream for those sessions).

SCM-011200 [**Required: SCIP/V.150.1 EI**] The SCIP/V.150.1 EI shall not use AS-SIP and SDP to negotiate a new UDP port number when the call is changing from Audio mode (SRTP) and Modem Relay mode (SPRT), or from Modem Relay mode back to Audio mode.

SCM-011210 [**Required: SCIP/V.150.1 EI**] The SCIP/V.150.1 EI shall not use AS-SIP and SDP to negotiate multiple UDP port numbers (one for audio (SRTP), another for mode transitions (SSE), and another for modem relay (SPRT)) during AS-SIP session establishment.

The SCIP-215 allows this multiple UDP port number approach, but the SCIP/V.150.1 EI shall not use this approach because it adds complexity to session establishment, and has a negative effect on SBCs.

2.20.2.5 UDP Port Number for SRTCP Media Control Packets

SCM-011220 [**Required: SCIP/V.150.1 EI**] The SCIP/V.150.1 EI shall maintain, for the duration of a call, the UDP port number used for the SRTCP media control packets that are sent and received during the Audio mode (when the call is "in the clear").

SCM-011230 This UDP port number shall be the UDP port number negotiated for SRTCP media control packets by the SCIP/V.150.1 EI and the remote party (SCIP/V.150.1 EI or remote SCIP/V.150.1 Gateway) using SDP during AS-SIP session establishment.

SCM-011240 [**Required: SCIP/V.150.1 EI**] When a call transitions from Audio mode to Modem Relay mode, the SCIP/V.150.1 EI shall stop sending SRTCP packets, but maintain the UDP port number that had been used for exchanging SRTCP packets.

SCM-011250 [**Required: SCIP/V.150.1 EI**] If a call transitions from Audio mode to Modem Relay mode, and then later back to the Audio mode, the SCIP/V.150.1 EI shall resume sending and receiving SRTCP packets using the same UDP port number previously used in Audio mode for those packets.

2.20.2.6 Use of V.150.1 SSE Messages for Media Transitions Between Audio and Modem Relay

SCM-011260 [**Required: SCIP/V.150.1 EI**] Per Section 4, Information Assurance, SCIP/V.150.1 EIs shall protect audio and video media streams using SRTP when exchanging these media streams with SCIP/V.150.1 Gateways and other SCIP/V.150.1 EIs.

NOTE: When SCIP/V.150.1 EIs exchange modem relay media streams with SCIP/V.150.1 Gateways and other EIs, the modem relay media streams are sent over SPRT, and not sent over SRTP. As a result, these modem relay media streams are not protected by SRTP.

SCM-011270 [**Required: SCIP/V.150.1 EI**] When SCIP/V.150.1 EIs exchange RFC 2833 events and V.150.1 SSE messages with SCIP/V.150.1 Gateways and other EIs, these RFC 2833 events and SSE messages shall also be protected using SRTP. These messages and events shall not be exchanged using SPRT, and they shall not be exchanged using RTP without SRTP.

SCM-011280 [**Required: SCIP/V.150.1 EI**] For all IP-TDM interworking, TDM-IP interworking, and IP-IP calls, SCIP/V.150.1 EIs shall declare that they support audio, modem relay, SRTP, SSE, and SPRT in the original SDP offer (AS-SIP INVITE message) and SDP answer (200 OK response) for each call. The SCIP/V.150.1 EIs shall not reserve any modem relay resource at this point, because the call will typically begin as an audio call, which does not require a modem relay resource.

SCM-011290 [**Required: SCIP/V.150.1 EI**] Once one end of the call decides to go secure, the SCIP/V.150.1 EI shall begin the process of changing the established media stream from audio media to modem relay media. The SCIP/V.150.1 EI shall begin this processing by exchanging SSE messages with the SCIP/V.150.1 Gateway or other SCIP/V.150.1 EI, per V.150.1 and SCIP-215.

SCM-011300 [**Required: SCIP/V.150.1 EI**] As part of the Audio-media-to-Modem-Relay-media conversion process, the SCIP/V.150.1 EI shall not send an outgoing AS-SIP re-INVITE message that requests Audio-to-Modem-Relay media conversion.

SCM-011310 [**Required: SCIP/V.150.1 EI**] As part of the Audio-media-to-modem-relay-media conversion process, the SCIP/V.150.1 EI shall not require the receipt of an incoming AS-SIP re-INVITE message that requests Audio-to-Modem-Relay media conversion.

SCM-011320 [**Required: SCIP/V.150.1 EI**] The SCIP/V.150.1 EI shall not reserve and allocate its modem relay resources for the media stream for this call until the SSE message exchange for Audio-to-Modem-Relay media conversion has begun.

SCM-011330 [**Required: SCIP/V.150.1 EI**] Once one end of the call decides to return to "voice in the clear," the SCIP/V.150.1 EI shall begin the process of changing the established media stream from modem relay media to audio media. The SCIP/V.150.1 EI shall begin this processing by exchanging SSE messages with the SCIP/V.150.1 Gateway or other SCIP/V.150.1 EI, per V.150.1 and SCIP-215.

SCM-011340 [**Required: SCIP/V.150.1 EI**] As part of the Modem-Relay-media-to-Audio-media conversion process, the SCIP/V.150.1 EI shall not send an outgoing AS-SIP re-INVITE message that requests Modem-Relay-to-Audio media conversion.

SCM-011350 [**Required: SCIP/V.150.1 EI**] As part of the Modem-Relay-media-to-Audio-media conversion process, the SCIP/V.150.1 EI shall not require the receipt of an incoming AS-SIP re-INVITE message that requests Modem-Relay-to-Audio media conversion.

SCM-011360 [**Required: SCIP/V.150.1 EI**] The SCIP/V.150.1 EI shall not release and de-allocate its modem relay resource for the media stream for this call, until the SSE message exchange for Modem-Relay-to-Audio media conversion has begun.

SCM-011370 [**Required: SCIP/V.150.1 EI**] The SCIP/V.150.1 EIs shall still be able to send and receive AS-SIP re-INVITE messages during an audio call. (For example, the EI can use the AS-SIP re-INVITE message to request an audio codec change during the audio/clear voice portion of a call when the EI is using G.711 for audio media but then asks the far end to use G.729 for audio media instead.) When the EI includes modem relay media information in an AS-SIP re-INVITE message, the EI shall make sure that this is the same modem relay information that was present in the initial AS-SIP INVITE message or 200 (OK) response that established the call. In this way, the AS-SIP re-INVITE message is not used to request an Audio-to-Modem-Relay transition.

2.20.2.7 Going Secure, Glare Conditions, and Modem Relay Preferred Devices

SCM-011380 [**Required: SCIP/V.150.1 EI**] The calling or called SCIP/V.150.1 EI shall be able to initiate going secure. The calling or called SCIP/V.150.1 EI shall be able to send an ANS signal towards the far-end SCIP endpoint (MG or EI).

SCM-011390 [**Required: SCIP/V.150.1 EI**] If a glare condition results from an SCIP/V.150.1 EI initiating going secure and sending an ANS signal toward the far-end SCIP endpoint (MG or EI) at the same time that the far endpoint initiates going secure and sending an ANS signal to the SCIP/V.150.1 EI, then the SCIP/V.150.1 EI and the far-end SCIP endpoint should both back off their request and try again later.

SCM-011400 [**Required: SCIP/V.150.1 EI**] An SCIP/V.150.1 EI operating as an SCIP MRP device shall automatically transition from the audio state to the modem relay state upon the SCIP call being answered. This means that the first media stream packet sent by the MRP device shall be a Secure RTP (SRTP) packet containing an IETF RFC 2833 message indicating that an ANS, /ANS, ANSam, or /ANSam Event is being signaled.

This also means that the first media stream packet received by the MRP device (i.e., sent to the MRP device by the other V.150.1 device on the call) shall be an SRTP packet containing an SSE message indicating a transition from audio to modem relay (Event Code 3). Once this transition is successful, the MRP device shall begin sending SPRT packets containing SCIP protocol information (secure voice or secure data media).

If the MRP device receives an RFC 233 message containing an ANS, /ANS, ANSam, or /ANSam Event before that device sends its own RFC 2833 message and ANS, /ANS, ANSam, or /ANSam Event, the MRP device shall send an SRTP packet back to the other V.150.1 device, containing an SSE message indicating a transition from audio to modem relay (Event Code 3). Once this transition is successful, the MRP device shall begin sending SPRT packets containing SCIP protocol information (secure voice or secure data media).

2.20.3 SCIP/V.150.1 EI Requirements Using SCIP-214.2 Protocol

It is also possible for two SCIP/V.150.1 EIs to communicate with one another over the UC VVoIP network using the SCIP-214.2 protocol, as defined in the NSA document SCIP 214.2, Secure Communication Interoperability Protocol (SCIP) over Real-Time Transport Protocol (RTP), Revision 1.0, January 2010.

Unlike SCIP-216 and SCIP-215, SCIP-214.2 does not use V.150.1 Modem Relay, SPRT, or SSE to exchange media over a VVoIP network. Instead, the SCIP media stream packets are sent from one EI to another over the VVoIP network, and do not traverse any SCIP/V.150.1 Gateways (MG-TS, MG-LS, ATAs, or IADs).

Support for SCIP/V.150.1 EIs using SCIP-214.2 is Optional. If SCIP-214.2 is supported then the following conditional requirements must be met.

SCM-011410 [**Conditional: SCIP/V.150.1 EI**] If the SCIP/V.150.1 EI supports secure communication using SCIP over Secure RTP, the SCIP/V.150.1 EI shall support all of the mandatory requirements in NSA document SCIP 214.2 with the following qualification:

a. SCIP 214.2 allows RTP to be used as the media transport protocol for the two EIs. Since UC uses Secure RTP (SRTP) as the media transport protocol instead of RTP, SCIP/V.150.1 EIs shall also use SRTP as the media transport protocol, when exchanging SCIP media with another using SCIP-214.2. In other words, SCIP/V.150.1 EIs shall support SCIP over RTP per SCIP-214.2, except that SRTP shall be used to carry SCIP instead of RTP.

SCM-011420 [**Conditional: SCIP/V.150.1 EI**] The SCIP/V.150.1 EI shall use the payload type of "scip" in SDP attachments in AS-SIP signaling to indicate that it supports SCIP over SRTP media using SCIP-214.2.

SCM-011430 [**Conditional: SCIP/V.150.1 EI**] Consistent with SCIP-214.2, the SCIP/V.150.1 EI shall "go secure" when one of the following conditions is met:

a. When the two EIs negotiate the "scip" payload type to be the only selected codec.

b. When the two EIs negotiate the "scip" payload type to be one of several selected codecs, and the first RTP packet with payload type "scip" is received from the other EI.

SCM-011440 [**Conditional: SCIP/V.150.1 EI**] Consistent with SCIP-216 and SCIP-215 requirements preventing the use of AS-SIP re-INVITE or UPDATE messages for "clear voice" to "secure voice" transitions, the SCIP/V.150.1 EI shall not use AS-SIP re-INVITE or UPDATE messages to perform "clear voice" to "secure voice" transitions, or to perform "secure voice" to "clear voice" transitions. The SCIP/V.150.1 EIs shall use the media stream methods defined in SCIP-214.2 to perform these transitions, and shall not use AS-SIP signaling messages for this purpose.

As a result, SCIP/V.150.1 EIs that support SCIP-214.2 shall declare support for the "scip" payload type in the first AS-SIP message in the SDP Offer-Answer exchange (e.g., in the INVITE message or in the 180 (Ringing) response).

SCM-011450 [**Conditional: SCIP/V.150.1 EI**] The SCIP/V.150.1 EIs shall use the following:

a. One UDP port number for SRTP media packets for both "clear voice" and "secure voice."

b. A separate UDP port number for SRTCP media control packets for both "clear voice" and "secure voice."

2.21 REQUIREMENTS FOR SUPPORTING AS-SIP-BASED ETHERNET INTERFACES FOR VOICEMAIL SYSTEMS

SC and SS support for AS-SIP-Based Ethernet Interfaces for voicemail systems (including Unified Messaging systems and ARDs) is optional; if such an interface is supported then the following conditional requirements specify how it is to be implemented.

SCM-011460 [**Conditional: SC, SS**] If an AS-SIP-Based Ethernet Interface for voicemail systems is supported, then the SC and SS shall support all mandatory requirements in RFC 3842. Per this RFC:

"Message Waiting Indication is a common feature of telephone networks. It typically involves an audible or visible indication that messages are waiting, such as playing a special dial tone (which in telephone networks is called message-waiting dial tone), lighting a light or indicator on the phone, displaying icons or text, or some combination." This RFC "describes a Session Initiation (SIP) event package to carry message waiting status and message summaries from a messaging system to an interested User Agent."

SCM-011470 [**Conditional: SC, SS**] If an AS-SIP-Based Ethernet Interface for voicemail systems is supported, then the SC and SS shall support the use of RFC 3842 Message Waiting Indication (MWI) for "tandeming" message waiting indications between Voicemail Systems, SSs, and SCs that are subtended from the SSs. The SC and SS shall support transmission of RFC 3842 MWIs in the Voicemail System => SS => SC direction, and transmission of any RFC 3842 MWI responses in the SC => SS => Voicemail System direction.

SCM-011480 [**Conditional: MSC, SSC**] If an AS-SIP-Based Ethernet Interface for voicemail systems is supported, then Master SCs and Subtended SCs shall also support RFC 3842 MWI for "tandeming" message waiting indications between SSs, MSCs, and SSCs. MSCs and SSCs shall support transmission of RFC 3842 MWIs in the SS => MSC => SSC direction, and transmission of any RFC 3842 MWI responses in the SSC => MSC => SS direction.

SCM-011490 [**Conditional: SC, SS**] If an AS-SIP-Based Ethernet Interface for voicemail systems is supported, then the SC and SS shall support all mandatory requirements in IETF Internet RFC 5806, Diversion Indication in SIP. Per this Internet RFC:

"This document proposes an extension to the Session Initiation Protocol (SIP). This extension provides the ability for the called SIP User Agent to identify from whom the call was diverted and why the call was diverted. The extension defines a general header, Diversion, which conveys the diversion information from other SIP user agents and proxies to the called user agent. This extension allows enhanced support for various features, including Unified Messaging, Third-Party Voicemail, and Automatic Call Distribution (ACD). SIP user agents and SIP proxies that receive diversion information may use this as supplemental information for feature invocation decisions."

SCM-011500 [**Conditional: SC, SS**] If an AS-SIP-Based Ethernet Interface for voicemail systems is supported, then the SC and SS shall support all the mandatory requirements in RFC 4244. Per this RFC:

"This document defines a standard mechanism for capturing the history information associated with a Session Initiation Protocol (SIP) request. This capability enables many enhanced services by providing the information about how and why a call arrives at a specific application or user.

This RFC defines a new optional SIP header, History-Info, for capturing the history information in requests."

SCM-011510 [**Conditional: SC, SS**] If an AS-SIP-Based Ethernet Interface for voicemail systems is supported, then the SC and SS shall support all of the mandatory requirements in RFC 3725. Per this RFC:

"Third party call control refers to the ability of one entity to create a call in which communication is actually between other parties. Third party call control is possible using the mechanisms specified within the Session Initiation Protocol (SIP). However, there are several possible approaches, each with different benefits and drawbacks. This RFC provides best current practices for the usage of SIP for third party control."

2.21.1 Requirements for Supporting AS-SIP Message Waiting Indications on AS-SIP EIs, TAs, and IADs

SCM-011520 [**Conditional: SC, AEI, TA, IAD**] If an AS-SIP-Based Ethernet Interface for voicemail systems is supported, then the SC, AEI, TA, and IAD shall support all of the mandatory requirements in the following:

a. RFC 3842 for SIP Message Waiting Indication.

b. RFC 5806 for Diversion Indication in SIP.

c. RFC 4244 for SIP Request History Information.

SCM-011530 [**Conditional: TA, IAD**] In the case of TAs and IADs, this requirement applies only to TAs and IADs that support AS-SIP on their IP side for signaling with the SC.

SCM-011540 [**Conditional: SC**] If an AS-SIP-Based Ethernet Interface for voicemail system is supported, then SCs shall be able to exchange SIP MWIs, SIP Diversion Indications, and SIP Request History Information with the AS-SIP EIs, TAs, and IADs that they serve.

SCM-011550 [**Conditional: SC, AEI, TA, IAD**] If an AS-SIP-Based Ethernet Interface for voicemail system is supported, then AS-SIP EIs, TAs, and IADs shall be able to accept SIP MWIs, SIP Diversion Indications, and SIP Request History Information from the SCs that serve them, and relay the information in those SIP fields on to their end users.

For example, if an AS-SIP EI, TA, or IAD receives an RFC 3842 SIP MWI from its SC, that AEI, TA, or IAD shall be able to provide a visual MWI (light a lamp, display an icon) and/or an audible MWI (burst of ringing, stutter dial tone) to the UC end user.

2.22 LOCAL ATTENDANT CONSOLE FEATURES

This section specifies optional requirements that are desirable for a local attendant console or station on the SC.

SCM-011560 [**Optional: SC**] The attendant console shall interoperate with PBAS/ASAC as described in Section 2.10.1, PBAS/ASAC.

SCM-011570 [**Optional: SC**] The attendant console shall interoperate with MLPP as described in Section 2.25.1, Multilevel Precedence and Preemption.

SCM-011580 [**Optional: SC**] The attendant console shall be able to initiate all levels of precedence calls (i.e., ROUTINE through FLASH OVERRIDE).

SCM-011590 [**Optional: SC**] The attendant console shall provide a visual display of the precedence level and calling number for each incoming directly dialed call to the attendant, and for each call diverted to the attendant (e.g., calls that reach the attendant through PCD).

2.23 MSC AND SSC

Multiple SCs may be deployed at a single serving area in a coordinated cluster with one SC acting as the Master (MSC) and the others – Subtended Session Controllers (SSCs) – subordinate to the MSC. MSC/SSC clusters may be used in both Strategic (Fixed) deployments and within tactical extensions of the DISN.

The MSC and SSC requirements in this section apply to MSCs and SSCs in both Strategic (Fixed) networks and Tactical (Deployable) networks.

If an SC product can be configured as a Master SC, the MSC requirements in this section apply. If an SC product can be configured as a Subtended SC, the SSC requirements in this section apply. Support for MSC and SSC configurations on an SC product, as specified in Section 2.10, Session Controller, is optional.

SCM-011600 [**Required: MSC, SSC**] All SC requirements in this section and in all other sections apply to both MSCs and SSCs, unless an individual requirement indicates otherwise.

SCM-011610 [**Required: MSC, SSC, PEI, AEI, ATA, IAD**] End instruments that are served by an MSC shall be treated just like EIs that are served by SSCs. The MSC shall treat its EIs (i.e., PEIs, AEIs, ATAs, IADs) in the same way that it would if it were operating as an SSC. The SSC shall treat its EIs (i.e., PEIs, AEIs, ATAs, IADs) in the same way that it would if it were operating as an MSC.

SCM-011620 [**Required: MSC**] The MSC shall adjudicate the enclave budget (the enclave ASAC budget between the MSC and its primary SS) between its SSCs. The MSC shall adjudicate the enclave ASAC budget in cases where this budget is nondirectional [**Required**] and directional [**Optional**].

SCM-011630 [**Required: MSC**] The MSC shall support at least one of two methods for adjudicating the enclave ASAC budget between its SSCs: the “Highest Priority Sessions” method and the “Strict Budget for All SCs” method. Support for either of these two methods is acceptable.

2.23.1 Highest Priority Sessions Method

SCM-011640 [**Required: MSC**] When processing outgoing call requests from its EIs, MGs, and its SSCs, and incoming call requests to its EIs, MGs, and its SSCs, the MSC shall always ensure that the highest precedence level sessions (i.e., P, I, F, FO) are served first over the MSC-to-SS interface. When call requests are received from or directed to the SSCs, the MSC shall always ensure that the highest precedence level sessions (i.e., P, I, F, FO) are served first, regardless of where the SSC is originated or terminated.

For example, assume a MSC with three SSCs, where the MSC-to-SS ASAC budget for voice is 28 voice sessions with no directionalization. Also, assume that each SSC is allowed up to 10 voice sessions (with no directionalization) on its SSC-to-MSC interface. The SSCs could not all simultaneously be allowed up to 10 voice sessions on the MSC-to-SS interface in this case; two requests would be blocked.

SCM-011650 [**Required: MSC**] When the capacity on the access link from the MSC to the SS is fully utilized, the MSC shall allow additional higher precedence sessions (destined for outside of the enclave, or arriving from outside of the enclave) to succeed by preempting existing lower precedence sessions on the access link. The MSC shall preempt the lower precedence sessions and establish the higher precedence sessions, independent of whatever SSC originated these sessions.

SCM-011660 [**Required: MSC**] In this case, the MSC shall block ROUTINE precedence sessions on the access link that are to or from the following:

a. End users on the MSC.

b. End users on any of the SSCs, once the access link session budget (ASAC budget) is met.

2.23.2 Strict Budget for All SCs Method

SCM-011670 [**Required: MSC**] When processing outgoing call requests from its EIs, MGs, and its SSCs, and incoming call requests to its EIs, MGs, and its SSCs, the MSC shall always ensure that each SSC is allocated a fixed subset of the ASAC budget on the MSC-to-SS access link. When call requests are received from or directed to the SSCs, the MSC shall always ensure that calls to or from each SSC are allowed to complete, as long as the source or destination SSC is below its subset of the ASAC budget (its "Strict Budget") for the access link.

SCM-011680 [**Required: MSC**] When the source or destination SSC is at or above its Strict Budget for the access link, the MSC shall do the following:

a. Block all ROUTINE voice session requests on the access link that are to or from end users on that SSC, as long as the SSC is at or above its Strict Budget.

b. Allow any precedence session requests to or from end users on that SSC, but only if there is an existing session within that SSC's Strict Budget that is of a lower precedence level and can, therefore be preempted.

c. If there is no existing lower precedence session that can be preempted, the MSC shall block the precedence session request, even if there are lower precedence sessions established to or from the other SSCs that could be preempted.

For example, assume a MSC with three SSCs, where the MSC-to-SS ASAC budget for voice is 30 voice sessions with no directionalization. Also assume that each SSC is allowed up to 10 voice sessions (with no directionalization) on its SSC-to-MSC interface. Each of the SSCs could also be allowed up to 10 voice sessions on the MSC-to-SS interface in this case. No session requests to or from an SSC would be blocked, unless that SSC was operating at or above its Strict Budget of 10 voice sessions for the access link.

SCM-011690 [**Required: MSC**] When the capacity on the access link from the MSC to the SS is fully utilized, the MSC shall allow additional higher precedence sessions (destined for outside of the enclave, or arriving from outside of the enclave) to succeed by preempting existing lower precedence sessions on the access link, but only if the higher and lower precedence sessions are both within the same Strict Budget and associated with the same SSC. If these sessions are associated with the same SSC, then the MSC shall preempt the lower precedence sessions and establish the higher precedence sessions. If these sessions are not associated with the same SSC, then the MSC shall block the higher precedence sessions.

SCM-011700 [**Required: MSC**] The MSC shall also block ROUTINE precedence voice sessions to or from any SSCs, once the Strict Budget for that SSC is met.

SCM-011710 [**Required: MSC**] The MSC shall not allow precedence sessions to or from one of the SSCs to complete, if the Strict Budget for that SSC is met, and there are no existing lower precedence sessions within that Strict Budget that can be preempted.

2.23.3 EMS Access, AS-SIP Signaling, Enclave Budgets, and MG Connections

SCM-011720 [**Required: MSC, SSC**] The MSC and the SSCs shall all be capable of directly connecting to both of the following:

a. Local EMS.

b. Remote VVoIP EMS.

SCM-011730 [**Required: MSC, SSC**] The MSC is not required to provide the local or remote EMS with an aggregated NM view of the SSCs. The MSC shall provide the local or remote EMS with an individual NM view of itself. Each SSC shall provide the local or remote EMS with an individual NM view of itself.

SCM-011740 [**Required: MSC, SSC**] The MSC and the SSCs shall be capable of communicating with each other using an AS-SIP protocol per AS-SIP 2013.

In cases where the MSC and the SSC are from the same SC vendor, the MSC and the SSCs are allowed to communicate with each other using a proprietary signaling protocol.

SCM-011750 [**Required: MSC, SSC**] All AS-SIP signaling that either 1) leaves the enclave for an external destination, or 2) arrives at the enclave from an external source shall pass through the MSC. The SSCs shall not support their own AS-SIP or proprietary signaling links to locations outside the enclave. The SSCs shall exchange all AS-SIP or proprietary signaling with the MSC within the enclave, and the MSC shall exchange all AS-SIP signaling with locations outside the enclave.

This approach allows for both 1) multiple SC vendors within the enclave and 2) a single SC vendor's integrated solution within the enclave.

SCM-011760 [**Required: MSC**] Each MSC shall maintain two separate enclave budget counts as follows:

> **SCM-011760.a** [**Required: MSC**] Intraenclave Budget Count. This shall be a count of all VVoIP calls traversing the MSC that both originate and terminate within the enclave. This count shall include both calls within the MSC itself (EI-to-EI calls, EI-to-MG calls), and calls to or from all of the SSCs within the enclave.
>
> NOTE: This count shall be based on local traffic engineering for the enclave, and shall not be associated with the access link budget on the MSC-to-SS interface.
>
> **SCM-011760.b** [**Required: MSC**] Interenclave Budget Count. This shall be a count of all VVoIP calls that either enter the MSC and originated from outside the enclave, or leave the MSC and terminate outside of the enclave. This count shall include incoming and outgoing calls to or from the MSC itself, and incoming and outgoing calls to or from all SSCs within the enclave.

SCM-011770 [**Conditional: MSC, SSC**] If all connections between the enclave and the local PSTN are made through the MG of the MSC, then all EIs on the MSC, and all EIs on each SSCs shall originate and receive commercial calls from the PSTN PRI/CAS trunk group at the MSC's MG. (This arrangement is desired and simplifies location services that are based on the commercial PSTN numbers of the various EIs in the enclave.)

SCM-011780 [**Conditional: MSC, SSC**] If connections are made between the enclave and the local PSTN through the MGs of SSCs, then the EIs of a single SSC shall originate and receive calls from the PSTN PRI/CAS trunk group at that SSC's MG.

SCM-011790 [**Required: MSC, SSC**] The MSC in an enclave shall provide the only TDM connection (T1.619 PRI, CAS, or SS7 trunk group) to the DISN TDM infrastructure (i.e., DSN

MFSs, Tandems, EOs, SMEOs, or PBXs) in the enclave. The SSCs in an enclave shall not provide any TDM connections to the DISN TDM infrastructure in the enclave.

2.24 MSC, SSC, AND DYNAMIC ASAC REQUIREMENTS IN SUPPORT OF BANDWIDTH-CONSTRAINED LINKS

This section provides requirements for MSCs, SSCs, and Dynamic Assured Services Admission Control (DASAC), and as such augments the following:

- UC Framework 2013, Section 2.8, Session Controller.
- Section 2.3, ASAC.
- Section 2.23, MSC and SSC.

The SC requirements apply to both MSCs and SSCs unless indicated otherwise.

This section focuses on the Deployable (Tactical) use of the MSC/SSC architecture and the introduction of DASAC. Dynamic ASAC enables an SC to admit, block, or preempt new voice and video calls based on the communications capacity (bps) required for the call and the link capacity available to support the call. Dynamic ASAC will augment the current ASAC approach in which SCs admit calls based on a call budget. Dynamic ASAC will be applied independently to voice and video calls.

The requirements for an MSC and its SSCs in support of bandwidth-constrained links apply to both Deployable (Tactical) SCs and Fixed (Strategic) SCs (i.e., the requirements are not unique to Deployable SCs).

Please note that "bandwidth" has two definitions per the online version of Merriam-Webster's dictionary (http://www.merriam-webster.com/dictionary/bandwidth):

> "1: a range within a band of wavelengths, frequencies, or energies…
>
> 2: the capacity for data transfer of an electronic communications system … <a bandwidth of 56 kilobits per second>"

The Deployed (Tactical) wireless UC community will be one of the primary audiences for this section. This community generally uses "bandwidth" per the first definition but this section uses "bandwidth" per the second definition according to its usage throughout the rest of this section.

2.24.1 MSC and SSC Architecture

Within Deployable (Tactical) domains, calls typically involve multiple bandwidth constrained links. Each such link must be subject to DASAC. These links typically are wireless (e.g., satellite, radio) in nature. Deployable (Tactical) sites generally exist within a tiered command and control hierarchy.

2.24.1.1 Master/Subtended Architecture Applies to Both Voice and Video

SCM-011800 [**Required: Deployable (Tactical) SC – Optional: Fixed (Strategic) SC**] A Deployable (Tactical) SC that supports the MSC/SSC functionality shall support both voice and video services.

2.24.1.2 MSC/SSC and DASAC

SCM-011810 [**Required: Deployable (Tactical) SC – Optional: Fixed (Strategic) SC**] The product shall support DASAC; see Section 2.24.2, Dynamic ASAC.

2.24.1.3 Directionalization Budget Inheritance

SCM-011820 [**Optional: Deployable (Tactical) SC, Fixed (Strategic) SC**] The product shall inherit the voice directionalization ASAC budget requirements (i.e., IPB, IPBi, IPBo) from this entire section and AS-SIP 2013, for both voice and video.

2.24.1.4 Minimum Number of Supportable SSCs per MSC

SCM-011830 [**Required: Deployable (Tactical) SC – Optional: Fixed (Strategic) SC**] A product that supports the MSC functionality shall support DASAC for a minimum of 10 SSCs.

2.24.1.5 MSC Also an SSC

SCM-011840 [**Required: Deployable (Tactical) SC – Optional: Fixed (Strategic) SC**] A product that acts as an MSC shall be capable of acting simultaneously as an SSC.

2.24.1.6 Two Budgets per Link per Media Type

SCM-011850 [**Required: Deployable (Tactical) SC – Optional: Fixed (Strategic) SC, SS**] An MSC/SSC pair will apply their respective DASAC budgets to their respective ends of the shared link. Likewise, the SS/MSC pair will apply their respective DASAC budgets to their respective ends of the shared link. During AS-SIP call processing a given link and its budget are inferred by the combination of the sender's CCA-ID and the receiver's CCA-ID.

2.24.1.7 Distinct Voice and Video DASAC Budgets

SCM-011860 [**Required: Deployable (Tactical) SC – Optional: Fixed (Strategic) SC**] The product shall be able to support an independent DASAC budget for voice and an independent DASAC budget for video.

2.24.1.8 Long Locals

SCM-011870 [**Optional: Deployable (Tactical) SC**] The product shall support long locals where the EIs and the SC physically reside at separate sites. The Deployable (Tactical) LAN's SC and SBC also may reside at separate sites.

2.24.1.9 Logical SCs

SCM-011880 [**Optional: Deployable (Tactical) SC**] A single physical product shall provide two or more logical SCs supporting two or more Deployable (Tactical) sites. Each logical SC is a software-based partition of the single physical SC asset. Each logical SC will have its own IP address and its own CCA-ID.

2.24.2 Dynamic ASAC

This section defines requirements for providing the Dynamic ASAC (DASAC) capability.

SCM-011890 [**Required: SS – Required: Deployable (Tactical) SC – Optional: Fixed (Strategic) SC**] The product shall manage the DASAC budget in a manner similar to that described in Section 2.3, ASAC, except that the budget shall be based on the amount of bandwidth (bps) available to support a new session.

SCM-011900 [**Required: SS – Required: Deployable (Tactical) SC – Optional: Fixed (Strategic) SC**] The product shall use a method of establishing and managing the DASAC budget per SC Path. The capacity calculation shall be based on the bottleneck communications link along the SC Path.

SCM-011910 [**Required: SS – Required: Deployable (Tactical) SC – Optional: Fixed (Strategic) SC**] The DASAC budget shall be based on the following metrics derived from the parameters shown in Table 2.24-1, EISC Estimation Parameters. A product with DASAC capability shall support an EI Session Capacity (EISC) estimation table for each SC Path and each codec class that operates on the SC Path. A codec class is defined by the codec type PPS produced by the codec.

Table 2.24-1. EISC Estimation Parameters

#	PARAMETER	SOURCE	COMMENT
1	Codec Rate (bps)	Product extracts from SDP message; stored per codec class	Could change on a session-by-session basis per EI and within a session
2	Packet Rate (PPS)	Product extracts from information in SDP message	Could change on a session-by-session basis per EI and within a session. When the respective EIs support bearer-based mid-session renegotiation and if the product lacks the ability to process this bearer layer information, the PPS parameter needs to be set to the highest bits per second rate option available to the bearer-based mid-session renegotiation capability

#	PARAMETER	SOURCE	COMMENT
3	Number of Sessions in Progress	Number of sessions in progress for this codec class. This includes sessions in both the setup and active states Running account kept by product	Initial value equals zero Incremented upon successful session connection Decremented upon successful session completion
4	Tunnel Overhead Factor (bytes)	Pre-provisioned and entered into product	Indicates the number of overhead bytes that must be added to the IP packet size to account for encryption or other types of tunnels. If some sessions are tunneled and others are not, use the number of bytes associated with the largest overhead tunnel. Default is 100 bytes. Minimum 0 bytes. Maximum 512 bytes
5	IP Overhead (bytes)	Pre-provisioned and entered into product, includes IP, UDP, and RTP or SRTP overhead associated with packet flow over the target link	If IPv6, use 60 bytes If IPv4, use 40 bytes Default is 60 bytes
6	Layer 2 Overhead (bytes)	Pre-provisioned and entered into product	Sized according to layer 2 protocol used on target link—this parameter is the same for all packets in all codec classes. Default is 20 bytes
7	Safety Factor (%)	Pre-provisioned and entered into product	This parameter is used to provide a margin of error for the EISC calculation. Default is 10%
8	Voice MUX Overhead per Packet (bytes)	Pre-provisioned and entered into product	This parameter is used on a per packet basis if a voice MUX is used. There is no default value. Minimum 0 bytes. Maximum 512 bytes
9	Overhead per Voice MUX Sample (bytes)	Pre-provisioned and entered into product	This parameter is an overhead that is applied to each voice sample bundled in an output voice packet. There is no default value. Minimum 0 bytes. Maximum 512 bytes

SCM-011920 [**Required: SS – Required: Deployable (Tactical) SC – Optional: Fixed (Strategic) SC**] The parameters in each EISC estimation table shall be used to determine the following:

1. EI Session Capacity (EISC). The bandwidth required (in bps) for a session. The EISC shall be computed by the product each time it detects signaling for a new session or a change in codec parameters for an ongoing session.
2. Transmission Link Session Capacity (TLSC). The capacity (bps) of the bottleneck link associated with the SC Path. The TLSC is a pre-provisioned parameter entered for each SC Path link via NM commands. The TLSC does not include an allocation for session signaling. Session signaling must be provisioned separately as part of traffic engineering for the bottleneck link on the path.

3. Available Link Session Capacity (AVSC). The capacity (bps) currently available for sessions on the SC Path. The AVSC shall be calculated each time during:
   a. The session establishment AS-SIP dialog (specifically the AS-SIP message containing the SDP answer).
   b. Mid-session re-INVITE dialog based on a mid-session codec change (specifically the AS-SIP message containing the new SDP answer to the new offer).
   c. Session teardown (specifically based on SC detecting the AS-SIP 200 (OK) for the BYE).

   The AVSC is the difference of the TLSC and the sum of EISCs for all sessions in progress and in the process of being established on the SC Path.

   i.e., AVSC = TLSC - ∑ [EISCs]
4. Determination of TLSC depends on the following:
   a. The allocation of capacity to the bottleneck router queue within the SC Path.
   b. The portion of that capacity that is reserved for voice and video applications that is not under the control of the SC.

SCM-011930 [**Required: SS – Required: Deployable (Tactical) SC – Optional: Fixed (Strategic) SC**] Parameters 1 through 3 in Table 2.24-1, EISC Estimation Parameters, are dynamic; the product shall calculate these parameters on a session-by-session basis. Parameters 4 through 9 are preloaded into the product based on traffic engineering analysis of the link.

SCM-011940 [**Required: SS – Required: Deployable (Tactical) SC – Optional: Fixed (Strategic) SC**] The product shall support DASAC for the following types of session packet flows:

a. Pass-through flows, where the bearer packets are not modified after they are generated in either an SC or EI.
b. Voice/Video multiplexed flows where payloads from different flows are combined in a new packet to reduce the effect of IP overhead before transmission on a bottleneck link.
c. Header compressed flows where all or some of the IP/UDP/RTP headers are compressed before transmission on a bottleneck link.
d. Tunneled flows, where the packet flows described earlier are also subject to tunneling, for example, using IPSec.

SCM-011950 [**Required: SS – Required: Deployable (Tactical) SC – Optional: Fixed (Strategic) SC**] The product shall use parameters 1 through 9 in Table 2.25-1, EISC Estimation Parameters, as appropriate, to calculate the total EISC and AVSC. Parameter values 1 through 3 shall be determined by the product (SC or SS). Parameters 4 through 9, as appropriate, shall be determined before operation and loaded into the product (SC or SS) database. These values shall

be chosen conservatively to ensure that there is no case where more sessions are admitted than can be supported by the SC Path.

SCM-011960 [**Required: SS – Required: Deployable (Tactical) SC – Optional: Fixed (Strategic) SC**] The product shall, on a session-by-session basis, scan the SDP messages, extract the EISC codec rate and PPS parameters from each SDP Answer message, and store these parameters in the appropriate DASAC table, for each session in progress.

SCM-011970 [**Required: SS – Required: Deployable (Tactical) SC – Optional: Fixed (Strategic) SC**] The product shall be able to support all codecs defined in Section 2.9.1.3, Audio Codecs, Voice Instruments, Section 2.9.3.3, Video Codecs (Including Associated Audio Codecs), and Appendix A Section A7.5.4 Codec Translation Functional.

SCM-011980 [**Required: SS – Required: Deployable (Tactical) SC – Optional: Fixed (Strategic) SC**] If the product does not have an entry for the negotiated audio codec or for the PPS for the session, the product shall set EISC at 110 Kbps.

SCM-011990 [**Required: SS – Required: Deployable (Tactical) SC – Optional: Fixed (Strategic) SC**] If the product supports an ongoing session in which the EIs can re-negotiate audio or video codec changes at the bearer layer (e.g., modem protocol), the product shall set EISC at the highest bit rate that can be re-negotiated by the EIs mid-session via the bearer layer.

SCM-012000 [**Required: SS – Required: Deployable (Tactical) SC – Optional: Fixed (Strategic) SC**] If the values of parameters 4 through 7 are not explicitly entered in the table, the product shall use the default parameters listed in Table 2.24-1, EISC Estimation Parameters.

SCM-012010 [**Required: SS – Required: Deployable (Tactical) SC – Optional: Fixed (Strategic) SC**] The product shall not use silence suppression, also known as voice activity detection, as a factor in calculating EISC for voice sessions.

SCM-012020 [**Required: SS – Required: Deployable (Tactical) SC – Optional: Fixed (Strategic) SC**] Each DASAC product also shall be provisioned with session budget parameters which provide an absolute limit on the number of voice and video sessions accepted in either direction for each link.

2.25 OTHER UC VOICE

2.25.1 Multilevel Precedence and Preemption

NOTE: In general, the Multilevel Precedence and Preemption (MLPP) requirements in this section apply to IP-based Precedence-Based Assured Services (PBAS), i.e., the use of the term "MLPP" in this section is not meant to restrict these requirements to services provided by TDM-based networks.

SCM-012030 [**Required: AEI, SC, SS – Optional: PEI**] The MLPP service applies to the MLPP service domain only. Connections and resources that belong to a call from an MLPP

subscriber shall be marked with a precedence level and domain identifier (consistent with ANSI Standards T1.619-1992 and T1.619a-1994) and shall be preempted only by calls of higher precedence from MLPP users in the same MLPP service domain

2.25.1.1 Precedence Levels

SCM-012040 [**Required: AEI, SC, SS – Optional: PEI**] The SC, SS, PEI and AEI shall provide five precedence levels. The precedence levels listed from lowest to highest are ROUTINE, PRIORITY, IMMEDIATE, FLASH, and FLASH OVERRIDE.

2.25.1.2 Invocation and Operation

SCM-012050 [**Required: AEI, SC, SS – Optional: PEI**] The precedence level of a call is selected by the subscriber on a per call basis. The subscriber may select any precedence level up to and including his or her maximum authorized precedence level. The network at the subscriber's originating interface ensures that the selected precedence level does not exceed the maximum level assigned to that telephone number. Once set for a call, this precedence level cannot be changed. In addition, a connection between two UC subscribers shall not have different precedence levels. A call will default automatically to the ROUTINE precedence unless a higher precedence is dialed. The DSN Worldwide Numbering and Dialing Plan is described in Section 2.18.1, DSN Worldwide Numbering and Dialing Plan.

SCM-012060 [**Required: AEI, SC, SS – Optional: PEI**] During a call setup, if there is a shortage of network resources, the SC or SS shall determine whether resources are held by calls of lower precedence. If there is a shortage, the SC or SS shall release the lowest of these lower precedence call(s) and seize the resources required to set up the higher precedence call. These resources include calls on trunks between an SC and a DSN circuit switch.

The preemption operation depends on whether the SC/SS needs to preempt a common network resource, such as one of the SC to DSN switch trunks that is currently being used by a different subscriber than the intended called subscriber.

SCM-012070 [**Required: AEI, SC, SS – Optional: PEI**] If a called user is to be preempted, both the called party and its connected-to parties shall be, at a minimum, audibly notified of the preemption using the preemption tone in Table 2.9-2, UC Information Signals, and the existing MLPP call shall be cleared immediately. The called party must acknowledge the preemption by going "on-hook" or pressing a feature button, before the higher precedence call is completed. Then the called party is offered the new MLPP call.

SCM-012080 [**Required: AEI, SC, SS – Optional: PEI**] After attempting a precedence call, the calling party shall receive an audible ringback precedence call tone when the call is offered successfully to the called party as a precedence call. These alerting tones are provided in Table 2.9-2, UC Information Signals.

SCM-012090 [**Required: AEI, SC, SS – Optional: PEI**] The calling party shall receive a BPA, as shown in Table 2.9-3, Announcements, for the following reasons:

- Equal or higher precedence calls have prevented completion.
- No idle network resources are available to make a connection to the dialed number and the called subscriber belongs to a network that does not support preemption.

SCM-012100 [**Required: AEI, SC, SS – Optional: PEI**] If the requested precedence level is not subscribed to, the calling party shall receive a UPA, as shown in Table 2.9-3, Announcements.

SCM-012110 [**Required: AEI, SC, SS – Optional: PEI**] The calling party shall receive a BNEA, as shown in Table 2.9-3, Announcements, if the called party is assigned as nonpreemptable. Precedence calls (i.e., PRIORITY and above) that are not responded to by the called party (e.g., call unanswered) shall be diverted IAW Section 2.2.10, Precedence Call Diversion. If precedence call waiting has been invoked, these calls shall be handled IAW Section 2.2.3, Precedence Call Waiting. Unanswered calls placed at a ROUTINE precedence level shall continue to ring.

2.25.1.3 Preemption in the Network

SCM-012120 [**Required: AEI, TA, IAD, SC, SS – Optional: PEI**] The following sections describe the treatment for precedence calls at the called party's interface and applies to both analog and digital (ISDN and non-ISDN) terminating Customer Premises Equipment (CPE).

2.25.1.3.1 Network Facilities Active with Lower Precedence Calls

SCM-012130 [**Required: AEI, SC, SS – Optional: PEI**] For PRIORITY precedence calls and above, during call setup, if there is a shortage of a network resource, then the network shall determine whether resources are held by calls of lower precedence. The network shall release the lowest of these lower precedence call(s) and seize the necessary resources that are required to set up the higher precedence call. These resources include calls on trunks between an SC and a DSN circuit switch.

SCM-012140 [**Required: AEI, SC, SS – Optional: PEI**] When a common network resource is preempted, all existing parties shall receive a preemption tone (see Table 2.9-2, UC Information Signals) and the existing connection is disconnected. The new higher precedence call is set up using the preempted resource.

2.25.1.3.1.1 CANCEL To/CANCEL From

SCM-012150 [**Required: SC, SS**] Requirements for the CANCEL to/CANCEL from feature shall be IAW Telcordia Technologies GR 477-CORE, Section 6, NTM Manual Controls.

SCM-012160 [**Required: SC, SS**] In addition, FLASH and FLASH OVERRIDE calls shall be exempted from these controls. The application of any SC/SS to circuit-switch trunk group control shall not prevent precedence calls from performing a preemptive search on all trunk groups that were friendly searched previously.

2.25.1.3.2 Network Facilities Active With Equal or Higher Precedence Call

SCM-012170 [**Required: AEI, SC, SS – Optional: PEI**] If all network resources required to complete a precedence call are busy with equal or higher precedence calls, the calling user shall be sent the BPA (see Table 2.9-3, Announcements).

2.25.1.3.3 MLPP Trunk Selection (Hunting)

SCM-012180 [**Required: SC MG, SS MG**] The UC route selections shall be based on Precedence Level/Calling Area (PL/CA) classmarks for both voice-grade and data-grade trunk groups. The UC hunting sequence shall be capable of being varied depending on the route. Hunt sequences shall be capable of scanning data-grade trunk groups for voice-grade calls. The hunting sequence shall be capable of searching all trunks. First, the hunting sequence shall examine the route digit so that, for data calls only, data-grade trunks shall be searched. For voice-grade calls, all trunks shall be searched.

2.25.1.3.3.1 Hunt Sequence for Trunks

SCM-012190 [**Required: SC MG, SS MG**] The SCs/SSs shall route UC calls to trunks that have classmarks to indicate the maximum PL/CA permitted. Calls shall not be originated over trunk groups when the call attempt exceeds the precedence level or calling area.

2.25.1.3.3.1.1 ROUTINE Precedence Calls

SCM-012200 [**Required: SC MG, SS MG**] For ROUTINE precedence calls, the SC/SS shall use an idle search on all programmed routes to the call destination. Failing to find an idle trunk, the SC/SS shall provide a trunk busy tone to the caller.

2.25.1.3.3.1.2 Precedence Calls Above ROUTINE Precedence

SCM-012210 [**Required: SC MG, SS MG**] The SC/SS shall provide for two methods of trunk route selection for precedence level calls above the ROUTINE precedence. Either method can be assigned to a destination route based on the UC Area Code (KXX) and/or UC Switch Code (KXX) of the call. In each method, trunks shall be tested individually for idle or busy conditions. If preemption is required, only a call of the lowest level of precedence, lower than the dialed precedence, shall be preempted.

2.25.1.3.3.1.2.1 Method 1

SCM-012220 [**Required: SC MG, SS MG**] In method 1, the SC/SS shall perform an idle search on the direct route and all alternative routes, as shown in Figure 2.25-1, Example Hunt Sequence for Method 1.

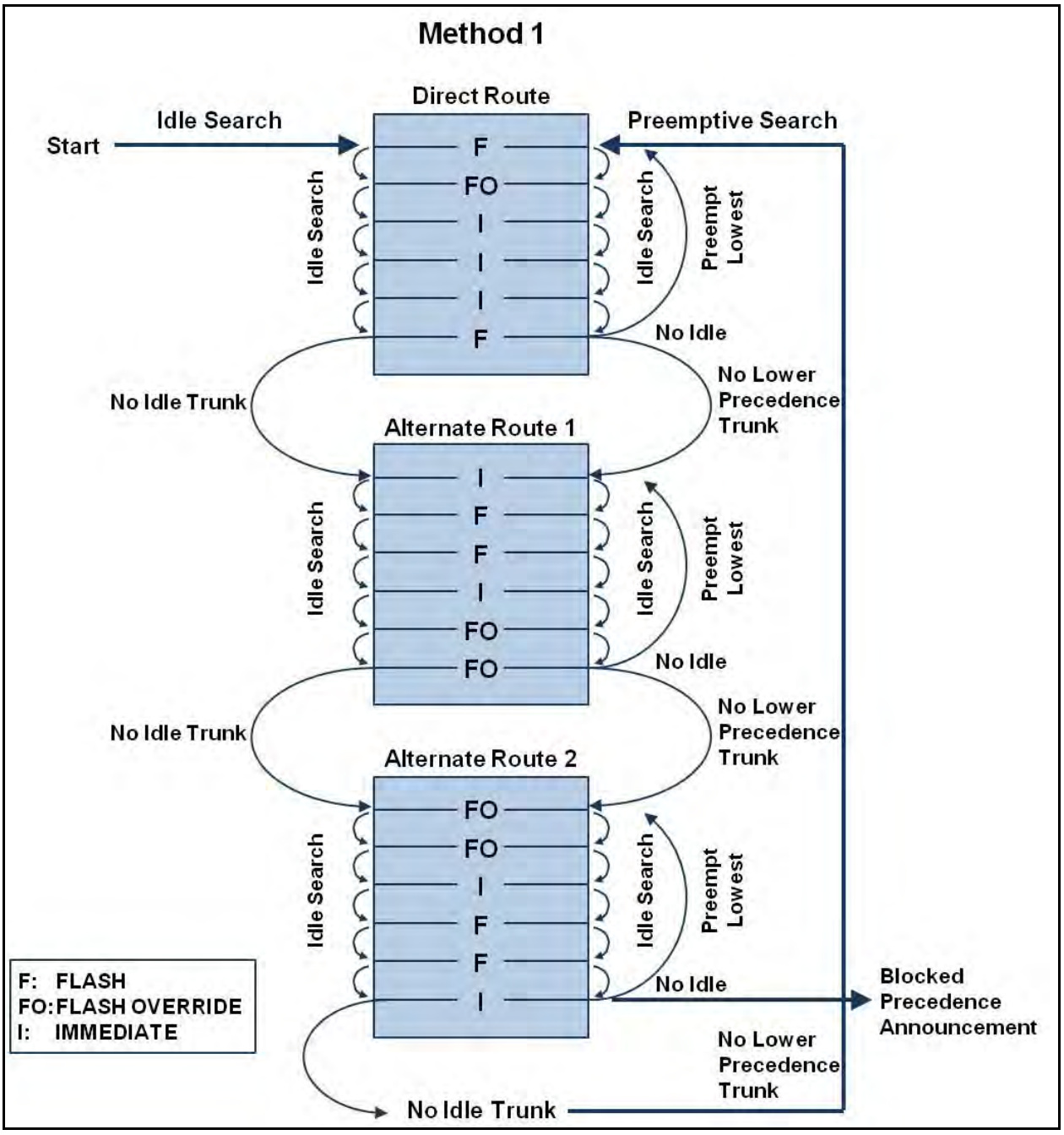


Figure 2.25-1. Example Hunt Sequence for Method 1

SCM-012230 [**Required: SC MG, SS MG**] Failing to find an idle trunk, the SC/SS shall enter the preemptive search. In the preemptive search, the SC/SS shall search again for an idle trunk in

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

2.25.1.3.3.1.2.2 Method 2

SCM-012240 [**Required: SC MG, SS MG**] In method 2, the SC/SS shall directly enter a friendly, then a preemptive search of the direct route before searching the next alternate route choice, as shown in Figure 2.25-2, Example Hunt Sequence for Method 2.

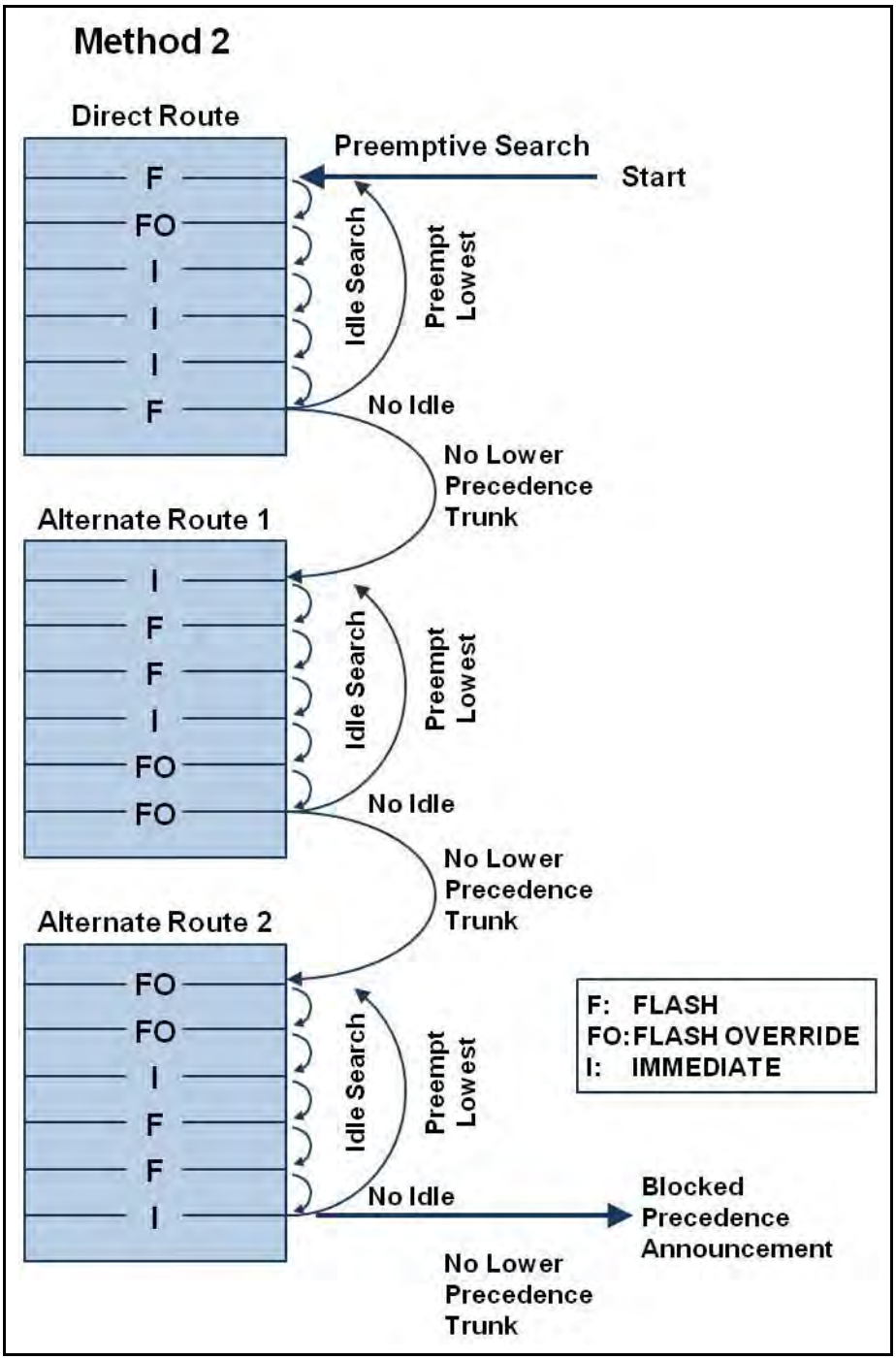


Figure 2.25-2. Example Hunt Sequence for Method 2

SCM-012250 [**Required: SC MG, SS MG**] In the preemptive search, the SC/SS shall search for an idle trunk in the direct route, and if so, shall select any idle trunk found. If no idle trunk exists in the direct route, the SC/SS shall preempt the call of the lowest precedence in the direct route, provided the precedence of the call selected for preemption is lower than the precedence of the call being processed. Failing to complete the call on the direct route, the SC/SS shall advance the preemptive search to the next alternate route, and repeat the preemptive search process described

here. This process will continue through all possible alternate routes. When the SC/SS is unable to preempt, it shall route the caller to the BPA.

2.25.1.3.4 MLPP Interworking With Other Networks

2.25.1.3.4.1 Calls From Non-MLPP Networks

SCM-012260 [**Required: MG, SC, SS**] Calls from non-MLPP networks that enter UC shall be assigned the lowest precedence level and the MLPP service domain identification at the network boundary and may be preempted within UC.

2.25.1.3.4.2 Precedence Calls to Non-MLPP Networks

SCM-012270 [**Required: SC, SS**] When a precedence call leaves the UC network and enters a network (i.e., PSTN, North American Treaty Organization (NATO), Enhanced Mobile Satellite Systems (EMSS), etc.) or a non-MLPP device (e.g., ARD) that does not support the MLPP service, the call is treated as a non-MLPP call. The SC/SS that is directly connected to the non-MLPP network shall send an LOC2 announcement to the call originator as described in Section 2.9.1.2.2, Announcements.

SCM-012280 [**Required: SC, SS**] The SC/SS MGs shall be capable of terminating incoming calls above ROUTINE to trunk groups classmarked as non-preemptable (e.g., to a PBX2, PSTN, or other non-UC network). The SC/SS shall be capable of providing the following capabilities:

a. The SC/SS shall divert the precedence call to an alternate DN or location capable of handling the precedence level of the call.

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

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

c. The SC/SS/MG shall extend the precedence call as routine (i.e., no T1.619a IEs) to the PBX2 or a non-MLPP network.

2.25.1.4 Preempt Signaling

2.25.1.4.1 Channel-Associated Signaling

SCM-012290 [**Optional: SC MG, SS MG**] Preemption on CAS trunks shall be accomplished at a UC signaling appliance by sending a measured supervisory signal toward both the calling user and the called user of an established or ringing call connection. The supervisory signal is recognized at the UC signaling appliance, causing the release of the call. Following call release,

a preempt warning tone of 440 + 620 Hz shall be applied to each end user. The preempt warning tone is introduced by the terminating UC signaling appliance at a composite level of 16 dBm, measured at the zero transmission level point (TLP). The preempt warning tone is maintained until a disconnect signal ("off hook" or feature button on EI) is returned to the UC signaling appliance. The trunk that was selected for Preemption for Reuse shall be reused to serve the waiting precedence call. Four preemption signals exist, depending on the circuit condition and intended disposition. They are Answered Call: Circuit to be Reused, Unanswered Call: Circuit to be Reused, Answered Call: Circuit Not to be Reused, and Unanswered Call: Circuit Not to be Reused, and are illustrated in Figure 2.25-3, UC Preempt Signals (Part 1) and Figure 2.25-4, UC Preempt Signals (Part 2).

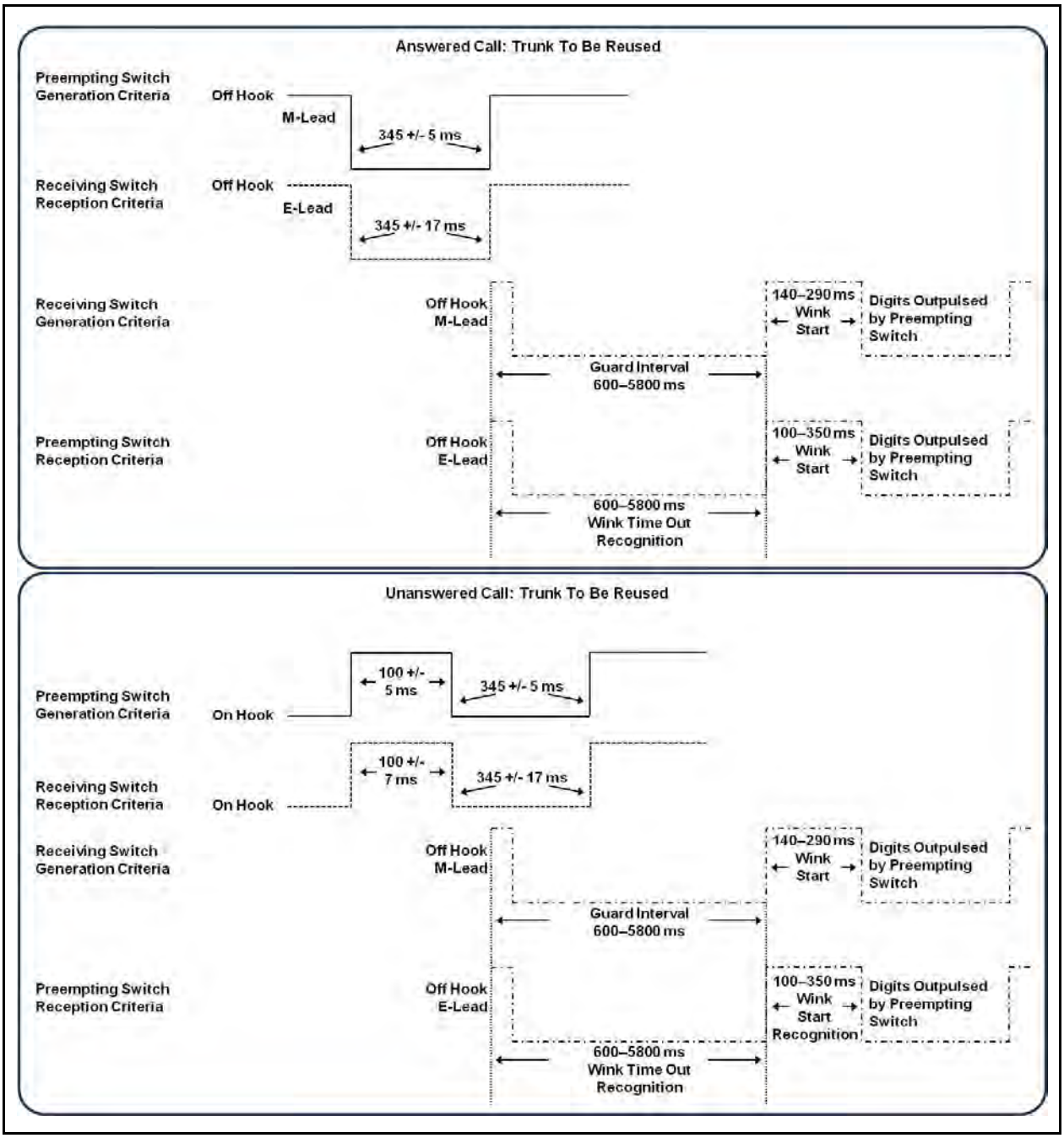


Figure 2.25-3. UC Preempt Signals (Part 1)

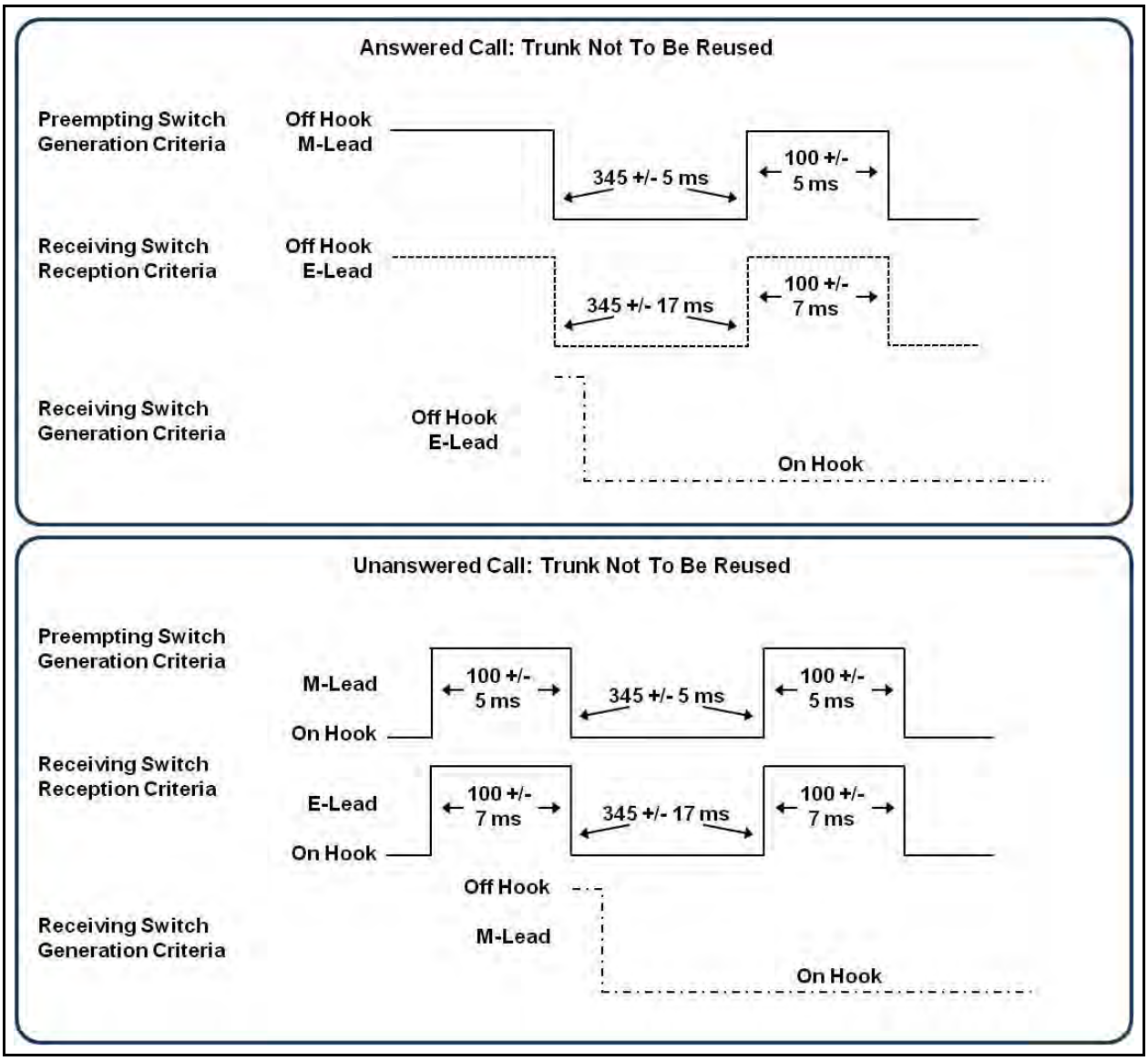


Figure 2.25-4. UC Preempt Signals (Part 2)

Preemption for Reuse shall be exercised only on classmarked trunks in a preemptable group. Preemption Not for Reuse may occur on any classmarked trunk when another link in the established connection is preempted for reuse. The UC signaling appliance MG shall apply a preemption warning tone to dial pulse (DP) and DTMF access trunks that do not use Wink Start signaling for supervision. Trunks that use Wink Start supervision shall conform to the preempt signals, as shown in Figure 2.25-3, UC Preempt Signals (Part 1). Trunks using common channel supervision (i.e., D-channel signaling) shall apply the preemption warning tone to the user that is preempted. The SC/SS that supports MF(R1) signaling shall be capable of interpreting and responding to the four preempt signals, as shown in Figure 2.25-3 and Figure 2.25-4.

2.25.1.4.2 Primary Rate Interface

SCM-012300 [**Required: SC MG, SS MG**] Requirements for MLPP PRI signaling shall be IAW ANSI Standards T1.619-1992 and T1.619a-1994.

2.25.1.5 Analog Line MLPP

2.25.1.5.1 Busy at the Called Party's Interface

SCM-012310 [**Required: TA, IAD, SC, SS**] The following busy line treatment at the called party's interface for precedence calls shall apply to analog terminating lines (i.e., lines off of a TA or IAD). The line treatments apply to inter-SC calls or calls between users on the same SC.

2.25.1.5.1.1 Line Active With an Equal or Higher Precedence Call Above ROUTINE Precedence

SCM-012320 [**Required: TA, IAD, SC, SS**] Precedence calls arriving at a party that is busy with an equal or higher precedence call shall be routed to a BPA (see Table 2.9-3, Announcements). If the called party has activated call forwarding, the SC/SS shall attempt to complete the call to the forward destination.

2.25.1.6 ISDN MLPP BRI

SCM-012330 [**Optional: TA, IAD, SC, SS**] The ISDN MLPP BRI allows the simultaneous transmission of voice and circuit-switched (CS) data over a single customer line connecting CPE and a IAD/TA. Specifically, the basic access allows the provision of two 64-Kbps B-channels that shall be used to carry voice or CS data, and a one 16-Kbps D-channel that can carry signaling and packet information.

SCM-012340 [**Optional: TA, IAD, SC, SS**] The MLPP requirements for this feature shall be IAW ANSI Standard ANSI T1.619-1992 and T1.619a-1994.

2.25.1.6.1 Single B-Channel, Single Appearance, Single Directory Number

SCM-012350 [**Optional: TA, IAD, SC, SS**] The following busy line treatment at the called party's interface for precedence calls shall apply to digital (ISDN and non-ISDN) terminating lines on an IAD or TA. The line treatments also apply to inter-SC calls and calls between users on the same SC.

2.25.1.6.1.1 Line Active With a Lower Precedence Call

SCM-012360 [**Optional: TA, IAD, SC, SS**] Precedence calls arriving at a busy user that is classmarked as preemptable shall preempt the active lower precedence call. The active busy user shall receive a continuous preemption tone until an "on-hook" signal is received and the other party shall receive a preemption tone for a minimum of 3 seconds (see Table 2.9-2, UC

Information Signals). After going "on-hook," the user to which the precedence call is directed shall be provided precedence ringing (Table 2.9-1, UC Ringing Tones and Cadences). The user shall be connected to the preempting call after going "off-hook."

SCM-012370 [**Optional: TA, IAD, SC, SS**] If call waiting is invoked by the terminating user, it shall be ignored and the existing lower precedence call shall be preempted (refer to Section 2.2.3.3, Busy With Lower Precedence Call).

2.25.1.6.1.2 Line Active With an Equal or Higher Precedence Call

SCM-012380 [**Optional: TA, IAD, SC, SS**] Precedence calls arriving at a user that is busy with an equal or higher precedence call shall be routed to a BPA (see Table 2.9-3, Announcements). If the called user has activated call forwarding, the call shall be forwarded to the new number at the same precedence level.

2.25.1.6.2 Single B-Channel, Multiple Appearances, Single Directory Number

SCM-012390 [**Optional: TA, IAD, SC, SS**] This section describes the requirements for processing precedence calls over a single B-channel ISDN interface with a station set that has multiple appearances and one DN.

SCM-012400 [**Optional: TA, IAD, SC, SS**] Incoming precedence calls to a multiple appearance ISDN station set shall provide a precedence ringing tone on the next available button as well as a visual display of the precedence level on the station set. Then the called party shall have the option of either placing the current call on hold and picking up the incoming precedence call, or ignoring the call.

SCM-012410 [**Optional: TA, IAD, SC, SS**] This process of placing a call on hold and answering a precedence call shall remain the same until the BRI is saturated (i.e., all call appearances are in use). When an incoming precedence call is made to a saturated BRI, the lowest precedence call, including those on hold, shall be preempted.

SCM-012420 [**Optional: TA, IAD, SC, SS**] If a call on hold has the lowest precedence, the SC/SS shall send a preemption tone to the call on hold caller. The SC/SS/IAD/TA sends a preemption tone to the corresponding appearance on the station set of the destination DN that has placed the call on hold. After a preset time the call is cleared and the SC/SS sends a precedence ring to the corresponding appearance on the station set of the destination DN. Next, the destination DN user hears the precedence ringing, indicating that the call on hold has been dropped. The DN user sees the precedence level of this new call on the station set display also. The DN user shall have the option of answering the call, letting it forward to an alternate party, and/or letting it divert to an attendant.

SCM-012430 [**Optional: TA, IAD, SC, SS**] If the active call has the lowest precedence, the SC/SS shall send a preemption tone to the active call and the destination directory number. When the destination directory number goes "on hook," a precedence ring is received indicating the incoming precedence call.

SCM-012440 [**Optional: TA, IAD, SC, SS**] In these two cases, the other calls on hold are not preempted, and they may be retrieved at any time.

2.25.1.6.3 Two B Channels, Multiple Appearances, Single Directory Number

SCM-012450 [**Optional: TA, IAD, SC, SS**] The requirements for processing precedence calls over a two B-channel ISDN interface, with a station set that has multiple appearances and one DN, shall be identical to that in Section 2.25.1.6.2, Single B-Channel, Multiple Appearances, Single Directory Number (i.e., precedence calls over a single B-channel ISDN interface with a station set that has multiple appearances and one DN).

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

2.25.1.6.4 Two B-Channels, Two Directory Numbers (Data Mode Only)

This section describes the requirements for processing precedence calls over a two B-channel ISDN interface with two DNs.

SCM-012460 [**Required: TA, IAD, SC, SS**] When an ISDN call appearance is set up as data-mode only (i.e., one or two B-channels equipped for data), preemption by incoming voice calls shall not be permitted. Any incoming higher precedence voice calls placed to a BRI in data-mode shall receive a BNEA or divert IAW Section 2.2.10, Precedence Call Diversion.

2.25.1.7 ISDN MLPP PRI

SCM-012470 [**Required: SC MG, SS MG, SC, SS**] Requirements for ISDN MLPP PRI shall be IAW ANSI Standards T1.619-1992 and T1.619a-1994.

SCM-012480 [**Optional: SC MG, SS MG, SC, SS**] Requirements for European Telecommunications Standards Institute (ETSI) ISDN MLPP PRI shall be IAW ITU-T Standard Q.955.3-1993.

2.25.1.7.1 Precedence Level Information Elements

SCM-012490 [**Required: SC MG, SS MG, SC, SS**] The MLPP ISDN PRI Setup Message shall contain the Precedence Level IE in Code Set 5, as shown in Table 2.25-1.

Table 2.25-1. MLPP ISDN PRI Precedence Level Information Element (Code Set 5)

OCTET 3:								
BIT:	**8**	**7**	**6**	**5**	**4**	**3**	**2**	**1**
	Precedence Level Information							
OCTET 1	**0**	**1**	**0**	**0**	**0**	**0**	**0**	**1**
	Element Identifier							
2	Length of Precedence Level Contents							
3	1 Ext	Coding Standard		Spare	Precedence Level			
4	0/1 Ext	Spare			Change Value	Spare	LFB Indication	
5	1st Network Identity Digit				2nd Network Identity Digit			
6	3rd Network Identity Digit				4th Network Identity Digit			
7	Most Significant Bit (DSN MLPP Service Domain 1st Octet)							
8	DSN MLPP Service Domain (2nd Octet)							
9	Least Significant Bit (DSN MLPP Service Domain 3rd Octet)							
Bit 8 Set to 1 as an extension bit								
BITS:	**7-6 (CODING STANDARD)**							
0 0	CCITT standardized coding							
1 0	National Standard*							
*The coding standard for DSN shall be assigned as "National."								
Bits:	**4 3 2 1 (PRECEDENCE LEVEL)**							
0 0 0 0	(FLASH OVERRIDE – highest)							
0 0 0 1	(FLASH)							
0 0 1 0	(IMMEDIATE)							
0 0 1 1	(PRIORITY)							
0 1 0 0	(ROUTINE – lowest)							
0 1 0 1 to 1 1 1 1	(Spare)							
OCTET 4:								
Bit 8	Set to 0/1 as an extension bit							
Bits 7-6-5	(Spare)							
Bit 4	(Change value)							
0	Precedence level coding privilege may be changed at network boundaries							
1	Precedence level coding privilege may not be changed at network boundaries							
Bit 3	(Spare)							

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

2.25.1.7.2 Disconnect Message Information Cause Values

SCM-012500 [**Required: SC MG, SS MG, SC, SS**] The MLPP ISDN PRI Q.931 Disconnect message shall contain the following cause values, shown in Table 2.25-2, as defined in the ANSI Standards T1.619-1992 and T1.619a-1994.

Table 2.25-2. Disconnect Message Cause Value

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

2.25.1.7.3 Signal Information Element

SCM-012510 [**Required: SC MG, SS MG, SC, SS**] For providing tones and announcements, the Signal IE, as described in 4.5.24 of ANSI T1.607, shall be used with the following two U.S. national codepoints for signal values, as shown in Table 2.25-3, U.S. National Codepoints for Signal Values.

Table 2.25-3. U.S. National Codepoints for Signal Values

SIGNAL VALUE	EXPLANATION	NORTH AMERICAN PRACTICE
9	Preemption tone is on	Precise tone is a continuous 440 Hz tone added to a 620 Hz tone
-	Precedence call alerting ringback tone on	Ringback tone (audible ringing tone) is a 440 Hz tone added to a 480 Hz tone repeated in a 1.64 s on, 0.36 s off pattern

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

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

SCM-012520 [**Required: SC MG, SS MG, SC, SS**] The ANSI T1.619a ISDN Setup Message called party number format shall be as shown in Table 2.25-4.

Table 2.25-4. ANSI T1.619a ISDN Setup Message Called Party Number Format

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

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

SCM-012530 [**Required: SC, SS**] Trunk-to-Trunk Tandem Calls. The SC/SS shall have the capability to assign a default MLPP service domain to an ANSI T1.619a trunk that tandems from a non-ANSI T1.619a trunk (i.e., T1/E1 CAS, ISDN PRI). The default MLPP service domain shall be assigned by the SC/SS via the administration terminal, and shall be a range from 00 00 00 to FF FF FF in hexadecimal.

SCM-012540 [**Required: SC, SS**] Trunk-to-EI Calls. The SC/SS shall have the capability to assign a MLPP service domain on a per user basis. The SC/SS shall have the capability to assign a default MLPP service domain to a user that terminates an incoming non-ANSI T1.619a trunk call.

SCM-012550 [**Required: SC, SS**] EI-to-Trunk Calls. The SC/SS shall have the capability to assign a default MLPP service domain to an ANSI T1.619a trunk that originates from an EI that is not assigned a MLPP service domain. The SC/SS shall allow calls placed from an EI with or without an assigned MLPP service domain to route over non-ANSI T1.619a trunks.

SCM-012560 [**Required: SC, SS**] Interaction between Unlike MLPP Service Domains. The following rules apply for calls placed between unlike MLPP service domains:

(1) The SC/SS shall allow connection between unlike MLPP service domains when resources are available.

(2) When a call is placed between unlike MLPP service domains, the SC/SS shall classmark the MLPP service domain of the connection based on the MLPP service domain that entered the SC/SS.

(a) Example 1: EI-to-EI. If an intra-SC call is placed between two subscribers with different MLPP service domains, the SC shall classmark the connection with the MLPP service domain of the originator.

(b) Example 2: Trunk-to-Trunk. If an incoming call is placed to an SC/SS via a non-ANSI T1.619a trunk (i.e., T1/E1 CAS, ISDN PRI) that tandems to an ANSI T1.619a trunk, the SC/SS shall assign the default MLPP service domain to the outbound ANSI T1.619a trunk, and classmark the connection as the SC/SS-assigned default MLPP service domain.

(c) Example 3: Trunk-to-EI. If an incoming call is placed to an SC/SS via a non-ANSI T1.619a trunk (i.e., T1/E1 CAS, ISDN PRI) that terminates to an EI, the SC/SS shall assign the default MLPP service domain to the EI and classmark the connection as the SC/SS-assigned default MLPP service domain.

(d) Example 4: EI-to-Trunk. If a call is originated from a subscriber over a non-ANSI T1.619a trunk (i.e., T1/E1 CAS, ISDN PRI), the SC/SS shall classmark the MLPP service domain of the connection as the MLPP service domain of the originator.

SCM-012570 [**Required: SC, SS**] The MLPP interaction shall not be allowed between unlike MLPP service domains.

2.25.1.8 MLPP Interactions With Common Optional Features and Services

This section describes the requirements for MLPP interactions with other features and services.

2.25.1.8.1 Multiline Hunt Service

Following are types of multiline hunt groups:

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

b. Distributed Hunt. This hunting feature is a group of EIs arranged so that incoming calls are sent to the EI in the group that has been idle the longest.

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

SCM-012570.a [**Optional: PEI, AEI, SC, SS**] MLPP Interactions, EI Hunting. If no EI in the hunt group is available and one or more existing calls are of lower precedence level than that of the incoming call, then an existing call of the lowest precedence level within the group shall be preempted.

SCM-012580 [**Optional: PEI, AEI, SC, SS**] A BPA shall be returned only when all remaining EIs in the hunt group are found busy with calls of equal or higher precedence.

SCM-012590 [**Conditional: PEI, AEI, SC, SS**] If Multiline Hunt Service is supported, then it shall be provided in accordance with Telcordia Technologies GR-569-CORE.

2.25.1.9 MLPP Interactions With Electronic Key Telephone Systems Features

2.25.1.9.1 Electronic Key Telephone Systems

SCM-012600 [**Optional: TA, IAD, SC, SS**] Electronic Key Telephone Systems functions shall be provided by the UC appliance as described in Telcordia Technologies GR 205 CORE. Additional MLPP requirements are listed in the following paragraphs.

2.25.1.9.1.1 Call Appearances

SCM-012610 [**Optional: TA, IAD, SC, SS**] A call appearance shall be shared by all EKTS users. There shall not be separate call appearances for MLPP calls. All users shall be able to originate the authorized precedence level and receive all levels of precedence on a single call appearance for each directory number. Each EKTS call appearance shall comply with the MLPP functionality specified in Section 2.25.1, Multilevel Precedence and Preemption.

2.25.1.9.1.2 Hold

SCM-012620 [**Optional: TA, IAD, SC, SS**] The EKTS Hold function shall comply with the requirements of Section 2.2.5, Call Hold.

2.25.1.9.1.3 Directory Number Bridging

SCM-012630 [**Optional: TA, IAD, SC, SS**] The EKTS Directory Number Bridging function shall comply with the requirements of Section 2.2.6, Three-Way Calling.

2.25.1.9.1.4 Intercom Calling

SCM-012640 [**Optional: TA, IAD, SC, SS**] The EKTS Intercom Calling feature shall not prevent the offering of an MLPP call to any of the parties involved in an intercom call.

2.25.1.9.1.5 Abbreviated or Delayed Ringing Treatment on Incoming Calls

SCM-012650 [**Optional: TA, IAD, SC, SS**] Incoming MLPP calls shall be considered as "distinctive alerting" and shall not be affected by the Abbreviated or Delayed Ringing Treatment. Precedence Alerting (see Table 2.9-1, UC Ringing Tones and Cadences) shall be applied to the call DN appearance and the call handled as described in Section 2.25.1.6, ISDN MLPP BRI. If the call is not answered and the EKTS-T1 time expires, the call shall be diverted to an operator. If Call Forwarding-No Reply is invoked by the called DN, then the Call Forwarding procedures of Section 2.2.2.2, Call Forwarding – No Reply at Called Station, apply at the expiration of the EKTS-T1 timer.

2.25.1.9.1.6 Bridged Call Exclusion

SCM-012660 [**Optional: TA, IAD, SC, SS**] The Bridged Call Exclusion (BCE) feature (automatic or manual) shall not degrade or prevent the MLPP interactions described in this section.

2.25.1.9.1.7 Non-ISDN Users

SCM-012670 [**Optional: TA, IAD, SC, SS**] Non-ISDN users (analog telephone) can be assigned as members of the EKTS group. The non-ISDN user will share a call appearance with other members of the EKTS group and shall be able to originate the authorized precedence level and receive all levels of precedence on that shared appearance.

2.25.1.10 Network Management Manual Controls

SCM-012680 [**Required: SC, SS**] Call gapping shall not apply to FLASH and FLASH OVERRIDE calls. In addition, FLASH and FLASH OVERRIDE calls shall be exempt from Cancel to (CANT) and Cancel from (CANF)..

2.25.2 Signaling

2.25.2.1 Introduction

This section covers the signaling requirements for UC signaling appliance systems. The requirements are based on Telcordia Technologies GR-506-CORE; ANSI T1.619 (1992); ANSI T1.619a (1994); ANSI T1.110 (1999); ANSI T1.116 (1996); ANSI T1.116a (1998); ANSI T1.111 (1996); ANSI T1.114 (2000); ANSI T1.112 (1996); and ANSI 1.113 (1995). Requirements for analog signaling also apply to digital circuits using CAS.

2.25.2.2 Network Power Systems for External Interfaces

SCM-012690 [**Required: TA, IAD, SC, SS – Optional: MG**] The UC signaling appliance systems shall meet the network power systems requirements specified in the Telcordia Technologies GR-506-CORE, Paragraph 2.1.

2.25.2.3 Line Signaling

2.25.2.3.1 Loop Start Line

SCM-012700 [**Required: TA, IAD**] In a loop start line arrangement, the IAD/TA supplies battery between the ring and the tip conductors. The IAD/TA detects a loop closure from the customer station as a seizure, after which it provides dial tone on the tip and ring conductors as a start dial signal.

The UC signaling appliance systems shall meet this requirement in accordance with the "R" requirements in Telcordia Technologies GR-506-CORE, Paragraphs 3 through 3.4.7, 6.2.1, 6.3.1, 13.6.1.1, 13.6.2.1, 13.6.3.1, and 13.7.1.

2.25.2.3.2 Ground Start Line

SCM-012710 [**Required: TA, IAD**] In a ground start line arrangement, the IAD/TA provides battery through a ground detector to the ring conductor and leaves the tip conductor open. The customer station seizes the line by applying a ground to the ring conductor. The IAD/TA responds by returning ground on the tip conductor and dial tone across the tip and ring as start dial signals. When the tip ground is detected from the IAD/TA, the customer station changes to loop closure for the off-hook state. Alerting the customer is done by connecting 20-Hz ringing to the ring conductor and ground to the tip conductor.

The UC signaling appliance systems shall meet this requirement in accordance with the "R" requirements in Telcordia Technologies GR-506-CORE, Paragraphs 4 through 4.4.8, 13.2.2, 13.6.1.1, 13.6.2.2, 13.6.3.2, and 13.7.2.

2.25.2.4 Trunk Supervisory Signaling

2.25.2.4.1 Reverse Battery

SCM-012720 [**Optional: SC MG, SS MG**] The trunk circuit at one end of a variety of loop signaling trunks applies battery and ground through suitable resistances to the tip and ring conductors. One polarity on the tip and ring leads is used for the on-hook state, and the reverse is used for the off-hook state.

The UC signaling appliance systems may meet this requirement in accordance with the "R" requirements in Telcordia Technologies GR-506-CORE, Paragraphs 7 and 8.

2.25.2.4.2 Immediate Start

SCM-012730 [**Optional: SC MG, SS MG**] Immediate start (by-link) is a feature that provides intersystem address signaling between the MG and a system that transmits and/or receives address signals without special address control signals. For the reception of digits from offices requiring immediate start, the system shall be prepared to recognize the first dial pulse promptly after the connect signal is received. For transmission of address information to an office requiring immediate start, the system shall delay outpulsing after sending the connect signal to ensure that the distant office is ready. It is desirable that the transmitting office verifies that battery and ground are of the proper polarity at the time of seizure. Failure to detect the proper condition may result in a retry of the call and a failure recorded.

The UC signaling appliance systems may meet this requirement in accordance with the "R" requirements in Telcordia Technologies GR-506-CORE, Paragraph 11.2.2.

2.25.2.4.3 Normal and Abnormal Wink Start Operation

2.25.2.4.3.1 Normal Operation

2.25.2.4.3.1.1 Normal Wink Start Operation

Wink start is a feature that provides control for address signaling between systems arranged with wink start as a special address control signal. The wink start signal is applicable to specified incoming, outgoing, and two-way trunks and is used to inform the calling office that the called office is prepared to receive address signals. For wink start operation, the transmitting office may test for the detection of the brief off-hook as a signaling integrity check.

SCM-012740 [**Optional: SC MG, SS MG**] The UC signaling appliance systems shall provide wink start operation in accordance with the requirements in Telcordia Technologies GR-506-CORE, Paragraph 11.2.1.

2.25.2.4.3.1.2 Glare Operation

Glare occurs when both interfaces of switching systems connected to the same inter-switching-system facility (trunk) apply a seizure signal at approximately the same time.

SCM-012750 [**Optional: SC MG, SS MG**]The UC signaling appliance systems shall provide glare detection and resolution IAW the requirements in Telcordia Technologies GR-506-CORE, Paragraph 11.5.

2.25.2.4.3.2 Abnormal Operation

2.25.2.4.3.2.1 Wink Start

SCM-012760 [**Optional: SC MG, SS MG**] After the connect signal is sent over the trunk, the originating office can normally expect to receive a wink start (timed off-hook) signal indicating that the terminating office is ready to receive address signaling. When the end of the wink start signal is received, the originating office shall begin outpulsing. The duration of the off-hook wink returned by the terminating office will be 140 to 290 ms. However, because of distortion in the trunk facilities, the duration of the wink received by the originating office may vary (refer to Figure 2.25-3, UC Preempt Signals (Part 1) and Figure 2.25-4, UC Preempt Signals (Part 2)). If the wink is shorter than the minimum allowable interval, it shall be ignored. If it is greater than the maximum interval, the call shall be considered to be in a glare condition as described in Section 2.25.2.4.3.2.2, Glare Resolution.

2.25.2.4.3.2.2 Glare Resolution

SCM-012770 [**Optional: SC MG, SS MG**] The UC signaling appliances shall meet the glare resolutions requirements defined in Telcordia Technologies GR-506-CORE, Paragraph 11.5 and subparagraphs.

2.25.2.4.4 Delay Dial

SCM-012780 [**Conditional: SC MG, SS MG**] If this feature is provided, it shall be in accordance with Telcordia Technologies GR-506-CORE.

2.25.2.4.5 Call for Service Timing

SCM-012790 [**Optional: SC MG, SS MG**] The MG shall ignore as a “hit” any transient off-hook signal whose duration is less than 35 ms on an incoming trunk. Off-hook signals greater than 60 ms may be considered as a valid seizure. Signals that are 15 to 60 ms in length are considered invalid seizures.

2.25.2.4.6 Guard Timing

SCM-012800 [**Optional: SC MG, SS MG**] The UC signaling appliance systems shall meet guard requirements in accordance with Telcordia Technologies GR-506-CORE.

2.25.2.4.7 Satellite Interface

SCM-012810 [**Optional: SC MG, SS MG**] The UC signaling appliance system shall accommodate the use of single satellite-derived trunk facilities. The only interface parameter that shall be modified is the guard timing. This interval may be extended from 1050 to 1250 ms to compensate for propagation delay.

2.25.2.4.8 Disconnect Control

SCM-012820 [**Optional: SC MG, SS MG**] The UC signaling appliance systems shall meet the Disconnect Control requirements in Telcordia Technologies GR-506-CORE, Paragraph 13 and all subparagraphs.

2.25.2.4.9 Reselect or Retrial

SCM-012830 [**Optional: SC MG, SS MG**] The actions that shall be taken by the MG are summarized in the following table based on the direction of the circuit (outgoing or two-way), the method of controlled outpulsing (wink start or delay dial), and the method of glare resolution on two-way circuit (hold or release). The MG shall reselect or retry on circuit supervision faults as shown in Table 2.25-5.

Table 2.25-5. Reselect or Retrial

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

2.25.2.4.10 Off-Hook Supervision Transitions (Unexpected Stop)

SCM-012840 [**Optional: SC MG, SS MG**] The UC signaling appliances shall detect and react to unexpected off-hook supervisory transitions while outpulsing on trunks, after receipt of the start-dial indication and until completion of the outpulsing. An unexpected stop is defined as an off-hook supervision transition whose duration exceeds the "hit" timing interval. When an unexpected stop is detected, the system may reselect another trunk.

2.25.2.5 Control Signaling

Control signaling is used for the reception and outpulsing of address, precedence, and routing information. Three types of outpulsing are DP, DTMF, and Multifrequency 2/6.

SCM-012850 [**Required: SC MG, SS MG**] The UC signaling appliances shall support as applicable the following signaling combinations: DTMF 2way, DP 2way, DTMF in-DP out, DP in-DTMF out, MF(R1) 2/6 2way.

SCM-012860 [**Required: SC MG, SS MG**] Audible tones shall be IAW Telcordia Technologies GR-506-CORE, Paragraph 17.

2.25.2.5.1 Dial-Pulse Signals

SCM-012870 [**Required: TA, IAD**] The UC DP signaling requirements are the same as those specified in Telcordia Technologies GR-506-CORE, Paragraph 10.

2.25.2.5.2 DTMF Signaling

SCM-012880 [**Required: TA, IAD – Optional: SC MG, SS MG**] The UC signaling appliance system shall be capable of outpulsing and interpretation of DTMF digits on outgoing or two-way trunks as specified in Telcordia Technologies GR-506-CORE, Paragraph 15, and Table 2.25-6.

Table 2.25-6. DTMF Generation and Reception From Users and Trunks

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

2.25.2.5.2.1 Standard Digit Format for Precedence

SCM-012890 [**Required: TA, IAD – Optional: SC MG, SS MG**] In addition, the UC signaling appliance system shall be capable of outpulsing and interpretation of DTMF precedence digits in digit 0 through 4 format (i.e., 0=FLASH OVERRIDE, 1=FLASH, 2=IMMEDIATE, 3=PRIORITY, and 4=ROUTINE).

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

SCM-012900 [**Optional: SC MG, SS MG**] The UC signaling appliance system shall be capable of outpulsing and reception of multifrequency (MF)(R1) 2/6 signaling requirements IAW Telcordia Technologies GR-506-CORE, Paragraph 16 and its subparagraphs, and Table 2.25-7, MF(R1) 2/6 Generation and Reception for Trunks.

Table 2.25-7. MF(R1) 2/6 Generation and Reception for Trunks

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

2.25.2.6 Alerting Signals and Tones

Alerting signals are applied by an EI or IAD/TA to inform the end-user of an incoming call. Section 2.9.1.2.1 defines ringing and information signal requirements.

2.25.2.7 ISDN Digital Subscriber Signaling System No. 1 Signaling

2.25.2.7.1 UC ISDN User-to-Network Signaling

The objective of this UC ISDN user-to-network signaling requirement is to provide digital out-of-band signaling on an ISDN interface. The UC ISDN user-to-network signaling requirement, which captures protocols under the umbrella of Digital Subscriber Signaling System No. 1

(DSS1), is intended to provide a signaling protocol that will allow signaling over an ISDN interface to support the following:

- Circuit-switched calls (both data and voice).
- Supplementary services that include unique UC features.
- Future UC access signaling requirements for other network services, including public and private network interworking in intracountry and intercountry environments, as applicable, and interoperability with other DoD Networks.

2.25.2.7.1.1 Application

SCM-012910 [**PRI: Required: MG, SC, SS – BRI: Optional: TA, IAD, SC, SS**] This section is the UC signaling appliance requirements for user-to-network signaling over an ISDN interface. It specifies the interface signaling protocol for application throughout the UC network and defines the requirements of the UC user-to-network signaling for exchanging information between CPE, including terminal equipment (TE) and PBXs, and UC network signaling appliances. The exchange of signaling information between CPE and UC network signaling appliances shall be over the D-channel of the ISDN interface. The D-channel may be used either for associated signaling or non-associated signaling as defined in ANSI T1.607, Annex F. In-band information and tones sent over the B-channel shall be allowed, when applicable. In the UC host countries, UC connections may be made with public, private, and military CPE and networks. Protocol and/or SG conversions shall be required in some instances to provide the desired UC connections. Such translations shall be handled on a case-by-case basis as detailed in site-specific contracts.

2.25.2.7.1.2 Physical Layer

SCM-012920 [**PRI: Required: MG, SC, SS – BRI: Optional: TA, IAD, SC, SS**] The UC user-to-network signaling physical layer specification for the BRI shall be ANSI T1.605 and ANSI T1.601 or ITU Recommendation I.430, as required, for OCONUS applications. The UC user-to-network signaling physical layer specification for the PRI operating at 1.544 Mbps shall be ANSI T1.408. The UC user-to-network signaling specification for the PRI operating at 2.048 Mbps shall be ITU Recommendation I.431.

2.25.2.7.1.2.1 S/T Reference Point

SCM-012930 [**Optional: TA, IAD**] For the BRI at the S/T reference point, B-channels shall have the capability of either restricted or unrestricted operation. The restricted capability is necessary for backward compatibility with networks that support the restricted 64 Kbps operation. The D channel shall have unrestricted capability.

2.25.2.7.1.3 Data-Link Layer

SCM-012940 [**PRI: Required: MG, SC, SS – BRI: Optional: TA, IAD, SC, SS**] The UC user-to-network signaling data-link layer shall be as specified in the ANSI T1.602, which is a pointer document completely aligned with the ITU-T Recommendations Q.920 and Q.921.

2.25.2.7.1.3.1 Data-Link Connections

SCM-012950 [**PRI: Required: MG, SC, SS – BRI: Optional: TA, IAD, SC, SS**] Point-to-point, broadcast, and multipoint data-link connections shall be provided for UC applications. The ANSI T1.602 depicts examples of point-to-point and broadcast data-link connections. Other point-to-point applications of this specification shall be allowed, such as the support of multiple terminals at the user-to-network interface. A data-link layer management entity shall be provided to support UC management.

2.25.2.7.1.3.2 Peer-to-Peer Procedures of Data-Link Layer

SCM-012960 [**PRI: Required: MG, SC, SS – BRI: Optional: TA, IAD, SC, SS**] Within the UC network, peer-to-peer procedures of the data-link layer shall follow the procedures described in the ANSI T1.602, with the additions provided in this paragraph. The network administration shall have the responsibility to determine the system parameter values on the UC user-to-network interface. These parameters shall initially be set to the default values of the ANSI standard. A means is available in ITU-T Recommendation Q.921, Appendix IV to change the assignment of the system parameters within the range of values specified by the ANSI standard. The UC TE shall support other values of T200 to allow for multiple terminals on the user side, together with satellite connections, in UC user-to-network transmission.

2.25.2.7.1.4 Layer 3 UC User-to-Network Signaling

SCM-012970 [**PRI: Required: MG, SC, SS – BRI: Optional: TA, IAD, SC, SS**] The Layer 3 protocols specify the messages and IEs, coding and formats, and procedures used on the user-to-network interface to establish, maintain, and terminate network connections across an ISDN.

2.25.2.7.1.4.1 Overview of Layer 3

SCM-012980 [**PRI: Required: MG, SC, SS – BRI: Optional: TA, IAD, SC, SS**] The overview of Layer 3 of the UC user-to-network signaling layer 3 shall be as specified in ANSI T1.615. The ANSI standard is consistent with the seven-layer model described in ITU Recommendation I.320. ANSI T1.615 describes, in general terms, the D-channel Layer 3 DSS1 functions and protocol used across an ISDN user-to-network interface.

2.25.2.7.1.4.2 UC User-to-Network Signaling for Circuit-Switched Bearer Service

SCM-012990 [**PRI: Required: MG, SC, SS – BRI: Optional: TA, IAD, SC, SS**] The UC user-to-network signaling Layer 3 specification for CS bearer service (or CS-Basic Call) shall be as specified in the ANSI T1.607 for ISDN PRI and BRI. ANSI T1.607 is aligned with the ITU Recommendation Q.931 (to the extent possible), and it covers U.S. unique requirements for CS-Basic Call.

2.25.2.7.1.4.3 Sequence of Messages for UC CS Calls

SCM-013000 [**PRI: Required: MG, SC, SS – BRI: Optional: TA, IAD, SC, SS**] Call establishment involves SETUP, SETUP ACK, CALL PROCEEDING, ALERTING, CONNECT, and CONNECT ACK messages. The PROGRESS message shall be used with interworking or with in-band information and patterns to indicate the progress of a call. A three-step call clearing phase shall use the DISCONNECT, RELEASE, and RELEASE COMPLETE messages. The miscellaneous messages—INFORMATION, STATUS ENQUIRY (and STATUS), and NOTIFY—shall be used for the purposes described in ANSI T1.607.

2.25.2.7.1.4.4 Message Functional Definitions and Content

SCM-013010 [**PRI: Required: MG, SC, SS – BRI: Optional: TA, IAD, SC, SS**] The Layer 3 messages used by the UC user-to-network signaling for CS connections shall be as specified by the ANSI T1.607, except for messages modified in the following paragraph.

SETUP Message. The SETUP message is sent by the calling user to the network or by the network to the called user to initiate call establishment. The UC calls shall use the SETUP message specified in ANSI T1.607. The Channel Identification, Calling Party Number (when available), and Called Party Number are mandatory IEs. For an MLPP call (invoking an MLPP feature) on the UC user-to-network interface, the SETUP message shall include the Precedence Level IE. It also shall contain other IEs, when such unique UC features are required and the call identity IE (as defined in ITU Recommendation Q.931) for the MLPP feature. The Precedence Level and MLPP service domain (both contained in the Precedence Level IE) and Calling Party Number (contained in the Calling Party Number IE), shall be used to mark the circuit (identified in the Channel Identification IE) to be preempted as "reserved" for reuse by the preempting call when the LFB option is exercised on the UC user-to-network interface. Table 2.25-8, SETUP Message for MLPP Call, shows the SETUP message content for an MLPP call; important differences from the SETUP message in ANSI T1.607 are specified in the following paragraphs.

Table 2.25-8. SETUP Message for MLPP Call

MESSAGE TYPE: SETUP SIGNIFICANCE: GLOBAL DIRECTION: BOTH			
INFORMATION ELEMENT	**ANSI T1.607 REFERENCE**	**DIRECTION**	**TYPE**
Protocol Discriminator	4.2	both	M
Call Reference	4.3	both	M
Message Type	4.4	both	M
Repeat Indicator	4.5	both	O (Note 1)
Bearer Capability	4.5	both	M (Note 2)
Channel Identification	4.5	both	M (Note 3)
Progress Indicator	4.5	both	O (Note 4)
Network Specific Facilities	4.5	both	O (Note 5)
Display	4.5	n-u	O (Notes 6 & 7)
Keypad Facility	4.5	u-n	O (Note 8)
Signal	4.5	n-u	O (Note 9)
Calling Party Number	4.5	both	M (Note 10)
Calling Party Subaddress	4.5	both	O (Note 11)
Called Party Number	4.5	both	M (Note 12)
Called Party Subaddress	4.5	both	O (Note 13)
Transit Network Selection	4.5	u-n	O (Note 14)
Lower Layer Compatibility	4.5	both	O (Note 15)
High Layer Compatibility	4.5	both	O (Note 16)
User-User	4.5	both	O (Notes 17 & 18)
Locking Shift (Note1)	4.5	u-n	O (Note 19)
Operator System Access	4.6	u-n	O (Note 20)
Precedence Level	Note2	both	M
NOTE: Notes 1 through 20 and references of the ANSI T1.607 IE are not repeated for this table but still apply. Refer to ANSI T1.607 IE for detailed notes and references. 1. The Locking Shift IE to identify IEs in U.S. National Codeset 5. 2. The Precedence Level IE is in U.S. National Codeset 5 and is defined in ANSI T1.619 (1992) and T1-619a (1994).			
LEGEND M: Mandatory O: Optional Elements			

2.25.2.7.1.4.5 General Message Format and Information Elements Coding

SCM-013020 [**PRI: Required: MG, SC, SS – BRI: Optional: TA, IAD, SC, SS**] The guidelines specified in the ANSI T1.607 shall be followed in this specification.

a. Application of Codesets Within UC. UC unique IEs shall use the following order of preference in using the codesets:

(1) Codeset 0 – highest.

(2) Codeset 5.

(3) Codeset 6 – lowest.

b. Application of IEs in UC. The UC user-to-network signaling protocol shall maximize the use of codeset "00" (ITU standardized coding) and codeset "10" (national standard) IEs (when codeset "00" is not possible). The requirements for the specific use of such IEs in the UC network are as follows:

c. Called Party Number IE. The Called Party Number IE, which identifies one called party of a call, shall accommodate the DSN numbering plan. The variable length number digits parameter in the IE shall carry the area code, switch code, and line number from the DSN numbering plan.

(1) Calling Party Number IE. The Calling Party Number IE, which identifies the origin of a call, shall accommodate the DSN Worldwide Numbering and Dialing Plan (WWNDP) as stated for the Called Party Number IE.

(2) Keypad Facility IE. The Keypad Facility IE, which conveys ASCII characters entered by means of a terminal keypad (when used), shall contain the digits entered by a UC user.

(3) Channel Identification IE. The Channel Identification IE identifies a channel within the interface(s) controlled by the signaling procedures. The channel number/slot map parameter within it identifies the B-channel controlled by a particular message. The following two methods of B-channel identification are available for use in the UC network: 1) binary channel number assigned to the channel and 2) a slot map that identifies the time slots used by the channel. The parameter shall be coded exclusively for one method depending on the number/map parameter information. Both PRIs, 1.544 Mbps and 2.048 Mbps, shall be supported IAW the slot map in ITU-T Q.931.

(4) Transit Network Selection IE. The Transit Network Selection IE identifies one requested transit network. It may be repeated in a message to select a sequence of transit networks through which a call must pass. For example, the element may be used in a SETUP message to specify one or a sequence of transit networks (other than the user-assigned transit network) through which a call must pass. In the case of UC user-to-network signaling, this IE shall be used to specify the UC network or a network other than the UC network as a transit network. (DoD networks and foreign PTTs are examples.)

(5) Cause IE. The Cause IE shall be IAW ANSI T1.619a.

(6) Signal IE. The Signal IE shall be IAW ANSI T1.619a. The signal shall be included in the DISCONNECT, PROGRESS, and SETUP messages, as appropriate, for the MLPP feature.

(7) Notification Indicator IE. The Notification Indicator IE, which indicates information pertaining to a call, shall contain the notification description code of "0 0 0 0 1 0 0" (value 4) for the MLPP feature to indicate to the calling user a possible call completion delay when an LFB query is invoked in response to an MLPP call setup.

2.25.2.7.1.4.6 Supplementary Services

SCM-013030 [**Conditional: TA, IAD, MG, SC, SS**] If provided, Supplementary Services shall be provided IAW the following standards:

a. ANSI T1.607-1998.
b. ANSI T1.613-1992.
c. ANSI T1.616-1992.
d. ANSI T1.621-1992.
e. ANSI T1.632-1993.
f. ANSI T1.642-1993.
g. ANSI T1.643-1995.
h. ANSI T1.647-1995.

2.25.3 ISDN

SCM-013040 [**Required**] The UC signaling appliance systems shall provide the ISDN BRI and PRI capabilities shown in Tables 2.25-9 through 2.25-13 that are marked with an R. The UC signaling appliance systems may provide the ISDN BRI and PRI capabilities shown in Tables 2.25-9 through 2.25-13 that are marked with an O, indicating Optional.

Tables 3-1 through 3-5 of Telcordia Technologies SR 3476 provide the specific requirements for features and capabilities listed in Tables 2.25-9 through 2.25-13. The MLPP interactions with ISDN are identified in Section 2.25.1, Multilevel Precedence and Preemption.

Table 2.25-9. BRI Access, Call Control, and Signaling

RQMT NO.	IAD/TA	SC MG	SS MG	SC	SS	FEATURE OR CAPABILITY
SCM-013050	O			O	O	ISDN BRI Layer 1
SCM-013060	O			O	O	4:1 Time Division Multiplex Method for ISDN Basic Access

RQMT NO.	IAD/TA	SC MG	SS MG	SC	SS	FEATURE OR CAPABILITY
SCM-013070	O			O	O	ISDN BRI Layer 2
SCM-013080	O			O	O	BRI Circuit-Mode Call Control Basic Call Control
SCM-013090	O			O	O	BRI Terminal initialization
SCM-013100	O			O	O	Service Profile Identifier
SCM-013110	O			O	O	Parameter Downloading
SCM-013120	O			O	O	Default Services for Terminals

Table 2.25-10. Uniform Interface Configurations for BRIs

RQMT NO.	TA/ IAD	SC MG	SS MG	SC	SS	FEATURE OR CAPABILITY
SCM-013130	O			O	O	Uniform Interface Configurations for BRIs. Single User with Multiple Applications Two Users Sharing a BRI
SCM-013140	O			O	O	More than two B-Channel Terminals on a BRI (Passive Bus)
SCM-013150	O			O	O	Associated Group Indicator
SCM-013160	O			O	O	DN Sharing over Multiple Call Types on an Integrated Terminal
SCM-013170	O			O	O	Non-Initializing Terminals

Table 2.25-11. BRI Features

RQMT NO.	TA/ IAD	SC MG	SS MG	SC	SS	FEATURE OR CAPABILITY
SCM-013180	O			O	O	Electronic Key Telephone Systems Multiple DNs per Terminal Analog Member of an EKTS Group Multiple DN Appearances per Call Appearance Call Handling Hold/Retrieve Bridging/DN-Bridging Intercom Calling Membership in a Multiline Hunt Group Abbreviated and Delayed Ringing

RQMT NO.	TA/ IAD	SC MG	SS MG	SC	SS	FEATURE OR CAPABILITY
						Automatic and/or Manual Bridged Call Exclusion
SCM-013190	O			O	O	Call Forwarding
SCM-013200	O			O	O	Call Forwarding Variable Courtesy Call Reminder Notification Call Forwarding Interface Busy Call Forwarding Don't Answer Call Forwarding Intragroup Only Call Forwarding Interface Busy Incoming Only Call Forwarding Don't Answer Incoming Only
SCM-013210	O			O	O	ISDN Call Hold Hold and Retrieve
SCM-013220	O			O	O	Flexible Calling Three-Way and Six-Way Calling Consultation Hold Conference Hold and Retrieve
SCM-013230	O			O	O	ISDN Display Service Protocol and Procedures Uniform Text (for NI-2 Uniform Services)
SCM-013240	O			O	O	Basic Business Group Denied Originating Denied Terminating Distinctive Alerting Indication
SCM-013250	O			O	O	Business Group Dial Access Features
SCM-013260	O			O	O	Dial Access to Automatic Flexible Routing
SCM-013270	O			O	O	Customer Access Treatment Code Restriction
SCM-013280	O			O	O	Code Restriction and Diversion
SCM-013290	O			O	O	Direct Outward Dialing
SCM-013300	O			O	O	Direct Inward Dialing
SCM-013310	O			O	O	ISDN Call Pickup

RQMT NO.	TA/ IAD	SC MG	SS MG	SC	SS	FEATURE OR CAPABILITY
SCM-013320	O			O	O	ISDN Directed Call Pickup
SCM-013330	O			O	O	Access To Analog Attendant Access Station Message Detail Recording Tracing of Terminating Calls Tandem Call Tracing Trace of a Call In Progress Bulk Calling Line Identification Selective Call Acceptance Selective Call Forwarding Selective Call Rejection
SCM-013340	O			O	O	Limitations and Restrictions for 911 PSAP – Call Hold Not Allowed for a 911 Call

Table 2.25-12. PRI Access, Call Control, and Signaling

RQMT NO.	TA/ IAD	SC MG	SS MG	SC	SS	FEATURE OR CAPABILITY
SCM-013350		R	R	R	R	PRI Layer 1
SCM-013360		R	R	R	R	PRI Layer 2 (Circuit)
SCM-013370		R	R	R	R	PRI Call Control and Signaling
SCM-013380		R	R	R	R	Basic Call Control for Circuit Mode Calls
SCM-013390		R	R	R	R	Multiple DS1 Facilities Controlled by a Single D-Channel
SCM-013400		R	R	R	R	Access to Selected Primary Rate Services on a Per-Call Basis

Table 2.25-13. PRI Features

RQMT NO.	TA/ IAD	SC MG	SS MG	SC	SS	FEATURE OR CAPABILITY
SCM-013410		O	O	O	O	Call-by-Call Service Selection FX Non-ISDN Tie IN WATS OUT WATS Non-ISDN ETN
SCM-013420		O	O	O	O	Interworking with Private Networks

2.25.4 Backup Power

SCM-013430 [**Required: TA, IAD, MG, SC, SS**] UC shall have backup power to maintain continuous operation whenever the primary source of power is disrupted. Back-up power design and implementation shall be incorporated into the design to assure that UC meets the reliability requirements of UCR 2013, Section 15, Reliability. General power requirements are described in Telcordia Technologies GR-513-CORE. Following the risk avoidance guidance in Telcordia Technologies GR-513-CORE, the backup power design shall minimize the probability of a complete loss of UC appliance system power.

2.25.4.1 UPS

The requirements for UPS in the following paragraphs are bare minimum essential requirements and may not assure the design goal of continuous operation.

2.25.4.1.1 UPS Load Capacity

SCM-013440 [**Required: TA, IAD, MG, SC, SS**] The Uninterruptible Power Supply (UPS) shall provide greater than 8 hours of mission busy hour current load requirements (rated in Ampere hours) plus at least 10 percent for UC equipment to include ancillary equipments.

2.25.4.2 Backup Power (Environmental)

SCM-013450 [**Required: SC, SS**] The backup power system shall have the capacity to operate environmental systems required to sustain continuous operation of UC appliance systems equipment to include ancillary equipments. Power to the environmental systems may not need to be continuous.

2.25.4.3 Alarms

SCM-013460 [**Required: TA, IAD, MG, SC, SS**] Power system alarms shall be generated to an attended monitoring location whenever there is a loss of power and shall remain until the power is restored. Power alarms shall remain active until the condition that activated the alarm is corrected.

2.25.5 Echo Canceller

This section provides the requirements for echo control equipment in the UC network. All MG EC devices are required to meet the requirements in the following paragraphs.

2.25.5.1 EC Functionality

SCM-013470 [**Required: SC MG, SS MG**] The EC shall meet the requirements of ITU T Recommendation G.165, ITU-T Recommendation G.168, and Telcordia Technologies Special Report, SR-2275, Section 7, Transmission.

SCM-013480 [**Required: SC MG, SS MG**] The EC shall support at least 64 ms echo tail length.

SCM-013490 [**Required: SC MG, SS MG**] The MOS technique, if applicable, and the perceptual evaluation of speech quality (PESQ) measurement, ITU-T Recommendation P.862 shall be used to assess the clarity of end-to-end voice circuits on which ECs are installed. The voice quality shall have an MOS of 4.0 or better, as measured IAW DoD Information Technology Standards Registry (DISR) voice quality standards.

SCM-013500 [**Required: SC MG, SS MG**] The MG EC shall be able to determine when a new call is being established and apply echo cancellation IAW this section.

SCM-013510 [**Required: SC MG, SS MG**] The EC shall have Normal and Forced Off operational states and they shall be settable by the EMS (see Section 2.25.5.1.5, Device Management), local control interface, or front/back control panel on a per DS0 basis:

SCM-013520 [**Required: SC MG, SS MG**] The Echo cancellation in the Normal operational state will remain in the enabled state between calls and during calls unless it is disabled as defined in this section.

SCM-013530 [**Required: SC MG, SS MG**] In the Forced Off state, the echo canceller shall not enable echo cancellation until the forced-off state has been changed.

2.25.5.2 2100-Hertz EC Disabling Tone Capability

SCM-013540 [**Required: SC MG, SS MG**] On a per-channel basis, a 2100 Hertz (Hz) disabling tone shall be recognized by the EC, causing the EC to disable, as specified in ITU-T Recommendation G.168.

SCM-013550 [**Required: SC MG, SS MG**] Re-enabling the EC, after the echo cancellation function has been disabled by the tone, it shall remain in a disabled state until one of the following events occurs.

a. No single-frequency sinusoid is present as defined in ITU-T Recommendation G.168, Section 7.

b. The end of the call is detected.

c. The end of data transmission is detected. This may be detected either by the lack of modem or fax tones on the channel, or by some proprietary method.

SCM-013560 [**Required: SC MG, SS MG**] Echo cancellers shall be capable of determining when a channel is in use (i.e., a call is active on the channel) or not. This function shall not interfere in any manner with an active call.

SCM-013570 [**Required: SC MG, SS MG**] The 2100 Hz disabling tone shall override all other control functions and shall disable echo cancellation for that particular call.

2.25.5.3 EC Hardware

SCM-013580 [**Required: SC MG, SS MG**] The EC shall be able to be connected to either analog and/or digital transmission facilities.

SCM-013590 [**Optional: SC MG, SS MG**] An analog trunk interface shall be able to provide echo cancellation on a per-trunk basis.

SCM-013600 [**Optional: SC MG, SS MG**] A digital trunk interface shall be implemented on a digital basis without conversion to analog. The digital EC shall treat all DS0 channels (PCM-24, PCM-30, or more for SONET) independently.

2.25.5.4 Echo Cancellation on PCM Circuits

SCM-013610 [**Required: SC MG, SS MG**] The PCM-24 or PCM-30 interfaces shall be IAW the requirements in ANSI T1.102, "Digital Hierarchy – Electrical Interfaces" (for PCM-25) and ITU-T Recommendations G.703 and G.732 (for PCM-30).

SCM-013620 [**Required: SC MG, SS MG**] When the bearer channel is used for 56 or 64 Kbps digital data or submultiples of 64 Kbps, the digital ECs shall not cause a loss of bit integrity.

SCM-013630 [**Required: SC MG, SS MG**] Echo cancellers inserted in a PCM-24 path using CAS (i.e., "robbed bit") shall have a selectable setting to exclude the signaling bits from the cancellation process.

SCM-013640 [**Required: SC MG, SS MG**] The EC shall be capable of performing echo cancellation for speech and audio bearer capability calls on the full 64 Kbps signal.

2.25.5.5 Device Management

SCM-013650 [**Required: SC MG, SS MG**] All UC EC devices will be monitored and managed by the remote VVoIP EMS, as described in Section 2.19.2, Requirements for FCAPS Management.

SCM-013660 [**Required: SC MG, SS MG**] Echo cancellers shall be capable of performing a self-test diagnostic function on nonactive and active channels on a noninterference basis and report any failures to the assigned EMS.

SCM-013670 [**Required: SC MG, SS MG**] The EC shall program its echo cancellation capability based on input via a direct connection to the external communications port, or using the front/ back programming panel, or by MG datafill.

2.25.5.6 Reliability

SCM-013680 [**Required: SC MG, SS MG**] The EC reliability and availability shall conform to Section 5 of Telcordia Technologies GR-512-CORE, as specified for individual devices. The vendor shall provide a reliability model for the system, showing all calculations along with how the overall availability will be met, if requested.

2.25.6 VoIP System Latency for MG Trunk Traffic

The System defined for the requirements in this section is the combination of the SC/SS and its MGs, PEIs and AEIs, IADs, and ATAs. The requirements in this section apply to the system as a whole and not to the individual components of the system.

SCM-013690 [**Required: SC, SS**] When bearer traffic exits the system via a TDM MG trunk interface, the one-way system latency shall not be greater than 65 ms averaged over any 5-minute period. The latency shall be measured from the EI handset to egress from the system via a TDM trunk. This latency shall be measured for all types of EIs offered by the System.

SCM-013700 [**Required: SC, SS**] When bearer traffic enters the system via a TDM MG trunk interface, the one-way system latency shall not be greater than 85 ms averaged over any 5-minute period. The latency shall be measured from the system TDM ingress to the EI handset. This latency shall be measured for all types of EIs offered by the System.

2.26 UC STATEFUL FIREWALL

2.26.1 Role of the UCSF

The UCR contains the specifications for a voice and video firewall called an SBC. The SBC is placed at the edge of the enclave B/P/C/S and sits between the LANs and the WAN. The SBC protects voice and video devices from attacks that originate outside of the enclave. The SBC requirements are presented in Section 2.17, SBC.

The role of the UC Stateful Firewall (UCSF) is to protect an SC or SS from attacks that originate from inside of the enclave. The Joint Interoperability Test Command (JITC) has validated that SCs and SSs have acceptable Information Assurance risks for most deployments. Therefore, the use of the UCSF is not universally mandated. However, some sites may determine that additional protection is required because of the risks associated with their unique scenario. When this occurs, the UCSF may be deployed to provide additional protection.

The UCSF is considered a UC Approved Products List (APL) product. UC APL products are also called Systems Under Test (SUTs). The RSF is a standalone APL product and therefore a standalone SUT. The RSF SUT is not part of the SC SUT or the SS SUT.

2.26.2 UCSF Requirements

2.26.2.1 UCSF General

SCM-013710 [**Required: UCSF**] The UCSF shall meet all SBC requirements with the exception of the requirements specified in Section 2.26.2.2, UCSF Enjoined Behavior.

SCM-013720 [**Required: UCSF**] The UCSF shall maintain a persistent TLS session with the SBC within the UCSF's enclave. Persistent means that the TLS session is established when the UCSF system joins the signaling network and is not established on a VVoIP/AS-SIP session-by-session basis.

SCM-013730 [**Required: UCSF**] The UCSF shall fulfill the same availability requirements as the SC that the UCSF is protecting. If the SC's availability requirement is 99.999, then the UCSF's availability requirement is also 99.999.

NOTE: With a few exceptions, the UCSF and the SBC perform the same functions. The functions performed by the UCSF are a very large subset of the functions performed by the SBC. These functions can be performed by the same hardware and software on both the UCSF and the SBC. Although the software may be the same, the UCSF's software configuration is typically different from the SBC's software configuration.

The hardware configuration used at a specific site is determined by the site's specific availability requirements, as defined in Section 2.17.6, Availability. At a specific site, both the UCSF and the SBC are subject to the same availability requirements. Although the availability requirements are the same, appliances from different vendors may be used. Using the same vendor's appliance for the UCSF and the SBC is not required.

2.26.2.2 UCSF Enjoined Behavior

SCM-013740 [**Required: UCSF**] The UCSF shall not take any corrective actions upon the SC failover from the primary SS to the secondary SS. The SBC-required actions upon failover from the primary SS to the secondary SS are described in Section 2.6. The UCSF shall not perform these actions.

SCM-013750 [**Required: UCSF**] The UCSF shall not bidirectionally anchor (NAT and/or NAPT) the media associated with a voice or video session that originates or terminates within its enclave. The SBC requirements for bidirectionally anchoring the media are described in Section 2.17.1, AS-SIP Back to Back User Agent. The UCSF shall not perform these actions.

SCM-013760 [**Required: UCSF**] The UCSF shall not maintain a persistent TLS session with SBCs that are outside of the UCSF's enclave. The SBC's requirements for maintaining persistent TLS connections with SBCs that are outside of the local enclave are described in Section 2.17.1, AS-SIP Back to Back User Agent. The UCSF shall not perform these actions.

SECTION 3
AUXILIARY SERVICES

3.1 INTRODUCTION

This section addresses required functionality, performance, capabilities, and associated technical parameters for Auxiliary Services and Systems.

3.2 DIRECTORY SERVICES ("WHITE PAGES")

AUX-000010 [**Required: CVVoIP Directory Service**] The Classified Voice and Video over Internet Protocol (CVVoIP) shall have a directory service capability for searching white pages that allows subscribers to look up specific and applicable user information assigned to other CVVoIP subscribers. This is considered a requirement and is included for consideration by the CVVoIP Session Controller/Softswitch (SC/SS) product development teams.

AUX-000020 [**Required: CVVoIP Directory Service**] For security reasons, the CVVoIP directory system shall be a separate implementation from the sensitive but unclassified (SBU) Voice and Video over Internet Protocol (VVoIP) directory system.

AUX-000030 [**Required: CVVoIP Directory Service**] A centralized, multivendor supported, standards-based directory schema shall be implemented.

Figure 3.2-1, Centralized Directory (White Pages) Service, illustrates the white pages directory arrangement.

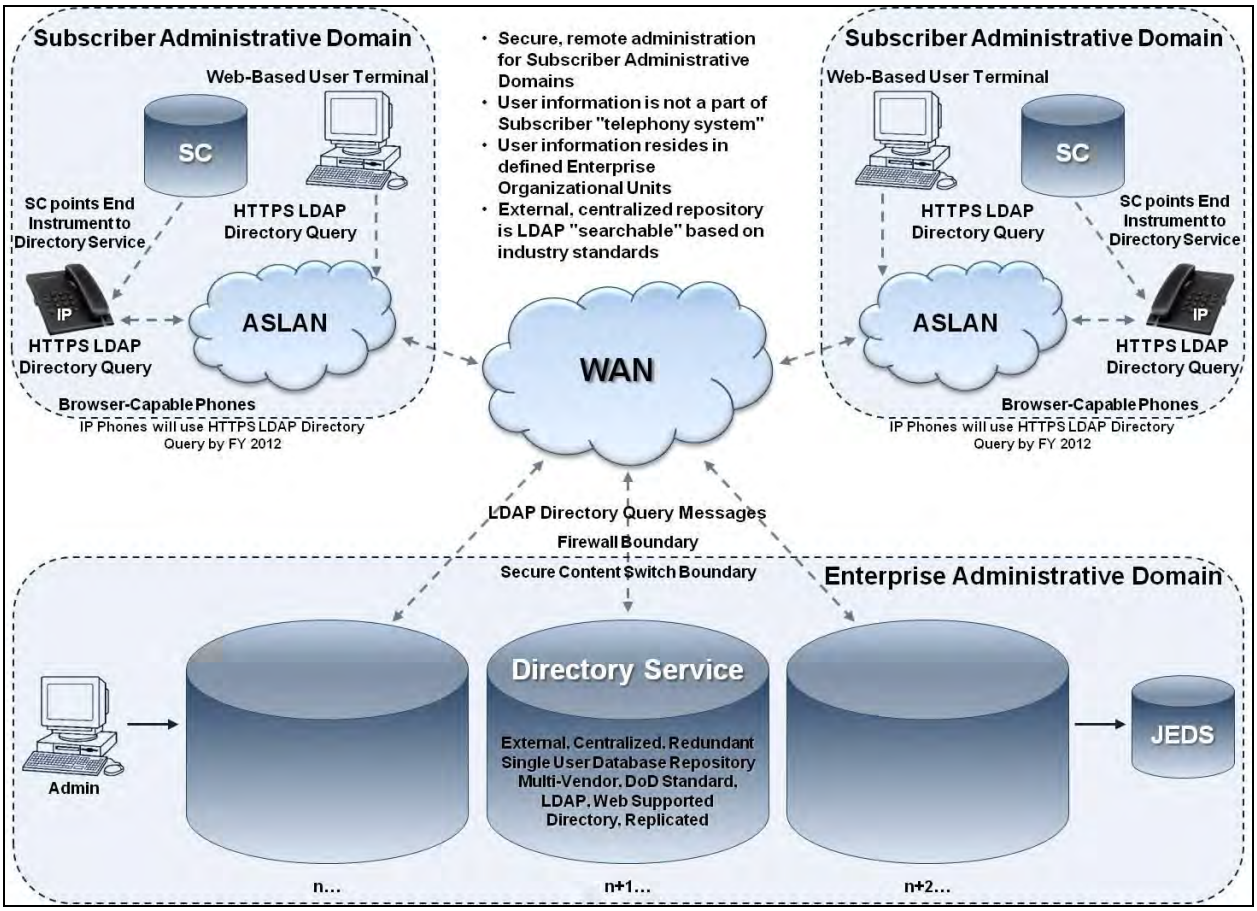


Figure 3.2-1. Centralized Directory (White Pages) Service

3.2.1 General Requirements for Centralized Directory (White Pages) Service

The general requirements that follow have been defined for the centralized directory (white pages) service.

3.2.1.1 Use of External and Centralized "Corporate" Directory

AUX-000040 [**Required: CVVoIP Directory Service**] Location and Architecture Design. The global Directories Services architecture shall be consolidated and external to all other attached subscriber "telephony systems." The architecture shall be distributed in design to support redundancy and survivability as illustrated in Figure 3.2-1. All telephony user information shall reside within the centralized Directory Services database.

AUX-000050 [**Required: CVVoIP Directory Service**] Maintenance, Administrative, and Management Responsibility. The overall responsibility to maintain the global Directory Services' user database structure shall reside with the Defense Information Systems Agency (DISA), with management of individual organizational units being delegated to each individual

SC/SS telephony system administrator. This decentralized administrative responsibility within the overall schema will ensure a constant and updated database of user information.

AUX-000060 [**Required: CVVoIP Directory Service**] Synchronization with the Local (SC/SS) and Defense RED Switch Network (DRSN) Directories. The local CVVoIP SC/SS user database for each organizational unit shall be automatically synchronized within the larger Directory Services server architecture as soon as the SC/SS administrator provisions the user information within the system. Individual SC/SS administrators shall be responsible for provisioning user information at the same time the provisioning of phone devices is accomplished. This ensures a constantly maintained, real-time database repository of user information for the white pages search and lookup functionality.

The DRSN directory information shall be the responsibility of DISA and shall be statically updated as DRSN systems are modified and user information is updated from the field. At a minimum, this is expected to be accomplished at least once a year.

AUX-000070 [**Required: CVVoIP Directory Service**] Redundancy, Survivability, and Recovery. Redundancy and survivability, as well as disaster recovery, are designed into the Directory Service architecture. DISA shall be responsible for the design, maintenance, and backup of the system.

3.2.1.2 Definition of Multivendor Standards Items

AUX-000080 [**Required: CVVoIP Directory Service**] Defined Attributes (Common Set of Fields). The CVVoIP Directory Service shall support the following Defined Attributes, per Figure 3.2-2, Directory Service Attribute Information.

Attribute Name	Attribute Description	Mandatory/ Optional/ Not Applicable	Search [P/W/ BOTH]	Display [P/W/ BOTH]	Comments – Layman's terminology
givenName	First Name	M		BOTH	First Name
sn	Last Name (Surname)	M	BOTH	BOTH	Last Name
displayName	Display-Name (first + last) or custom	NA			Automated – combined display field of First Name and Last Name
initials	Initials	O			Initials
middleName	Other-Name	O			Middle Name or Initial
generationQualifier	Generation-Qualifier	O			Suffix
employeeID	Employee-ID	M			EDIPI Electronic Data Interchange Person Identifier (CAC)
employeeType	Employee-Type	M			Personnel Type (e.g., Civilian, Contractor, Military)
employeeNumber	Employee-Number	O			PIN Number
title	Title	M	BOTH	BOTH	Rank
userPassword	User-Password	O			User Password
mail	E-Mail-Addresses	O			Email SIPR Address
telephoneNumber	Telephone-Number	M		WEB	DSN/PSTN Telephone #
ipPhone	Phone-Ip-Primary	M		BOTH	VoSIP Telephone #
facsimileTelephoneNumber	Facsimile-Telephone-Number	NA			RESERVED
pager	Phone-Pager-Primary	NA			CMS Telephone N#
otherTelephone	Phone-Office-Other	O		WEB	DRSN Telephone #
otherFacsimileTelephoneNumber	Phone-Fax-Other	NA			RESERVED
otherHomePhone	Phone-Other-Home	NA			RESERVED
otherIpPhone	Phone-Ip-Other	NA			JWICS Telephone #
otherMobile	Phone-Mobile-Other	NA			RESERVED
otherPager	Phone-Pager-Other	NA			RESERVED
o	Organization-Name	M		WEB	Military Branch (e.g., AR, AF, NV, MC, DOD, CIV)
company	Company	M		WEB	COCOM/MAJCOM/DIVISION (e.g., CENTCOM, SOCOM, AMC, 10th Mtn, AFMC)
department	Department	M	BOTH	BOTH	Unit (e.g., 2/75th RNG BN, 379th AEW, 2CSF)
physicalDeliveryOfficeName	Physical-Delivery-Office-Name	M	BOTH	BOTH	C/P/S (e.g., Camp/Post/Station – MacDill AFB, Ft Hood)
flags	Flags	M			Set to 1000 to make each OU searchable
userCert	User-Cert	NA			Future Use – SPM
userCertificate	X509-Cert	NA			Future Use – SPM
userPKCS12	PKCS #12 PFX PDU for exchange of personal identity information	NA			Future Use – SPM

Figure 3.2-2. Directory Service Attribute Information

AUX-000090 [**Required: CVVoIP Directory Service**] Length and ASCII Characters of Each Attribute Field. ASCII characters shall be limited to characters that are supported by both SC/SS enclaves and the DRSN system. These are necessary to ensure proper display of white pages results. Alphanumeric characters that are supported shall be (0123…, abcd…, ABCD), periods (.), dashes (-), and commas (,).

Length of fields shall be configurable and shall be the basis of what is supported.

AUX-000100 [**Required: CVVoIP Directory Service**] "Ownership," administration, and management responsibility of each organizational unit and its fields. Each individual SC/SS administrator shall "own" and be responsible for the administration and management of each user's information governed by its telephony system. As each phone is provisioned and assigned within this system, the applicable user information shall be added to, modified in, and/or deleted from the assigned Directory Service organizational unit within the domain. Each SC/SS administrator shall use the designed provisioning tool that DISA has developed which simplifies the task and ensures continuity of required user database information.

3.2.1.3 Search Criteria and Display Presentation for EIs (Computers and IP Phones

AUX-000110 [**Required: CVVoIP Directory Service**] The CVVoIP Directory Service shall support the following Search Criteria and Display Presentation for End Instruments (EIs), per Figure 3.2-3, Directory Service Search and Display Criteria.

On the IP Phone		On the Computer Web Page	
Search Fields Layman's Terms (Attribute)	Display Order Layman's Terms (Attribute)	Search Fields Layman's Terms (Attribute)	Display Order Layman's Terms (Attribute)
Last name (sn)	VoSIP Telephone # (ip Phone)	Last name (sn)	VoSIP Telephone # (ip Phone)
Unit (department)	Last name (sn)	Unit (department)	Last name (sn)
Rank (title)	First name (givenName)	Rank (title)	First name (givenName)
C/P/S (physicalDeliveryOfficeName)	Rank (title)	C/P/S (physicalDeliveryOfficeName)	Rank (title)
	Unit (department)		Unit (department)
			C/P/S (physicalDeliveryOfficeName)
			COCOM/MAJCOM/DIVISION (company)
			Military Branch (o)
			DSN/PSTN Telephone # (phoneNumber)
			DRSN Telephone # (otherTelephone)

Figure 3.2-3. Directory Service Search and Display Criteria

AUX-000120 [**Required: CVVoIP Directory Service**] Lightweight Directory Access Protocol (LDAP) Criteria and Browser (Display) Functionality. Industry standard LDAP connection protocols (port 389) shall be used and supported.

AUX-000130 [**Required: CVVoIP Directory Service**] Standardized browser support for computer white pages functionality (parsing and display of search results) shall be restricted to secure Web protocols [Transport Layer Security (TLS)/Hypertext Transport Protocol Secure (HTTPS)] only. This shall be part of the Directory Services architecture capability and shall ensure the privacy and security of user information to authorized viewers.

AUX-000140 [**Required: CVVoIP Directory Service**] Standardized browser support for Internet protocol (IP) phone white pages functionality (parsing and display of search results) shall be mandatory, so that Web-based [Hypertext Markup Language (HTML)/Extensible HTML (XHTML)] user information can be displayed. As of calendar year (CY) 2012, display of unsecure Web protocols is no longer supported [Hypertext Transport Protocol (HTTP)]. As of CY 2012, only secure Web protocols (TLS/HTTPS) shall be supported.

AUX-000150 [**Required: CVVoIP Directory Service**] The CVVoIP Directory Service shall support the following Definitions of EI Display Fields:

a. Browser Requirements. EIs (e.g., IP Phones) shall support HTML/XHTML-based (http://www.w3.org/TR/xhtml1/) rendering of content. Computers (e.g., Web browsers) with HTML-based applications, such as Microsoft Internet Explorer version 7.X, 8.X, and 9.X, are recommended.

b. Character Fields (Attributes). See Figure 3.2-3, Directory Service Search and Display Criteria, for details.

c. Length of Attribute Fields.

(1) Web Browsers. The length of the displayed fields on the Web interface of a computer shall be matched and validated with the limitations/policies imposed by the underlying directory server schema definition. Search results shall be presented in multiple lines with more display information available because of the size of the screening area. On each line, the Web browser shall display the data representing the attributes for the matched (found) entries as concatenated together using various delimiters (such as "," "-," "/"). The length of the information being displayed on the Web browser interface shall be configurable to be truncated to preset values on a per-attribute basis. This shall be accomplished using the Directory Service Web-based administrative interface. If attributes with additional characters are stored in the underlying directory server, then the Web-based user interface shall truncate the displayed content to the limits imposed by the Directory Service application configuration parameters. All these parameters shall be set to optimal lengths, given the size of the screening area that computers offer.

(2) End Instruments. Search results shall be presented in multiple lines. On each line, the phone shall display the data representing the matched entries' attributes, as concatenated together using various delimiters (such as "," "-," "/") with a maximum of 64 characters per line. If attributes with additional characters are stored in the underlying directory server, then the phone user interface shall truncate the displayed content to the limits imposed by the phone device and as defined in the Directory Service application configuration parameters.

d. How Many/Which Fields of Identification. See Figure 3.2-3, Directory Service Search and Display Criteria, for details.

e. Soft/Hard Key Functions (such as a "directory access button"). The CVVoIP SC/SS manufacturers shall provide a single action, "directory access" function, through software and/or hardware, on all supported, Joint Interoperability Test Command (JITC)-certified IP Phones. Through these methods, the action shall be a programmable, Web-based function key that can have a Uniform Resource Locator (URL). This shall allow users to have the capability to use one button to start all actions when using the Directory Service.

3.3 ROUTING DATABASE

3.3.1 Introduction

This section specifies DISA requirements for the Routing Database, the Commercial Cost Avoidance feature, and the Hybrid Routing (HR) feature.

These requirements apply to these Unified Capabilities (UC) Approved Product List (APL) Products:

- The SS.
- The SC.
- The Local Routing Database (LRDB).
- The Master Routing Database (MRDB).

These requirements are organized into four areas:

- SS-to- LRDB queries for HR.
- SC-to-LRDB queries for Commercial Cost Avoidance.
- SC-to-MRDB updates [for Defense Switched Network (DSN) numbers and commercial numbers].
- LRDB and MRDB functional requirements.

Figure 3.3-1, Routing Database Architecture: SS, shows the basic architecture that is used for these initial Routing Database requirements. This architecture and these requirements are intended to be generic, and to support interoperability between multiple SS, SC, and Routing Database vendors. A multi-vendor interoperable protocol is used between network elements from different vendors (e.g., an SS or SC from one vendor, and an LRDB from another vendor).

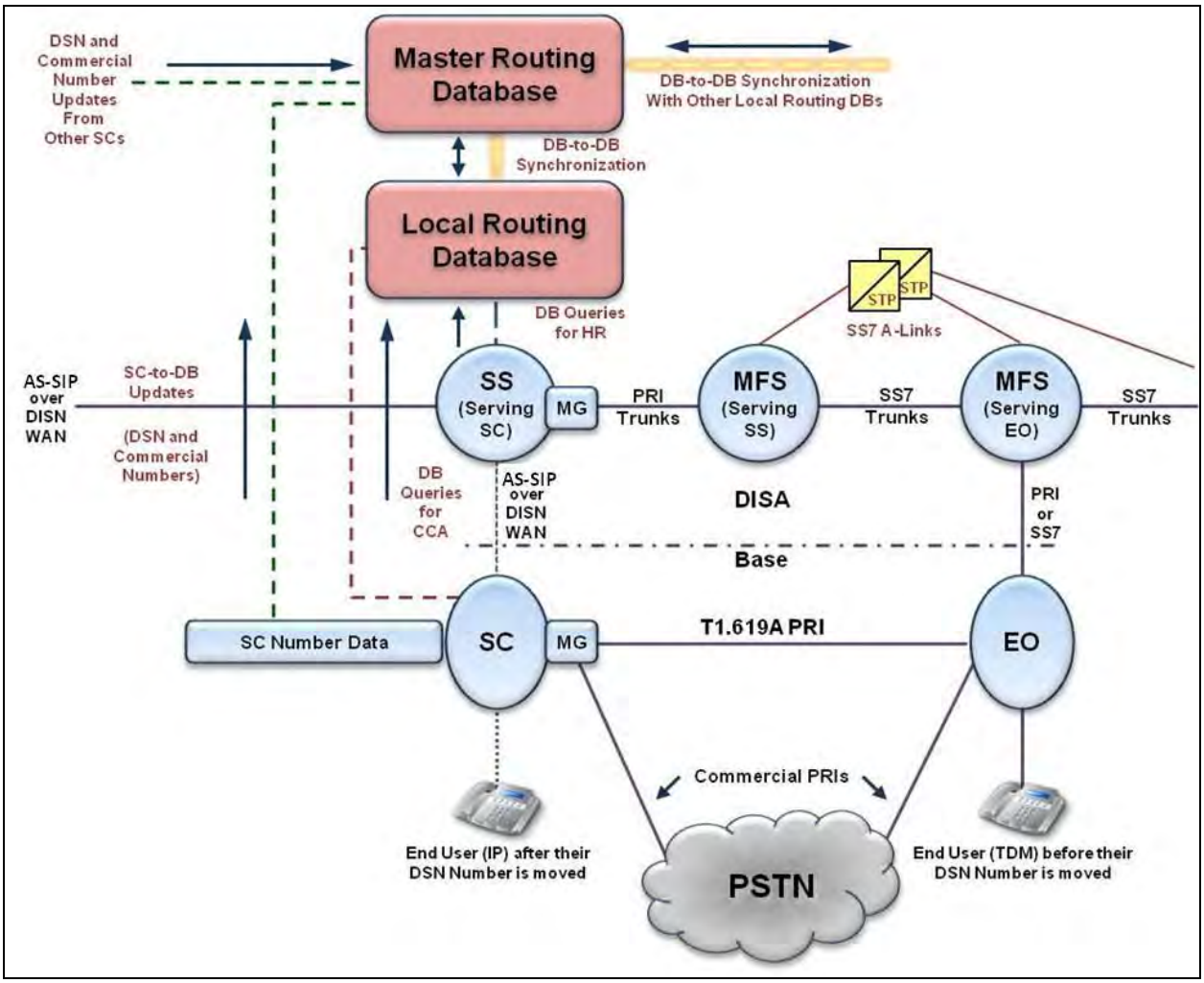


Figure 3.3-1. Routing Database Architecture: SS

3.3.1.1 Assumptions

The SC, LRDB, and MRDB requirements in this section are based on the following assumptions:

- These requirements assume that a Multi-Vendor-Interoperable (MVI) Protocol is used on the following interfaces:
  - The interface between the SS and the LRDB for HR queries and responses.
  - The interface between the SC and the LRDB for Commercial Cost Avoidance queries and responses.
  - The interface between the SC and the MRDB for Database updates (transfers of DSN and commercial numbers from the SC to the MRDB).
  - The interface between the LRDB and MRDB for Database-to-Database synchronization.

  The MVI Protocol used here is LDAP Version 3 (LDAPv3).

- A Routing Database "data schema" is needed to specify the "information elements" that are included in the Database queries for HR (SS ⇔ LRDB), the Database queries for Commercial Cost Avoidance (SC ⇔ LRDB), the Database updates (SC ⇔ MRDB), and the Database synchronization messages (LRDB ⇔ MRDB). For these requirements, this data schema is based on LDAPv3.
- Examples of information that needs to be included in the various Database queries, Database responses, and Database updates follow:
  - The Database queries for HR need to contain the full 10-digit DSN called number.
  - The Database responses for HR need to indicate either the "number not found" or the "number found" along with an identifier for the destination SC for that DSN called number. [The SC identifier could also be absent when the number is found, meaning that the number is located on an End Office (EO)]. The responses also should contain an identifier for the primary SS that serves that SC, and an identifier for the backup SS that serves that SC. The Call Connection Agent (CCA) Identifier (CCA-ID) is the required identifier for the destination SC, the primary SS, and the backup SS in this case.
  - The Database queries for Commercial Cost Avoidance need to contain the full internationally significant commercial called number [in the format of "Country Code (CC) plus Nationally Significant Number (NSN)"].
  - The Database responses for Commercial Cost Avoidance need to either indicate "number not found," or contain the full 10-digit DSN called number that matches the commercial called number.
  - The Database updates (SC-to-MRDB) need to contain the full DSN called number, the full commercial called number, the identifier of the source SC, the identifier of the primary SS for that SC, and the identifier of the backup SS for that SC. The CCA-ID is the recommended identifier for the SC, primary SS, and backup SS in this case.

3.3.2 SS to LRDB Interface: Database Queries for HR

The requirements in this section apply to the SS and the LRDB. The LRDB can be located in a site that is physically remote from the SS site.

AUX-000160 [**Required: SS, LRDB**] The SS and the LRDB shall support the HR feature per the requirements in this section.

AUX-000170 [**Required: SS**] The SS shall support an interface to a LRDB to support Database queries and Database responses for the HR feature.

AUX-000180 [**Required: LRDB**] The LRDB shall support an interface to the SS to support Database queries and Database responses for the HR feature.

AUX-000190 [**Required: SS, LRDB**] The query-response interface between the SS and the LRDB shall be LDAPv3 over TLS over IP. On the SS, this LDAPv3 interface shall be compliant with RFC 4511 and all the LDAP technical specifications listed in Section 1 of RFC 4510. On the LRDB, see the LDAPv3 interface requirements in Section 3.3.5.2.1, General Architecture, Protocols, and Interfaces.

AUX-000200 [**Required: SS, LRDB**] The encoding of the LDAPv3 messages and data schema used on the Database query interface between the SS and the LRDB shall follow the Basic Encoding Rules (BERs) of Abstract Syntax Notation One (ASN.1). On the SS, this encoding shall be consistent with Section 5.1, Protocol Encoding, of RFC 4511, June 2006, as referenced by RFC 4510. On the LRDB, see the LDAPv3 interface requirements in Section 3.3.5.2.1, General Architecture, Protocols, and Interfaces.

AUX-000210 [**Required: SS, LRDB**] The interface between the SS and the LRDB shall be secured using TLS, consistent with the requirements for securing Assured Services (AS) Session Initiation Protocol (SIP) (AS-SIP) messages using TLS in Section 4, Information Assurance. This security shall provide mutual authentication between the SS and the LRDB, message confidentiality for the Database query and Database response, and message integrity for the Database query and Database response.

AUX-000220 [**Required: SS, LRDB**] The interface between the SS and the LRDB shall traverse the data firewalls (and not the Session Border Controller [SBC] firewalls) at both the SS and the LRDB sites.

AUX-000230 [**Required: SS, LRDB**] The interface between the SS or SS and the LRDB shall traverse the Customer Edge (CE) Routers at both the SS and the LRDB sites, using the Differentiated Services Code Point (DSCP) for User Signaling traffic, and the associated CE Router (CE-R) queues.

AUX-000240 [**Required: SS**] The interface between the SS and the LRDB shall terminate on the Ethernet interface used for VVoIP signaling traffic at the SS, as described in Section 4, Information Assurance.

AUX-000250 [**Required: SS**] The SS shall allow HR to be activated for all calls going through the SS. The SS also shall allow HR to be activated only for calls going through the SS to a specific set of DSN numbers. In this second case, the SS shall allow DISA to configure the set of DSN numbers for which HR is activated.

AUX-000260 [**Required: SS**] The DISA-configurable set of DSN numbers for HR shall support the following elements:

a. Individual 10-digit numbers from the UC numbering plan.

b. Ranges of 10-digit numbers from the UC numbering plan.

   Each range shall be configurable so that DISA can specify the first and last numbers in the range.

AUX-000270 [**Required: SS**] The SS shall allow a configurable range to include one of the following:

a. An entire DSN Area Code (first three digits specified).

b. An entire DSN Area Code and Office Code (first six digits specified).

c. A "thousands group" within a DSN Area Code and Office Code (first seven digits specified).

d. A "hundreds group" within a DSN Area Code and Office Code (first eight digits specified).

e. A "tens group" within a DSN Area Code and Office Code (first nine digits specified).

AUX-000270.a [**Optional: SS**] DISA also shall be able to independently specify the first and last numbers in a range without having to limit that range to a single Area Code, a single Office Code, a single thousands group, a single hundreds group, or a single tens group.

AUX-000280 [**Required: SS**] The SS shall allow DISA to configure the following within the set of DSN numbers for which HR is activated:

a. Up to 20 individual DSN numbers.

b. Up to 20 ranges of DSN numbers.

AUX-000290 [**Required: SS**] When the HR feature is activated for all calls and when the HR feature is activated for calls to a specific set of DSN numbers, the SS shall apply the HR feature on calls that enter the SS on all line or Local Area Network (LAN)-side and trunk or Wireless Area Network (WAN)-side interfaces, both Time Division Multiplexing (TDM) and Voice over IP (VoIP).

3.3.2.1 HR Query From SS

AUX-000300 [**Required: SS**] When the HR feature is activated for all calls, the SS shall make an HR query to the LRDB for each call that is placed to a DSN number. When the HR feature is activated for calls to a specific set of DSN numbers, the SS shall make an HR query to the LRDB for each call that is placed to a DSN number within that set of DSN numbers.

AUX-000310 [**Required: SS**] In both cases, the SS shall not make HR queries for calls that are placed to Public Switched Telephone Network (PSTN) numbers or PSTN service codes such as 911 (in the United States), 112 (in Europe), or 411 (in the United States).

AUX-000320 [**Optional: SS**] The SS shall maintain a cache of the response data to HR queries. The response data maintained in the cache for each HR query shall be associated with the DSN called for which the HR query was made.

AUX-000330 [**Conditional: SS**] If the SS maintains a cache of HR response data, then the SS shall use the cached data, if any, for a given DSN number instead of making an HR query to the LRDB on a subsequent call to that DSN number.

AUX-000340 [**Conditional: SS**] If the SS maintains a cache of HR response data, then the SS shall also support expiration of cache entries, including the ability to configure the lifetime of cache entries and configurable limits to the size of the cache.

AUX-000350 [**Required: SS**] The HR query that the SS sends to the LRDB shall contain the full 10-digit DSN called number for that call. The HR query shall be sent in the LDAPv3 Search Request message. This Search Request message shall contain the following fields in ASCII format:

a. Base Object field containing an LDAP Distinguished Name containing the Domain Components "uc" and "mil" (dc=uc, dc=mil).

b. Scope field containing the value "wholeSubtree."

c. Filter field containing the following:

   (1) Directory Number field containing the 10-digit DSN called number.

AUX-000360 [**Required: LRDB**] The LRDB shall accept and process the previous HR query from the SS containing the full 10-digit DSN called number.

AUX-000370 [**Required: LRDB**] The LRDB shall store the following information in its Database record for each 10-digit DSN number:

a. CCA-ID of the SC serving that DSN number (the "destination SC").

b. CCA-ID of the primary SS serving the destination SC.

c. CCA-ID of the backup SS serving the destination SC.

d. Full internationally significant commercial number matching that DSN number (if this commercial number exists).

NOTE: The CCA-IDs may be absent from the record in cases in which the DSN and commercial numbers in the record are associated with a DSN end user who is served by a DSN EO or Private Branch Exchange (PBX).

3.3.2.2 Database Response When DSN Number Is Found

AUX-000380 [**Required: LRDB**] When the LRDB finds a database record that matches the DSN number in the HR query, the LRDB shall return an HR response to the SS containing the following information taken from that record:

a. CCA-ID of the destination SC.

b. CCA-ID of the primary SS serving the destination SC.

c. CCA-ID of the backup SS serving the destination SC.

d. Full internationally significant commercial number matching that DSN number (if this commercial number exists).

NOTE: The CCA-IDs may be absent from the record in cases in which the DSN and commercial numbers in the record are associated with a DSN end user who is served by a DSN EO or PBX.

AUX-000390 [**Required: LRDB**] The LRDB shall send this HR response in the LDAPv3 Search Result Entry and Search Result Done messages.

AUX-000400 [Required: LRDB] The Search Result Entry message shall contain the following fields in ASCII format:

a. Object Name field containing an LDAP Distinguished Name containing the following:

(1) User ID component containing the commercial number (e.g., UID=7038821234).

(2) Domain Components "uc" and "mil" (dc=uc, dc=mil).

The commercial number in the User Identifier (UID) field may be represented in either national or international format (depending on the SC that uploads the number in the Database).

b. Attributes field containing the following attributes:

(1) UID field containing the commercial number.

(2) Object Class field containing "mobSLR."

(3) Subscriber Type field containing "asftswtch."

(4) SIP Alias field containing the full commercial called number followed by "@uc.mil" (e.g., 17038821234@uc.mil).

(5) Sip User Name field containing the UID (i.e., commercial number) followed by "@uc.mil" (e.g., 7038821234@uc.mil).

(6) Directory Number field containing the 10-digit called DSN number.

(7) LSCCCAID field containing the CCA-ID of the destination SC.

(8) SSCCAID field containing the CCA-IDs of the primary SS and the backup SS serving the destination SC, separated by a comma.

(9) The LRDB also can include other attribute fields here that the SS may ignore.

The commercial number in the UID field may be represented in either national or international format, depending on the SC that uploads the number in the Database.

AUX-000410 [**Required: LRDB**] The Search Result Done message shall contain the following field in ASCII format:

- Result Code field indicating "Success."

3.3.2.3 Database Response When DSN Number Is Not Found

AUX-000420 [**Required: LRDB**] When the LRDB finds no Database record that matches the DSN number in the HR query, the LRDB shall return an HR response to the SS containing a "number not found" indication.

AUX-000430 [**Required: LRDB**] The LRDB shall send this HR response in the LDAPv3 Search Result Done message. The Search Result Done message shall contain the following field in ASCII format:

- Result Code field indicating "Success."

3.3.2.4 SS Actions Based on Database Response

AUX-000440 [**Required: SS**] In the Number Found case, the SS shall accept and process the aforementioned HR response from the LRDB containing the SC CCA-ID, the primary SS CCA-ID, and the backup SS CCA-ID.

AUX-000450 [**Required: SS**] In the Number Found case, the SS shall also accept and process HR responses from the LRDB that do not contain any CCA-IDs.

AUX-000460 [**Required: SS**] In the Number Not Found case, the SS also shall accept and process the aforementioned HR response from the LRDB containing the "number not found" indication.

AUX-000470 [**Required: SS**] In the Number Found case, if the HR response contains CCA-ID values, then the SS shall route the call to the SC specified by the SC CCA-ID in the HR response.

a. If that SC is not subtended by the SS, then the SS shall route the call to the SS specified by the primary SS CCA-ID in the HR response.

b. If the primary SS is not accessible from the SS that sent the query and received the response (e.g., because the primary SS is out of service), then that querying SS shall route the call to the SS specified by the backup SS CCA-ID in the HR response.

AUX-000480 [**Required: SS**] The SS shall support an internal table configurable by DISA or the DoD Component that lists the CCA-IDs of all the SCs served by that SS, and the CCA-IDs of all of the other SSs in the UC network to which this SS can route AS-SIP sessions.

a. For each CCA-ID listed in this table, this SS shall allow DISA or the DoD Component to store the DISN WAN IP address of the SBC that fronts the SC or SS associated with that CCA-ID.

b. This SS shall use this internal table to resolve CCA-IDs returned by the LRDB into destination SC and SS SBC IP addresses on the DISN WAN.

c. This SS shall use these destination SC and SS SBC IP addresses to route calls to the destination SCs and SSs, per the previously listed requirements.

AUX-000490 [**Required: SS**] In the Number Not Found case and in the Number Found case when the HR response does not contain a value (i.e., CCA-IDs are absent), the SS shall use the route specified in its internal routing tables for the called DSN number to route the call request to one of the following:

a. The destination SC (by an outgoing AS-SIP route).

b. Another SS (by an outgoing AS-SIP route).

c. A Multifunction Switch (MFS) or EO connected to the Media Gateway (MG) of that SS (by an outgoing T1.619a Primary Rate Interface [PRI] route).

d. The destination EI (AS-SIP End Instrument [AEI], Proprietary Internet Protocol Voice End Instrument [PEI], or analog EI) served by an SC that is internal to the SS (when an internal SC is supported).

AUX-000500 [**Required: SS**] In the Number Not Found case and in the Number Found case when the HR response does not contain a value for the CCA-IDs (i.e., CCA-ID is absent),

a. When the SS determines that the call to the DSN number previously arrived at the SS from an incoming T1.619a PRI route from an MFS,

b. And then determines that the call should be routed back to that MFS over an outgoing T1.619a PRI route using the same PRI,

c. The SS shall use a "route optimization" procedure on that PRI to do the following:

d. Return the call to the MFS.

(1) Remove the incoming PRI B-Channel and outgoing PRI B-Channel from the call path so that these two B-Channels are not kept in use for the remainder of the call.

This "route optimization" procedure shall be MVI, and shall work with MFS products from other vendors (besides the SS vendor), without requiring any enhancements or software patches to the other vendors' MFS products.

The SS vendor shall identify for DISA what this MVI route optimization procedure is, so that DISA can share it with other MFS vendors, and perform interoperability testing on it using the SS and MFS products from other vendors.

AUX-000510 [**Required: SS**] If the SS determines that it has lost connectivity with the LRDB (e.g., because that Database has failed), then the SS shall apply the Failover to Secondary LRDB procedures, per the requirements in Section 3.3.5.2.5, Failover Procedures.

AUX-000520 [**Required: SS**] If the SS applies these failover procedures and does not receive the necessary routing information from the Secondary LRDB, then the SS shall use its internal routing data tables to complete the call to the DSN number.

AUX-000530 [**Conditional: SS**] If the SS supports caching of Database responses for the HR feature, and the SS loses TLS connectivity with the LRDB, then the SS shall first check the current HR cache data for Number Found information matching the called DSN number on each call in which HR treatment is required.

a. If this current HR cache data contains Number Found information for the called DSN number, then the SS shall complete that call using the CCA-IDs (SC, primary SS, and backup SS) in that HR cache data.

b. If this current HR cache data contains Number Found information for the called DSN number but no CCA-IDs, then the SS shall assume a Number Not Found case and apply the Number Not Found treatment described in the previous requirements.

c. If the current HR cache data does not contain Number Found information for the called DSN number, then the SS shall assume a Number Not Found case and apply the Number Not Found treatment described in the previous requirements.

3.3.3 SC to LRDB Interface: Database Queries for Commercial Cost Avoidance

The requirements in this section apply to the SC and the LRDB. The LRDB can be located in a site that is physically remote from the SC site.

AUX-000540 [**Required: SC, LRDB**] The SC and the LRDB shall support the Commercial Cost Avoidance feature per the requirements in this section.

AUX-000550 [**Required: SC**] The SC shall support an interface to an LRDB to support Database queries and Database responses for the Commercial Cost Avoidance feature.

AUX-000560 [**Required: LRDB**] The LRDB shall support an interface to the SC to support Database queries and Database responses for the Commercial Cost Avoidance feature.

AUX-000570 [**Required: SC, LRDB**] The query-response interface between the SC and the LRDB shall be LDAPv3 over TLS over IP. On the SC, this LDAPv3 interface shall be compliant with IETF RFC 4511 and all the LDAP technical specifications listed in Section 1 of RFC 4510. On the LRDB, see the LDAPv3 interface requirements in Section 3.3.5.2.1, General Architecture, Protocols, and Interfaces.

AUX-000580 [**Required: SC, LRDB**] The encoding of the LDAPv3 messages and data schema used on the Database query interface between the SC and the LRDB shall follow the BER of ASN.1. On the SC this encoding shall be consistent with Section 5.1, Protocol Encoding, of RFC 4511. On the LRDB, see the LDAPv3 interface requirements in Section 3.3.5.2.1, General Architecture, Protocols, and Interfaces.

AUX-000590 [**Required: SC, LRDB**] The interface between the SC and the LRDB shall be secured using TLS, consistent with the requirements for securing AS-SIP messages using TLS in Section 4, Information Assurance. This security shall provide mutual authentication between the

SC and the LRDB, message confidentiality for the Database query and Database response, and message integrity for the Database query and Database response.

AUX-000600 [**Required: SC, LRDB**] The interface between the SC and the LRDB shall traverse the data firewalls (and not the SBC firewalls) at both the SC and LRDB sites.

AUX-000610 [**Required: SC, LRDB**] The interface between the SC and the LRDB shall traverse the CE-Rs at both the SC and LRDB sites, using the DSCP for User Signaling traffic and the associated CE-R queues.

AUX-000620 [**Required: SC**] The interface between the SC and the LRDB shall terminate on the Ethernet interface used for VVoIP signaling traffic at the SC, as described in Section 4, Information Assurance.

AUX-000630 [**Required: SC**] The SC shall allow Commercial Cost Avoidance to be activated for all of the following types of calls:

a. Originated by EIs or MGs on the SC.

b. Placed to commercial called numbers instead of DSN called numbers.

   This is the "activated for all commercial numbers" option for Commercial Cost Avoidance.

AUX-000640 [**Required: SC**] The SC shall also allow Commercial Cost Avoidance to be activated for all of the following types of calls:

a. Originated by EIs or MGs on the SC.

b. Placed to commercial called numbers instead of DSN called numbers.

c. Placed to numbers within a specific set of commercial numbers.

   In this second case, the SC shall allow DISA to configure the set of commercial numbers for which Commercial Cost Avoidance is activated.

   This is the "activated for select commercial numbers" option for Commercial Cost Avoidance.

AUX-000650 [**Required: SC**] The DISA-configurable set of commercial numbers for Commercial Cost Avoidance shall support the following elements:

a. Individual numbers from the worldwide E.164 commercial numbering plan.

b. Ranges of numbers from the worldwide E.164 commercial numbering plan.

   Each range shall be configurable so that DISA can specify the first and last numbers in the range.

AUX-000660 [**Required: SC**] The SC shall allow a configurable range to include the following:

a. An entire E.164 CC (e.g., CC 1 for the United States and Canada, CC 49 for Germany, and CC 82 for South Korea).

b. CC 1 and an entire three-digit Area Code (e.g., in the United States or Canada).

c. CC 1 and an entire three-digit Area Code and three-digit Office Code.

d. A range of numbers within CC 1, a single Area Code, and a single Office Code (e.g., a thousands group, hundreds group, or tens group within CC 1, the Area Code, and the Office Code).

e. For countries outside CC 1, an entire E.164 CC and City Code.

f. For countries outside CC 1, a range of numbers within an E.164 CC and City Code (e.g., a thousands group, hundreds group, or tens group within that CC and City Code).

AUX-000670 [**Optional: SC**] DISA also shall be able to independently specify the first and last numbers in a range without having to limit that range to a single Area Code, a single Office Code, a single thousands group, a single hundreds group, or a single tens group.

AUX-000680 [**Required: SC**] The SC shall allow DISA to configure the following within the set of commercial numbers for which Commercial Cost Avoidance is activated:

a. Up to 20 individual commercial numbers.

b. Up to 20 ranges of commercial numbers.

AUX-000690 [**Required: SC**] The SC shall support a configuration option to deactivate Commercial Cost Avoidance queries for all calls. Note that the scope of this setting is limited to interaction between the SC and the LRDB at the invocation of the Commercial Cost Avoidance feature when calls are made. It shall have no impact on the MRDB database updates performed by the SC for both Commercial Cost Avoidance and HR (as specified in Section 3.3.4, SC to MRDB Interface: Database Updates for Commercial Cost Avoidance and Hybrid Routing).

3.3.3.1 Commercial Cost Avoidance Query From SC

AUX-000700 [**Required: SC**] When the Commercial Cost Avoidance feature is activated for all commercial numbers, the SC shall make a Commercial Cost Avoidance query to the LRDB for each call that is placed to a commercial number. The SC shall not make Commercial Cost Avoidance queries for calls that are placed to PSTN service codes such as 911 (in the United States), 112 (in Europe), or 411 (in the United States).

AUX-000710 [**Required: SC**] When the Commercial Cost Avoidance feature is activated for a select set of commercial numbers, the SC shall make a Commercial Cost Avoidance query to the LRDB for each call that is placed to a commercial number within that DISA-configured set. The SC shall not make Commercial Cost Avoidance queries for calls that are placed to PSTN service codes such as 911 (in the United States), 112 (in Europe), or 411 (in the United States).

AUX-000720 [**Required: SC**] The SC shall query the LRDB on "99 dialed commercial PSTN number" and "98 dialed commercial PSTN number" call requests from SC end users. When the Database responds to this query with a DSN number that matches the dialed PSTN number, the SC shall route the call request over the appropriate IP (AS-SIP) or TDM (T1.619A PRI) path using the DSN number returned by the Database. When the Database responds with a "Number Not Found" indication, the SC shall route the call request to the local TDM PSTN trunk group (PRI or Client Access Server [CAS]) on the SC's MG, using the originally dialed commercial number.

AUX-000730 [**Required: SC**] The Commercial Cost Avoidance query that the SC sends to the LRDB shall contain the full internationally significant commercial called number (CC + Nationally Significant Number) for that call. The Commercial Cost Avoidance query shall be sent in the LDAPv3 Search Request message. This Search Request message shall contain the following fields in ASCII format:

a. Base Object field containing an LDAP Distinguished Name containing the Domain Components "uc" and "mil" (dc=uc, dc=mil).

b. Scope field containing the value "wholeSubtree."

c. Filter field containing the following:

   (1) SIP Alias field containing the full commercial called number followed by "@uc.mil" (e.g., 17038821234@uc.mil).

AUX-000740 [**Required: LRDB**] The LRDB shall accept and process the Commercial Cost Avoidance queries from the SC that contain the full internationally-significant commercial called number.

AUX-000750 [**Required: LRDB**] The LRDB shall accept Commercial Cost Avoidance queries from the SC, in which this query contains the PSTN called number from the 99 dialed PSTN number or 98 dialed PSTN number call request from the SC end user. The LRDB shall be able to accept these queries for both continental United States (CONUS) "PSTN called numbers" [in which the called number is from the 10-digit North American Numbering Plan (NANP)] and outside CONUS (OCONUS) (PSTN) called numbers (in which the called number is from either outside the NANP or within the NANP and located in Alaska, Hawaii, or the U.S. overseas territories).

AUX-000760 [**Required: LRDB**] The LRDB shall be capable of storing associations of PSTN numbers with 10-digit DSN numbers from the DSN numbering plan. The Database shall be capable of storing these associations for both CONUS and OCONUS PSTN numbers, as described in the previous requirement.

AUX-000770 [**Required: LRDB**] The LRDB shall store the following information in its database record for each commercial number:

a. The full 10-digit DSN number matching that commercial number.

b. The CCA-ID of the SC serving that DSN number (the "destination SC").

c. The CCA-ID of the primary SS serving the destination SC.

d. The CCA-ID of the backup SS serving the destination SC.

NOTE: The CCA-IDs may be absent from the record in cases in which the DSN and commercial numbers in the record are associated with a DSN end user who is served by a DSN EO or PBX.

3.3.3.2 Database Response When Commercial Number Is Found

AUX-000780 [**Required: LRDB**] When the LRDB finds a database record that matches the commercial called number in the Commercial Cost Avoidance query, the LRDB shall return a Commercial Cost Avoidance response to the SC containing the following information, taken from that record:

a. The full 10-digit DSN number matching the commercial number.

The LRDB shall send this Commercial Cost Avoidance response in the LDAPv3 Search Result Entry and Search Result Done messages.

AUX-000790 [**Required: LRDB**] The Search Result Entry message shall contain the following fields in ASCII format:

a. Object Name field containing an LDAP Distinguished Name containing the following:

(1) User ID component containing the commercial number (e.g., UID=7038821234).

(2) Domain Components "uc" and "mil" (dc=uc, dc=mil).

The commercial number in the UID field may be represented in either national or international format, depending on the SC that uploads the number to the Database.

b. Attributes field containing the following attributes:

(1) User ID field containing the commercial number.

(2) Object Class field containing "mobSLR."

(3) Subscriber Type field containing "asftswtch."

(4) SIP Alias field containing the full commercial called number, followed by "@uc.mil" (e.g., 17038821234@uc.mil).

(5) SIP User Name field containing the UID (i.e., commercial number) followed by "@uc.mil" (e.g., 7038821234@uc.mil).

(6) Directory Number field containing the full 10-digit DSN number.

(7) LSCCCAID field containing the CCA-ID of the destination SC serving the DSN number.

(8) SSCCAID field containing the CCA-IDs of the primary SS and the backup SS serving the destination SC, separated by a comma.

(9) Other attribute fields that the SC may ignore.

The commercial number in the UID field may be represented in either national or international format, depending on the SC that uploads the number to the Database.

AUX-000800 [**Required: LRDB**] The Search Result Done message shall contain the following field in ASCII format:

- Result Code field indicating "Success."

3.3.3.3 Database Response When Commercial Number Is Not Found

AUX-000810 [**Required: LRDB**] When the LRDB finds no database record that matches the commercial number in the Commercial Cost Avoidance query, the LRDB shall return a Commercial Cost Avoidance response to the SC containing a Number Not Found indication.

AUX-000820 [**Required: LRDB**] The LRDB shall send this Commercial Cost Avoidance response in the LDAPv3 Search Result Done message. The Search Result Done message shall contain the following field in ASCII format:

- Result Code field indicating "Success."

3.3.3.4 SC Actions Based on Database Response

AUX-000830 [**Required: SC**] In the Number Found case, the SC shall accept and process the Commercial Cost Avoidance response from the LRDB containing the DSN number that matches the commercial called number.

AUX-000840 [**Required: SC**] In the Number Not Found case, the SC shall also accept and process the Commercial Cost Avoidance response from the LRDB containing the "Number Not Found" indication.

AUX-000850 [**Required: SC**] In the Number Found case, the SC shall use the route specified in its internal routing tables for the digits of the returned DSN number to route the call request to one of the following:

a. The primary or backup SS for that SC (by an outgoing AS-SIP route).

b. The DSN EO connected to the MG of that SC (by an outgoing T1.619a PRI route).

c. A UC EI or MG served by that SC (if the returned DSN number identifies an EI on that SC or a subscriber located behind the MG of that SC).

AUX-000860 [**Required: SC**] In the Number Not Found case, the SC shall use the route specified in its internal routing tables for the original commercial called number to route the call request to the following:

a. PSTN EO connected to the MG of that SC (by an outgoing commercial PRI or CAS trunk route).

AUX-000870 [**Required: SC**] If the SC determines that it has lost connectivity with the LRDB (e.g., because that Database has failed), then the SC shall apply the Failover to Secondary LRDB procedures, per the requirements in Section 3.3.5.2.5, Failover Procedures.

AUX-000880 [**Required: SC**] On Commercial Cost Avoidance call requests that are rerouted to DSN numbers by the LRDB, the SC shall respond to SS signaling, indicating that the call attempt to the DSN number was rejected (i.e., an AS-SIP 4xx, 5xx, or 6xx response to an AS-SIP INVITE message) by overflowing these calls from the local AS-SIP trunk group to the local TDM PSTN trunk group (PRI or CAS). The SC shall signal the originally dialed commercial number to the PSTN when overflowing this call to the PSTN trunk group.

AUX-000890 [**Required: SC**] On Commercial Cost Avoidance call requests that are rerouted to DSN numbers by the LRDB, the SC shall respond to DSN EO signaling indicating that the call attempt to the DSN number was rejected [i.e., an ISDN DISCONNECT, RELEASE, or RELEASE COMPLETE response to an Integrated Services Digital Network (ISDN) SETUP message] by overflowing these calls from the local T1.619a PRI trunk group to the local TDM PSTN trunk group (PRI or CAS). The SC shall signal the originally dialed commercial number to the PSTN when overflowing this call to the PSTN trunk group.

3.3.4 SC to MRDB Interface: Database Updates for Commercial Cost Avoidance and Hybrid Routing

The requirements in this section apply to the SC and the MRDB. The MRDB can be located in a site that is physically remote from the SC site.

AUX-000900 [**Required: SC, MRDB**] The SC and the MRDB shall support the Routing Database update feature per the requirements in this section; in Section 3.3.5, LRDB and MRDB; and in Section 3.3.6, MRDB and LRDB Operations.

AUX-000910 [**Required: SC**] The SC shall support an interface to an MRDB to support Database updates for the Commercial Cost Avoidance and HR features.

AUX-000920 [**Required: MRDB**] The MRDB shall support an interface to the SC to support Database updates for the Commercial Cost Avoidance and HR features.

AUX-000930 [**Required: SC, MRDB**] The Database update interface between the SC and the MRDB shall be LDAPv3 over TLS over IP. On the SC, this LDAPv3 interface shall be compliant with RFC 4511 and all the LDAP technical specifications listed in Section 1 of RFC 4510. On the LRDB, see the LDAPv3 interface requirements in Section 3.3.5.2.1, General Architecture, Protocols, and Interfaces.

AUX-000940 [**Required: SC, MRDB**] The encoding of the LDAPv3 messages and data schema used on the Database update interface between the SC and the MRDB shall follow the BER of ASN.1. On the SC, this encoding shall be consistent with Section 5.1, Protocol Encoding, of RFC 4511. On the LRDB, see the LDAPv3 interface requirements in Section 3.3.5.2.1, General Architecture, Protocols, and Interfaces.

AUX-000950 [**Required: SC, MRDB**] The Database update interface between the SC and the MRDB shall be secured using TLS, consistent with the requirements for securing AS-SIP messages using TLS in Section 4, Information Assurance. This security shall provide mutual authentication between the SC and the MRDB, message confidentiality for the Database updates, and message integrity for the Database updates.

AUX-000960 [**Required: SC, MRDB**] The Database update interface between the SC and the MRDB shall traverse the data firewalls (and not the SBC firewalls) at both the SC and MRDB sites.

AUX-000970 [**Required: SC, MRDB**] The Database update interface between the SC and the MRDB shall traverse the CE-Rs at both the SC and MRDB sites, using the DSCP for User Signaling traffic and the associated CE-R queues.

AUX-000980 [**Required: SC**] The Database update interface between the SC and the MRDB shall terminate on the Ethernet interface used for VVoIP signaling traffic at the SC, as described in Section 4, Information Assurance.

3.3.4.1 LDAP Update Operations

AUX-000990 Before sending an Update operation (Add or Modify) to the Database, the SC shall send a Search operation to the Database using the Distinguished Name for the record to be updated (see Section 3.3.5.2.3, Request Processing, for additional requirements). The Search operation shall be one of the following:

- The LDAP Search Request message for HR queries, specified in requirement AUX-000310 in Section 3.3.2.1, HR Query From SS (in this case, the Search Request message contains a Directory Number field containing the 10-digit DSN called number).
- The LDAP Search Request message for CCA queries, specified in requirement AUX-000680 in Section 3.3.3.1, Commercial Cost Avoidance Query From SC (in this case, the Search Request message contains a SIP Alias field containing the full commercial called number followed by "@uc.mil" [e.g., 17038821234@uc.mil]).
- If no matching record is found, then the SC shall proceed with the Update using an Add operation.
- If the matching record is found, and the CCA-ID of the requesting SC matches the SC CCA-ID in that record, then the SC shall proceed with the Update using a Modify operation.

- If the matching record is found, but the CCA-ID of the requesting SC does not match the SC CCA-ID in that record (or if there is no SC CCA-ID in that record), then the SC shall not perform the update and shall issue the necessary warnings or alerts to indicate that such an operation is not allowed until further intervention by network craftspeople or administrators.
  - For example, the network craftsperson at the requesting SC may contact another network craftsperson at the SC identified in the Database record, and ask the other craftsperson to delete the "old" SC's record from the Routing Database so that the "new" SC's record can be added.

3.3.4.1.1 LDAP Add Operation

AUX-001000 [**Required: SC**] The SC shall send a Database update automatically to the MRDB whenever a new end user is added to the SC, unless the RTS Routing Database "opt out" indication has been made for that user.

AUX-001010 [**Required: SC**] The SC shall send this Database update automatically to the MRDB whenever the "opt out" indication for an existing user is changed from "on" to "off."

(See Section 3.3.4.2, RTS Routing Database "Opt Out" for SC End Users, for "opt out" related requirements.)

AUX-001020 [**Required: SC**] If the preceding Search request resulted in a No Record Found indication, then the SC shall perform the update using an LDAP Add operation. This operation shall contain the following:

a. User ID (i.e., commercial number) for that end user.
b. Full 10-digit DSN number for that end user.
c. Full internationally significant commercial number for that end user.
d. CCA-ID of the SC serving the DSN number.
e. CCA-ID of the primary SS serving that SC.
f. CCA-ID of the backup SS serving that SC.
g. Indication that the end user, DSN number, and commercial number should be added to the Database.

   The commercial number in the UID field may be represented in either national or international format, depending on the SC that uploads the number to the Database.

AUX-001030 [**Required: SC**] This Database update shall be sent in the LDAPv3 Add Request message. This Add Request message shall contain the following fields in ASCII format:

a. An Entry field containing an LDAP Distinguished Name containing the following:

   (1) A User ID component containing the commercial number (e.g., UID=7038821234).

(2) The Domain Components "uc" and "mil" (dc=uc, dc=mil).

The commercial number in the UID field may be represented in either national or international format, which will depend on the SC that uploads the number to the Database.

b. An Attributes field containing the following attributes:

(1) A User ID field containing the commercial number.

(2) An Object Class field containing "mobSLR."

(3) A Subscriber Type field containing "asftswtch."

(4) A SIP Alias field containing the full commercial called number followed by "@uc.mil" (e.g., 17038821234@uc.mil).

(5) A Sip User Name field containing the UID (i.e., commercial number) followed by "@uc.mil" (e.g., 7038821234@uc.mil).

(6) A Directory Number field containing the full 10-digit DSN number.

(7) An LSCCCAID field containing the CCA-ID of the destination SC serving the DSN number.

(8) An SSCCAID field containing the CCA-IDs of the primary SS and the backup SS serving the destination SC, separated by a comma.

The commercial number in the UID field may be represented in either national or international format, which will depend on the SC that uploads the number to the Database.

3.3.4.1.2 LDAP Modify Operation

AUX-001040 [**Optional: SC**] The SC shall automatically send a Database update to the MRDB whenever an existing users' number data (DSN and/or commercial) is modified at the SC, and the RTS Routing Database "opt out" indication for that user has not been set.

AUX-001050 [**Conditional: SC**] If the SC sends this Database update, and the preceding Search request resulted in a "record found/matching SC CCA-ID" indication, then the SC shall perform the update using an LDAP Modify Replace operation. This operation shall contain the following:

- The User ID (i.e., commercial number) for that end user.
- An indication of the attribute names to be modified and the new values to be inserted.
- The commercial number in the UID field may be represented in either national or international format (which will depend on the SC that uploads the number to the Database).

AUX-001060 [Conditional: SC] If the SC sends this Database update, then the update shall be sent in the LDAPv3 Modify Request message containing a Replace operation. This Modify Request message shall contain the following fields in ASCII format:

a. An Entry field containing an LDAP Distinguished Name containing the following:

   (1) A User ID component containing the commercial number (e.g., UID=7038821234).

   (2) The Domain Components "uc" and "mil" (dc=uc, dc=mil).

b. The intended operation: replace.

c. An Attributes field containing the following:

   (1) One or more Attribute names (the ones to be modified).

   (2) One or more Attribute values (the new values to replace the existing value).

   The commercial number in the UID field may be represented in either national or international format (which will depend on the SC that uploads the number to the Database).

When adding a new SC user's data (DSN and commercial numbers) to the MRDB, the SC may use a sequence of LDAP Add and Modify messages to add the data, instead of using a single LDAP Add Message to add the data. In this case, the following requirement applies:

AUX-001070 [**Conditional: SC**] If the SC uses a sequence of LDAP messages to add a new SC user's data to the MRDB, then the SC shall be able to add the new SC user's data using at least one of the following methods:

- A single Add operation containing User ID and CCA data (UID, SIP UserName, SIP Alias, DirNumber) and HR data (LSCCCAID, SSCCAID).
- An Add operation containing User ID and CCA data (UID, SIP UserName, SIP Alias, DirNumber), followed by a Modify operation containing HR data (LSCCCAID, SSCCAID).
- An Add operation containing User ID data (UID, SIP UserName), followed by a Modify operation containing CCA data (SIP Alias, DirNumber) and HR data (LSCCCAID, SSCCAID).

3.3.4.1.3 LDAP Delete Operation

AUX-001080 [**Required: SC**] The SC shall automatically send a Database update to the MRDB whenever an existing end user is deleted from the SC, unless the RTS Routing Database "opt out" indication has been made for that user.

AUX-001090 [**Required: SC**] The SC shall send a Database update automatically to the MRDB whenever the "opt out" indication for an existing user is changed from "off" to "on."

AUX-001100 [**Required: SC**] If the preceding Search request resulted in a "record found/matching SC CCA-ID" indication, then the SC shall perform the update using an LDAP Delete operation. This operation shall contain the following:

a. The commercial number (i.e., User ID) for that end user.

b. An indication that the end user, DSN number, and commercial number should be deleted from the Database.

AUX-001110 [**Required: SC**] This Database Update shall be sent in the LDAPv3 Delete Request message. This Delete Request message shall contain the following field in ASCII format:

a. An LDAP Distinguished Name containing the following:

(1) A User ID component containing the commercial number (e.g., UID=7038821234).

(2) The Domain Components "uc" and "mil" (dc=uc, dc=mil).

AUX-001120 [**Optional: SC**] If the Search response preceding the Delete operation indicated that there was no SC CCA-ID in the record, or indicated that the SC CCA-ID in the record did not match the CCA-ID of the requesting SC, then the SC shall not send the LDAP Delete operation, but shall still delete the end user data from the SC. The SC shall issue the appropriate alerts or notification to the network craftspeople/administrators in this case, as manual intervention will be necessary to complete this operation at the Database itself.

For example, the network craftsperson at the requesting SC may contact the network craftsperson at the MRDB, and notify the Database craftsperson that his or her request to delete the SC's record failed. Then the Database craftsperson can check the Database for all Database records that contain the SC's deleted number, and remove any of those records that are redundant or out-of-date.

3.3.4.1.4 LDAP Confirmation Responses

AUX-001130 [**Required: MRDB**] The MRDB shall accept and process the Database updates from the SC for added end users, modified end users, and deleted end users, as listed in the previous requirements. In addition, the MRDB should return a confirmation response to the SC whenever a new end user is added to the Database, an existing user's data is modified in the Database, and an existing end user is deleted from the Database.

AUX-001140 [**Required: MRDB**] In the "added end user" case, the MRDB shall send this confirmation response to the SC in the LDAPv3 Add Response message. The Add Response message shall contain the Result Code field in ASCII format indicating "Success."

AUX-001150 [**Required: MRDB**] In the "modified end user data" case, if all the modifications requested to the record were successful, the MRDB shall send this confirmation response to the SC in the LDAPv3 Modify Response message. The Modify Response message shall contain the Result Code field in ASCII format indicating "Success."

AUX-001160 [**Required: MRDB**] In the "modified end user data" case, if any modifications requested to the record were not successful, the MRDB:

a. Shall not perform any other modification that was requested in that message.

b. Shall send a rejection response to the SC in the LDAPv3 Modify Response message indicating the reason for failure. The Modify Response message shall contain the Result Code field in ASCII format indicating the reason for the failure (e.g., noSuchAttribute, invalidAttributeSyntax).

AUX-001170 [**Required: MRDB**] In the "deleted end user" case, the MRDB shall send this confirmation response to the SC in the LDAPv3 Delete Response message. The Delete Response message shall contain the Result Code field in ASCII format indicating "Success."

3.3.4.1.5 Multiple Database Update Interfaces to Multiple SCs

AUX-001180 [**Required: MRDB**] The MRDB shall be capable of maintaining multiple Database update interfaces to different SCs at the same time. Each individual Database update interface shall support the requirements in this document for the protocols, data schemas, and security mechanisms used between an individual SC and the MRDB. The MRDB shall support at least 40 interfaces with multiple SCs, simultaneously.

AUX-001190 [**Optional: MRDB**] The MRDB shall also be capable of supporting 80 interfaces with multiple SCs, simultaneously.

3.3.4.2 RTS Routing Database "Opt Out" for SC End Users

It is desired that an entry in the RTS Routing Database not be made for certain UC SC end users. To support this goal, an "opt out" indication is required, as follows:

AUX-001200 [**Required: SC**] The user information maintained by an SC for an EI provisioned on that SC shall include an indication to exclude an entry for that user from the RTS Routing Database. It shall be possible to set or change this indication for an end user in the same way, and at the same time, that any other provisioning information for an end user can be set or changed.

AUX-001210 [**Required: SC**] The default state for this setting shall be "off". That is, in the absence of explicitly making this indication, this setting should remain off, and an entry for that end user shall be included in the RTS Routing Database.

AUX-001220 [**Required: SC**] The SC shall consider the setting of this indication when performing an LDAP Add, Modify or Delete operation with the MRDB, as specified above in Section 3.3.4.1, LDAP Update Operations.

AUX-001230 [**Required: SC**] The changing of this indication from "on" to "off" shall trigger an LDAP Add operation from the SC to the MRDB, as specified above in Section 3.3.4.1.1, LDAP Add Operation.

AUX-001240 [**Required: SC**] The changing of this indication from "off" to "on" shall trigger an LDAP Delete operation from the SC to the MRDB, as specified above in Section 3.3.4.1.3, LDAP Delete Operation.

3.3.5 LRDB and MRDB

3.3.5.1 Overview and Terminology

Each theater is expected to have two or more LRDBs handling the LDAPv3 Search operations (Commercial Cost Avoidance queries and HR queries) originating from the SCs and SSs in that theater.

The LRDB(s) will be responsible for (1) performing the Search requests from the SSs (for HR queries) and Search requests from the SCs (for Commercial Cost Avoidance queries) within the local theater, and (2) maintaining synchronization with the Primary MRDB.

One predetermined theater, CONUS (to be referred to as the primary theater), will have a Primary MRDB that will be responsible for (1) receiving Update operations (DSN and commercial number updates) from all SCs across all theaters, including its own, (2) performing the synchronization updates to all LRDBs in all theaters, and (3) performing synchronization with its Backup MRDB in that primary theater.

The requirements in this section follow the architecture described in Figure 3.3-2, Reference Architecture for LRDBs, and Figure 3.3-3, Reference Architecture for MRDBs.

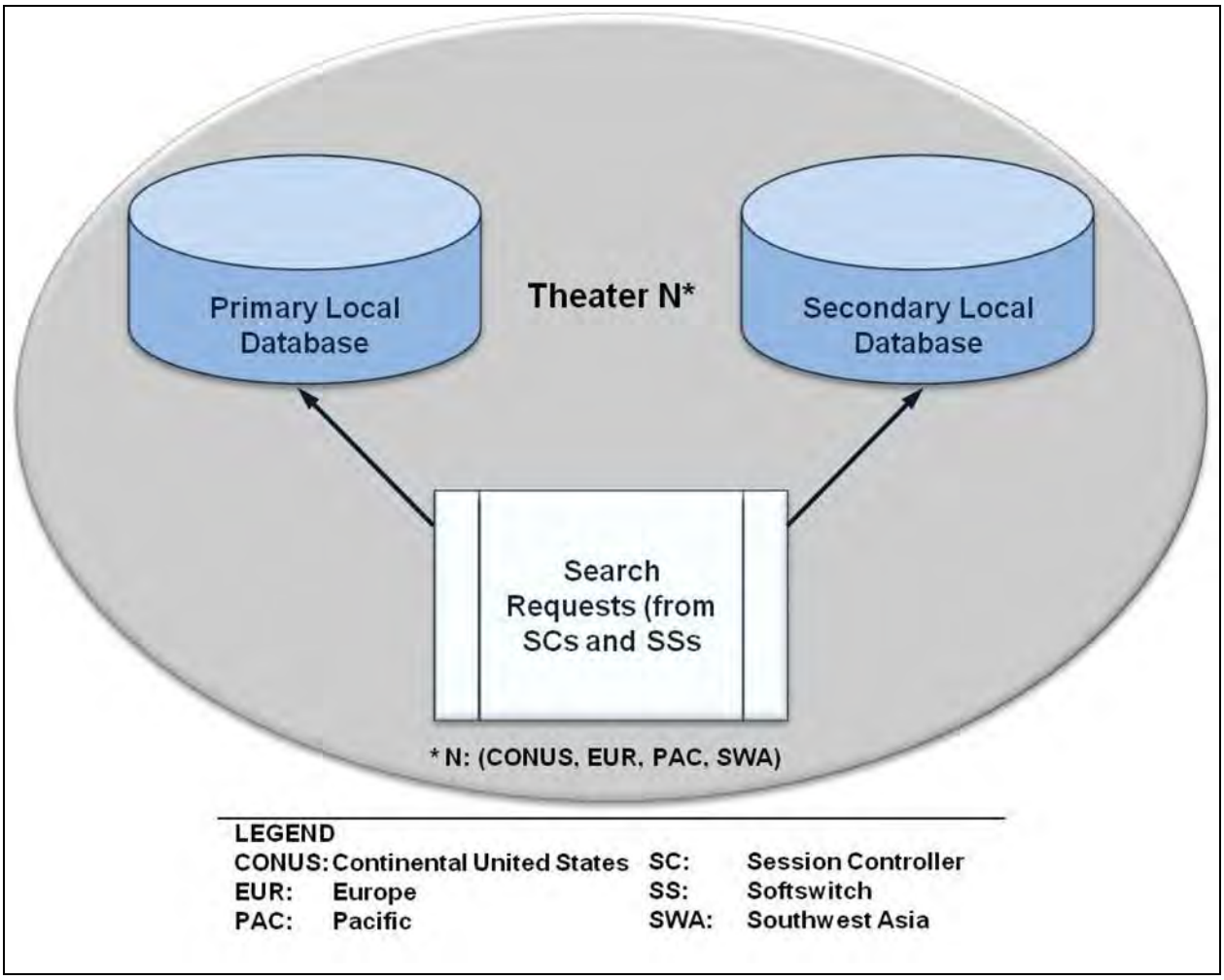


Figure 3.3-2. Reference Architecture for LRDBs

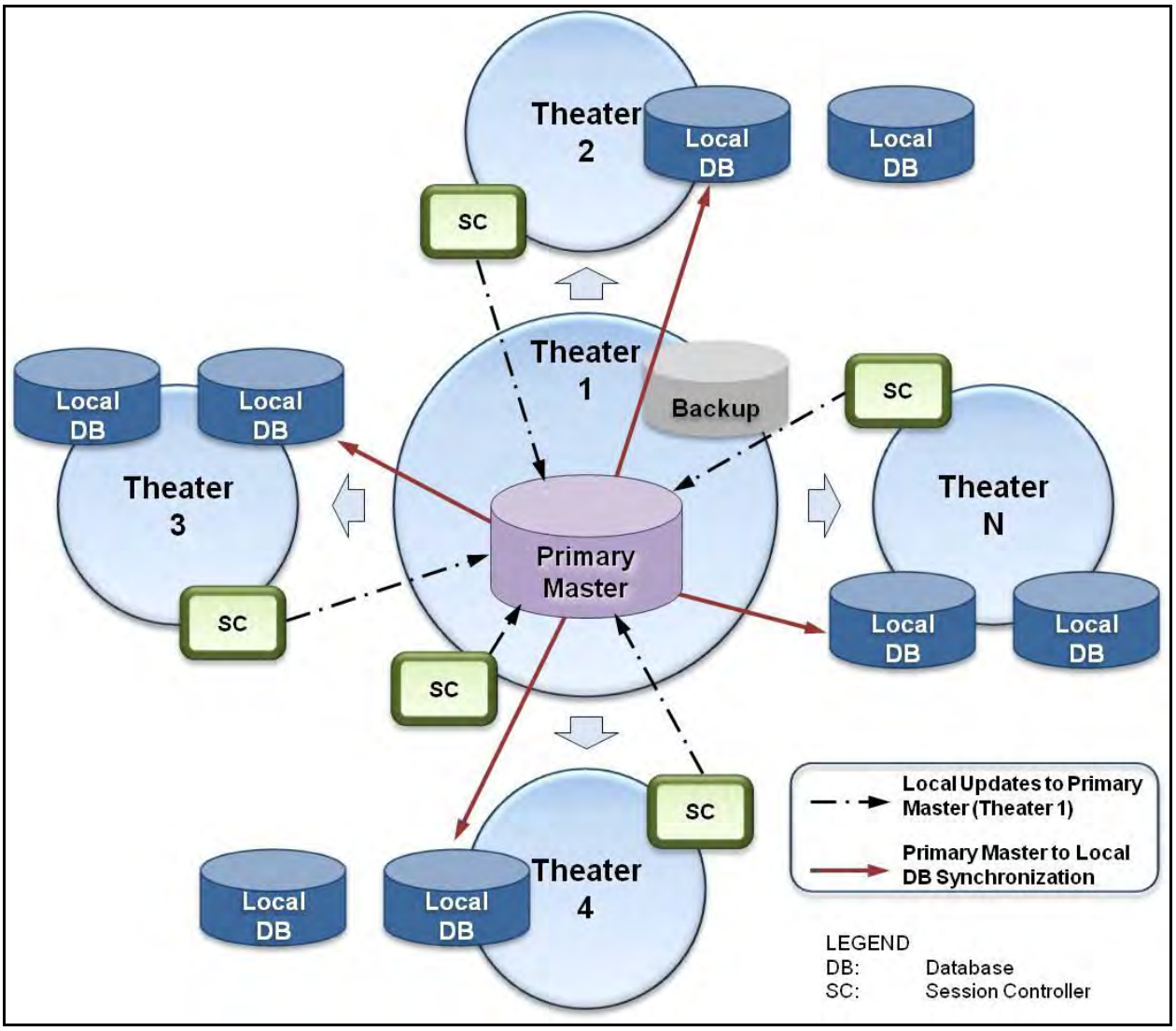


Figure 3.3-3. Reference Architecture for MRDBs

In the following requirements, "bulk update" refers to a method where number records are updated at the MRDB "in bulk," rather than updated individually using LDAP Write operations (like Add, Modify, and Delete). The source of the data for the "bulk updates" may be a set of SCs containing number records, or it may be another database that is a copy of the MRDB (e.g., the Backup MRDB).

Bulk updates will be used during the initial provisioning of the MRDB (e.g., population of the MRDB from multiple SCs that already contain number records) or during full reloads of the Database (e.g., population of the MRDB from the Backup MRDB, after a loss of data at the MRDB). An example of a "bulk update" technique is transfer of LDIF files from the SCs to the MRDB, using e-mail messages or File Transfer Protocol (FTP) sessions to carry the LDIF files from the sources to the destination. LDIF file transfer implies a manual export of LDIF data at the source end (SCs or Backup MRDB) and a manual import of LDIF data at the receiving end

(MRDB). Other bulk update techniques can also be used, if supported by the MRDB vendor and the SC vendors.

3.3.5.2 Routing Database

This section contains requirements for the LRDB and MRDB.

3.3.5.2.1 General Architecture, Protocols, and Interfaces

AUX-001250 [**Required: LRDB, MRDB**] The LRDB and MRDB shall support one or both of the following sets of LDAPv3 RFCs:

a. RFC 2251, RFC 2252, RFC 2253, RFC 2254, RFC 2255, RFC 2256, RFC 2829, RFC 2830.

b. RFC 4511 and all the LDAP technical specifications listed in Section 1 of RFC 4510.

AUX-001260 [Conditional: LRDB, MRDB] If the LRDB and MRDB support only the older set of LDAPv3 RFCs noted previously (RFC 2251, …, RFC 2830), then the LRDB and MRDB shall be interoperable with SC, SS, and other appliances that support LDAPv3 RFC 4511 and all the LDAP technical specifications listed in Section 1 of RFC 4510.

AUX-001270 [**Required: LRDB**] Each LRDB shall be implemented as an independent, stand-alone replica of the data in the MRDB, where that data is not distributed among several physical LRDBs.

AUX-001280 [**Required: MRDB**] Each MRDB shall be implemented as an independent, stand-alone Database, where the Database data is not distributed among several physical Databases.

3.3.5.2.2 Capacity and Record Structure

AUX-001290 [**Required: LRDB, MRDB**] The LRDB and MRDB shall be able to store up to 8 million records, where each record ranges in length from 500–2,000 characters.

It is expected that each database will grow over time, from an initial size of roughly 10,000 small records to a target size of 8 million large records. Therefore, the following requirements and objectives apply.

AUX-001300 [**Required: LRDB, MRDB**] The LRDB and MRDB shall support an initial capacity of 10,000 records.

AUX-001310 [**Required: LRDB, MRDB**] The LRDB and MRDB shall support a full capacity of 8 million records, while adhering to the same performance and availability requirements listed in this document.

AUX-001320 [**Required: LRDB, MRDB**] The LRDB and MRDB shall support the standard LDAP Directory Information Tree (DIT) format for their entries. The required attributes in each entry shall be as shown in Table 3.3-1, LDAP DIT Attribute Formats.

Table 3.3-1. LDAP DIT Attribute Formats

ATTRIBUTE	DESCRIPTION	EXAMPLE
dn	Alphanumeric ASCII string: Distinguished Name; uid containing the commercial number, followed by dc=uc, dc=mil	uid=3012251234, dc=uc, dc=mil
uid	Alphanumeric ASCII string: Unique user ID; commercial number	3012251234
objectClass	Alphanumeric ASCII string: value is "mobSLR" for Routing Database	mobSLR
subscriberType	Alphanumeric ASCII string: value is "asftswtch" for Routing Database	Asftswtch
SIP Alias	Alphanumeric ASCII string; Full internationally significant commercial number matching the DSN number [PSTN number@uc.mil]	3012251234@uc.mil (also OCONUS commercial numbers are allowed)
SIP UserName	Alphanumeric ASCII string; UID (i.e., commercial number matching the DSN number) followed by "@uc.mil"	3012251234@uc.mil (also OCONUS commercial numbers are allowed)
dirNumber	Alphanumeric ASCII string; 10-digit DSN telephone number	3123751234 (DISA Ft. Meade example)
LSCCCAID	Alphanumeric ASCII string; CCA-ID of the SC serving the DSN number	ULSCMEA02 (DISA Ft. Meade SC)
SSCCAID	Alphanumeric ASCII string; CCA-ID of the Primary and Backup SSs serving this SC	UMFSSAND01.UMFSSCO01 (Andrews and Scott AFB Softswitches)
serverHome	null	
isMobile	false	

LEGEND

ASCII: American Standard Code for Information Interchange
CCA: Call Connection Agent
DISA: Defense Information Systems Agency
DSN: Defense Switched Network
ID: Identification
SC: Session Controller
SS: Softswitch
OCONUS: Outside the Continental United States
PSTN: Public Switched Telephone Network
UID: User Identifier

3.3.5.2.3 Request Processing

The SCs and SSs are expected to direct their LDAP Search requests to the LRDBs for call processing purposes. The SC is expected to direct its update requests to the MRDB; it could add a new entry, delete an existing entry, or modify values of attributes in an existing entry. Adding new attributes that are not predefined in the schema is not allowed.

For the update operations, the SC must check whether the record exists in the MRDB before it inserts or deletes any records or applies any modifications.

AUX-001330 [**Required: SC**] The SC shall formulate its updates to the MRDB (or Backup MRDB) in the following sequence:

a. Send a Search operation on the record to be updated, requesting the entire entry.

   The Search operation can be one of the following:

   - The LDAP Search Request message for HR queries, specified in requirement AUX-000310 in Section 3.3.2.1, HR Query From SS.
   - The LDAP Search Request message for CCA queries, specified in requirement AUX-000680 in Section 3.3.3.1, Commercial Cost Avoidance Query From SC.

b. If the entry is found and returned, then the SC shall send the intended Update operation (Delete or Modify).

c. If the entry is not found, then the SC shall do one of the following:

   (1) Perform the intended Add operation.

   (2) Abandon the Update operation.

   The requesting SC will not be allowed to perform updates on a record in which the SC CCA-ID in the record does not match its own SC CCA-ID. Section 3.3.4.1, LDAP Update Operations, contains more detailed requirements.

3.3.5.2.3.1 Client Time-Out

If an LDAP operation does not return results within a preset time, then the LDAP client (SC or SS) should be able to terminate (time-out) the session in a reasonable amount of time.

AUX-001340 [**Required: SC, SS**] The SC or SS shall allow the setting of an LDAP client time-out interval between 1–5 seconds, adjusted in increments of 1 second [default 2 seconds].

Setting a time-out interval helps terminate an otherwise indefinite “hang” situation.

AUX-001350 [**Required: SC, SS**] The SC or SS shall terminate the pending request (Search, Add, Delete, or Modify) via an Abandon operation, if the time-out interval expires and no response was received from the database.

3.3.5.2.3.2 Bind over TLS

The LDAP standards allow for different methods of authentication:

- Anonymous access is obtained by providing no name and no password in the LDAP Bind operation.
- Unauthenticated access is obtained by providing a name but no password in the LDAP Bind operation.
- Authenticated access is obtained by providing a valid name and password in the LDAP Bind operation. With this method, the name and password may still be transported in the clear and be unprotected.

  For UC, confidentiality and integrity protection are required. Transport Layer Security (TLS) (defined in RFC 5246) provides confidentiality and integrity protection. Available implementations of LDAP, such as OpenLDAP, support TLS. The name of the standard LDAP operation for initiating TLS/Secure Socket Layer (SSL) is startTLS. Upon successful completion of this LDAP operation, SSL/TLS is initiated between the LDAP Client (e.g., the SC or SS) and the LDAP Server (e.g., the LRDB or the MRDB).

  All DBs and clients (SCs and SSs) are required to have valid X.509 certificates to be able to use the TLS framework. With TLS in use, none of the LDAP connections would be opened in the clear.

AUX-001360 [**Required: SC, SS**] All connections between the SC or SS to any of the DBs shall use TLS by default.

AUX-001370 [**Required: SC, SS**] An Anonymous or Unauthenticated Bind request shall be disallowed by default on all connections from the SC and SS to any of the DBs.

AUX-001380 [**Required: MRDB, Backup MRDB, LRDB**] The MRDB, Backup MRDB, and LRDB shall not accept or process an Anonymous or Unauthenticated Bind request.

The time that a TLS connection stays open is to be determined by the network administrator.

AUX-001390 [**Optional: MRDB, Backup MRDB, LRDB**] The MRDB, Backup MRDB, and LRDB shall allow the setting of an Idle Time-out Timer T_{idle} (range: 5–30 minutes; increments of 5 minutes; default 10 minutes). When T_{idle} expires, the Database shall shut down the TLS connection.

3.3.5.2.3.3 LRDB Request Processing

AUX-001400 [**Required: LRDB**] The LRDB shall be able to recognize and perform the following LDAP operations originating from SCs and SSs for Commercial Cost Avoidance and HR queries, respectively:

a. Bind Request and Response.

b. Unbind Request.

c. Search Request and Response.

d. Abandon Request.

The LRDB is not required to support Update (LDAP Add, Modify, or Delete) requests from the SCs or SSs. However, the LRDB is expected to support these Update requests for purposes of data population and provisioning through administrative LDAP interfaces, per the following requirement.

AUX-001410 The LRDB shall be able to recognize and perform the following LDAP operations when received from the MRDB, a Database craftsperson station, or the Database Administrator (DBA) over an administrative LDAP interface:

AUX-001410.a [Optional: LRDB] Bind request and response.

AUX-001410.b [Optional: LRDB] Unbind request.

AUX-001410.c [Optional: LRDB] Search request and response.

AUX-001410.d [Optional: LRDB] Add request and response.

AUX-001410.e [Optional: LRDB] Delete request and response.

AUX-001410.f [Optional: LRDB] Modify request and response.

AUX-001410.g [Optional: LRDB] Abandon request.

AUX-001420 [**Required: LRDB**] When the LRDB successfully locates the entry for an LDAP Search operation, it shall generate and return the appropriate LDAP response message, containing, at a minimum, the following:

a. The dirNumber (DSN telephone number), LSCCCAID, and SSCCAID values, for responses to HR queries.

b. The dirNumber (DSN telephone number), SIP Alias (commercial number), and SIP UserName (commercial number) values, for responses Commercial Cost Avoidance queries.

AUX-001430 [**Required: LRDB**] When the LRDB fails to locate the entry for a Search operation, it shall generate and return the appropriate LDAP Result Code, which includes but is not limited to the following:

a. Result Code 0 (indicating “Success”), with no arguments.

b. Result Code 16, LDAP_NO_SUCH_ATTRIBUTE (indicating that the specified attribute does not exist in the entry).

c. Result Code 32, LDAP_NO_SUCH_OBJECT (indicating that the Database server cannot find the entry specified in the request).

It is expected that the SCs and SSs will process the different LDAP Result Codes based on the logic for the type of call (Commercial Cost Avoidance or HR). It is expected that, if no Database entry was found or if timeouts occur at either side (the database side or the client side), or if other LDAP errors are encountered, then the Commercial Cost Avoidance logic will route the call to the commercial number. In the HR logic, if no Database entry is found, or if timeouts occur, then the call is either (a) processed by internal SS routing tables or (b) returned to an MFS and subsequently to an End Office for call completion.

3.3.5.2.3.4 MRDB Request Processing

The MRDB is required to support Update (LDAP Add, Modify, and Delete) requests from all SCs in all theaters. The MRDB is not intended to serve real-time Query requests (LDAP Searches) from SCs and SSs for HR and Commercial Cost Avoidance purposes. However, occasionally a Database craftsperson station, a DBA station, or provisioning logic in the SC or SS may launch an LDAP Search request to the MRDB to determine the existence of specific records there. As a result, the MRDB is expected to support those LDAP Search requests.

AUX-001440 The MRDB shall be able to recognize and perform the following LDAP operations:

AUX-001440.a [Required: MRDB] Bind request and response.

AUX-001440.b [Required: MRDB] Unbind request.

AUX-001440.c [Required: MRDB] Search request and response.

AUX-001440.d [Required: MRDB] Add request and response.

AUX-001440.e [Required: MRDB] Delete request and response.

AUX-001440.f [Required: MRDB] Modify request and response.

AUX-001440.g [Required: MRDB] Abandon request.

AUX-001450 [**Required: MRDB**] When the MRDB successfully locates the entry for an LDAP Search operation, it shall generate and return the appropriate LDAP response message for that message, containing the dirNumber (DSN telephone number), LSCCCAID, SSCCAID, SIP Alias (Commercial number), and SIP UserName (Commercial number) values.

AUX-001460 [**Required: MRDB**] When the MRDB fails to locate the entry for a Search operation, it shall generate and return the appropriate LDAP Result Code. Examples follow:

a. Result Code 0 (indicating “Success”), with no arguments.
b. Result Code 16 (indicating “Attribute not found”).
c. Result Code 32 (indicating “Object not found”).

These Search requests are not used for routing calls (Commercial Cost Avoidance or HR); instead, they are used to verify the existence of an MRDB record. It is therefore expected that, after the Search requests are completed, SCs will use subsequent logic to launch applicable Update requests to the MRDB. For example, if no Database entry was found for a DSN number, then the SC might initiate an Add operation for that number. Conversely, if a Database entry was found for that DSN number, then the SC would not initiate an Add operation for that number, but might instead initiate a Delete or Modify operation for that number. If other LDAP errors were encountered, then the SC LDAP logic could (a) reattempt the Update operation (Add, Delete, Modify) again for that number or (b) issue an error report, indicating multiple unsuccessful Database attempts, that requires administrative intervention.

3.3.5.2.4 Performance and Availability

Performance characteristics of a database, such as query throughput and bulk update times, are highly dependent on the design and configuration of the hardware for that database, including but not limited to the following:

- Processor speed.
- LDAP cache (memory) size.
- Number and size of hard disks used.

The performance requirements for the LRDB and MRDB in this document can be met with various hardware configurations (e.g., processors, cache, and hard disks), as indicated previously, through optimization techniques, and other vendor-specific guidelines or products. Specifically, the MRDB needs to be optimized for processing LDAP Update requests, while the LRDB needs to be optimized for processing LDAP Search requests.

Each SC and SS is expected to direct its Search requests to a pre-specified LRDB in its theater. The load-sharing architecture for LRDBs will be determined by the DISA network engineers in each theater, based on the projected traffic volume originating from each SC or SS in that theater (i.e., the number of Search requests directed to each LRDB will vary between LRDBs, and will vary from one theater to another).

The LRDBs in each theater are expected to store a very recent image of the data stored in the MRDB. These copies should be almost identical in content, based on the time that each LRDB received its latest synchronization update from the MRDB. Creating and using these "local" copies, the LRDB in each theater should also reduce round-trip LDAP signaling latency for the SCs and SSs, and should make the routing data available to them in a reasonable amount of time.

In addition, to ensure data availability and redundancy, the architecture requires support for both a Primary MRDB and a Backup MRDB (where the Backup MRDB contains a complete copy of the Primary MRDB). While the MRDB primarily focuses on LDAP Updates, the following availability requirements apply to all of the LDAP requests (both Searches and Updates).

AUX-001470 [**Required: LRDB, MRDB**] Under normal operating conditions (i.e., there is no Database overload or scheduled downtime for Database maintenance), the LRDB and MRDB shall process 99.99 percent of all LDAP requests received (i.e., Bind, Search, Add, Modify, Delete).

AUX-001480 [**Required: LRDB**] The unavailability time for each LRDB shall not exceed 0.01 percent of 1 year (translating into 1 hour per year; approximately 5 minutes per month). The unavailable time shall apply only to failure situations and does not comprise preventive maintenance or scheduled upgrade times.

It is expected that, when one of the LRDBs in the theater is unavailable, the other LRDB(s) in the theater will be available. It is not expected that all the LRDBs in a given theater will be unavailable at the same time.

AUX-001490 [**Required: MRDB, Backup MRDB**] The unavailability time for each MRDB and Backup MRDBs shall not exceed 0.01 percent of 1 year, translating into 1 hour per year; approximately 5 minutes per month. The unavailable time applies only to failure situations and does not comprise preventive maintenance or scheduled upgrade times.

AUX-001500 [**Required: LRDB, MRDB, Backup MRDB**] The LRDB, MRDB, and Backup MRDB shall each support a minimum of 200 LDAP Search operations per second.

AUX-001510 [**Required: LRDB, MRDB, Backup MRDB**] The LRDB, MRDB, and Backup MRDB shall each support a minimum of 20 LDAP Update (Add, Delete, and Modify) operations per second under normal operation. (Bulk updates during the initial provisioning of the database and bulk updates during full reloads of the database are not considered normal operation.)

AUX-001520 [**Required: LRDB, MRDB, Backup MRDB**] When the SC sends an LDAP Update operation to the Primary MRDB, the Primary MRDB shall relay this update to a pre-specified group of databases (configured in the Primary MRDB), including the Backup MRDB and multiple LRDBs, immediately. The total time from the initialization of a given LDAP Update by the SC, propagation of the data, and receipt of the updates in the pre-specified group of DBs shall not exceed 5 minutes.

The Primary and Backup MRDBs also support synchronization procedures of partial and full database content, with each other and with the local DBs. These procedures are discussed in Section 3.3.5.2.7, Synchronization Between Primary and Backup MRDBs, and Section 3.3.5.2.8, Synchronization Between LRDB and MRDB.

In both the HR and CCA applications, the Search requests serve real-time UC call setup. Therefore, the response times are important.

AUX-001530 [**Required: LRDB, MRDB, Backup MRDB**] The LRDB, MRDB, and Backup MRDB's processing time for an LDAP Bind request shall not exceed 2 milliseconds (ms). This time excludes the round-trip network delays as the Bind requests from (and Bind responses to) the SCs and SSs transit the Defense Information Systems Network (DISN).

AUX-001540 [**Required: SC, SS, LRDB, MRDB, Backup MRDB**] The total LDAP Bind connect time, including all the following time intervals plus DISN transit time, shall not exceed 20 ms:

a. Initializing the LDAP port at the SC or SS.

b. Preparing the Bind request at the SC or SS.

c. Processing the LDAP Bind request at the Database (authenticating the LDAP Username and password).

d. Preparing the Bind result at the LRDB, MRDB, or Backup MRDB.

e. Processing the Bind result at the SC or SS.

NOTE: The 20 ms limit on LDAP Bind connect time is not applicable for tactical deployments, nor when network transit includes a satellite hop.

AUX-001550 [**Required: LRDB, MRDB, Backup MRDB**] The LRDB, MRDB, and Backup MRDB's processing time for an LDAP Search request shall not exceed 10 ms. This time excludes the round-trip network delays as the Search requests from (and Search responses to) SCs and SSs transit the DISN.

AUX-001560 [**Required: LRDB, MRDB, Backup MRDB**] The LRDB, MRDB, and Backup MRDB's processing time for an LDAP Update request (Add, Modify, or Delete) shall not exceed 100 ms. This time excludes the round-trip network delays as the Update requests from (and Update responses to) SCs transit the DISN.

3.3.5.2.4.1 LDAP Directory Considerations

Indexing of LDAP servers reduces search times by facilitating the location of the entry without having to check every single entry for a match. Index tuning is a recommended tool that a database vendor could provide to improve performance.

Other factors that affect the performance of the database server and the processing time of a query include (a) the layout of the DIT and (b) the complexity of the Search request. The LDAP applications will perform better if simple operations are used as much as possible. Therefore, Search requests should ask only for the attributes needed and not retrieve all attributes from every entry, because doing so would slow the database processing significantly.

Some ideas for improving LDAP performance include the following practices:

- Flat directory trees yield quicker response times than deep ones:
  - One-level searches are recommended.
  - Simple search filters (exact filters) should be used more frequently than wildcard filters.

AUX-001570 [**Optional: LRDB, MRDB, Backup MRDB**] In the design of the LRDB and MRDB DIT, frequently accessed Database entries shall be placed closer to the root of the dc=uc tree to help speed access to the different Database entries and their attributes.

AUX-001580 [**Optional: SC, SS**] SC and SS Search requests launched to the LRDB, MRDB, and Backup MRDB shall be optimized to search only for the necessary CCA and HR data and to reduce the use of wildcard filters that return multiple Database entries.

3.3.5.2.4.2 Data Caching

One means of boosting query throughput is to implement a memory cache for frequently retrieved data, since typically accessing the memory cache is faster than accessing a hard disk. Caches can be implemented at the client site (in this case at the SC or SS) or at the server (Database) site.

AUX-001590 [**Conditional: SC, SS**] When Database response caching is supported, the SC and SS shall implement storage buffers that are capable of supporting LDAP entry caches. This capability shall be configurable; the caching or buffering option shall be turned on or off as needed.

AUX-001600 [**Conditional: SC, SS**] When Database response caching is supported, the SC and SS shall be able to support caching at a minimum of 300 entries/records. The maximum amount of record storage (the cache size) shall be settable by DISA, based on Database utilization trends. The required memory cache size shall be provisioned accordingly.

AUX-001610 [**Conditional: SC, SS**] When Database response caching is supported, if the entry is not found in the cache, then the SC or SS shall route the Search request to the LRDB.

AUX-001620 [**Conditional: SC, SS**] If Database response caching is supported, then the cache retention period shall be settable in increments of 30 minutes and shall not exceed 48 hours. When the cache retention period expires, the contents of the cache shall be cleared/purged.

The term “cache retention period” applies to individual entries in the cache, and not to the set of cache entries as a whole. For example, if the cache retention period is 30 minutes and an individual cache entry has been in the cache for 30 minutes, then the individual cache entry should be purged. This does not mean that the whole set of cache entries should be purged every 30 minutes.

While caching offers the advantage of improving throughput, the common disadvantage is the possibility of aged data. Therefore, the network administrators, with the assistance of the vendor, should inspect the cache periodically to determine the ideal expiration time, and tune the contents of the cache accordingly.

3.3.5.2.5 Failover Procedures

Under normal operations, the SC communicates the LDAP Updates directly to the Primary MRDB. The Backup MRDB is synchronized with the Primary MRDB periodically to be able to stand in for the Primary MRDB when the latter experiences downtime.

The SCs will maintain communication with both the Primary and Backup MRDBs via periodic "keep-alive" messages. Lack of response from an MRDB will indicate to the SC that the MRDB is potentially experiencing a failure. Procedures are described in this section's requirements to help (1) minimize loss of update information intended for the MRDB, (2) automatically redirect the Update requests to an available MRDB, and (3) alert network personnel of the failed MRDB.

After the Primary MRDB has been repaired, the MRDB DBA will be able to initiate transfer of the downtime SC Update transactions from the Backup MRDB to the Primary MRDB. The administrator should ensure that the Primary MRDB is not returned to service (i.e., not re-connected to the SCs that it serves) until its data records are updated. Once the Primary MRDB is returned to service, each SC craftsperson should be able to reconnect their SC to that MRDB.

Each SC should automatically redirect its DB Update traffic (LDAP Add, Modify, and Delete messages) from the Primary MRDB to the Backup MRDB when the Primary MRDB fails. But the restoration of SC "DB Update" traffic from the Backup MRDB to the Primary MRDB requires SC craftsperson involvement, since the restoration of the Primary MRDB requires DBA involvement.

The SCs and SSs will maintain communication with Primary and Secondary LRDBs via periodic keep-alive messages. Lack of response from an LRDB will indicate to the SC or SS that the LRDB is potentially experiencing a failure. A set of procedures are described in this section's requirements to help (1) realize the cost savings of the Commercial Cost Avoidance feature, (2) reduce call setup delays for the HR feature, and (3) automatically redirect the Search requests to an available Database for prompt processing.

NOTE: The SCs exchange keep-alive messages with all DBs (MRDB, Backup MRDB, and LRDB). The SSs exchange keep-alive messages with the LRDBs only.

AUX-001630 [**Required: SC, SS**] The SC or SS shall use keep-alive messages to verify that the MRDB (or the Backup MRDB) and the LRDBs are available.

a. The frequency of the keep-alive messages shall be settable (Timer Ta) by the SC and SS administrators based on traffic volumes, with a default of Ta= 5 minutes.

b. The value of Ta shall range from 0–30 minutes and shall be settable in increments of 5 minutes.

AUX-001640 [**Required: SC, SS**] The keep-alive messages sent from the SC or SS to the LRDB or MRDB shall consist of the following sequence:

a. Bind request. (If a previous Bind request is still in effect and has not expired, then a new Bind request shall not be sent.)

b. Search request on a predetermined LDAP Distinguished Name (DN).

When a new Bind request is sent, upon receiving a successful Bind response with resultCode = 0, the SC or SS shall issue a Search request for a predetermined LDAP DN.

When a previous Bind request is still in effect and has not expired, the SC or SS shall issue a Search request for a predetermined LDAP DN.

It is expected that the LDAP DN selected by the SC/SS administrator for these preset keep-alive messages will always be populated in each LRDB and MRDB, to avoid keep-alive failure errors.

When the SC or SS receives a Search response message indicating that the entry is found, the keep-alive message is considered successful, and the SC or SS shall complete the operation and shall reset Ta.

The SC or SS shall also reset Ta after each successful LDAP Request/Response exchange (Search, Add, Modify, or Delete) between the SC or SS and the target LRDB or MRDB.

AUX-001650 [**Required: SC, SS**] The SC or SS shall keep track of the last status (active or inactive) for each LRDB or MRDB to which it sent a keep-alive message. The status shall indicate if the Database is functional or is out of service. This status will be used in subsequent determinations of applying failover procedures.

AUX-001660 [**Required: MRDB, Backup MRDB, LRDB**] The MRDB, Backup MRDB, and LRDB shall support the processing of keep-alive messages from the SCs and SSs.

3.3.5.2.5.1 MRDB Failover

During failover operation, when the Primary MRDB becomes unavailable and the Backup MRDB becomes the active MRDB, the SCs send their updates (individual or bulk) to the Backup MRDB, and the Backup MRDB queues these updates for later transmission to the Primary MRDB (i.e., when the Primary MRDB is restored to service). The Backup and Primary MRDBs support periodic synchronization procedures to ensure that their data content is consistent.

AUX-001670 [**Required: SC**] Each SC that accesses the Primary and Backup MRDBs shall support the configuration of two DISA network IP addresses for those MRDBs: one for the Primary MRDB (used when the Primary is active) and another for the Backup MRDB (used when the Primary has failed).

3.3.5.2.5.1.1 Primary Master Down, Backup Master Active

AUX-001680 [**Required: SC**] If the SC does not receive a response from the Primary MRDB within 2 seconds of sending a keep-alive message or a valid LDAP message (update or search), then the SC shall try sending another keep-alive message or resend the same LDAP message.

AUX-001690 [**Required: SC**] If no response is received from the Primary MRDB within 5 seconds of the retry attempt, then the SC shall do the following:

a. Stop sending LDAP Updates to the Primary MRDB.

b. Establish, if necessary, an LDAPv3 over TLS connection with the Backup MRDB.

c. If the most recent status of the Backup MRDB is "functional," then continue with step d. otherwise, the SC shall withhold any updates and continue sending keep-alive messages to both Primary and Backup MRDBs until one responds.

d. Send all subsequent LDAP Update operations (additions and deletions of DSN or commercial number pairs) to the Backup MRDB instead.

e. Continue keep-alive messages with the Primary and Backup MRDBs.

AUX-001700 [**Optional: Backup MRDB**] The Backup MRDB shall always queue the LDAP Updates it receives from the SC.

Updates received by the Backup MRDB are most likely to occur during periods of the Primary MRDB's unavailability.

AUX-001710 [**Required: SC**] The SC shall continue sending the LDAP Updates to the Backup MRDB until it receives a successful response to a keep-alive message from the Primary MRDB.

AUX-001720 [**Optional: MRDB**] The Primary MRDB shall not send a successful response to any keep-alive messages until it has been loaded with the queued updates from the Backup MRDB and/or the SC. This should be ensured by the network personnel performing the necessary repairs on the MRDB before returning the MRDB back online, after the cause of failure has been resolved and the Primary MRDB has regained functionality.

AUX-001730 [**Optional: LRDB, MRDB, Backup MRDB**] The Primary MRDB shall support a request to transfer the downtime queued update, for a given time period specified by the network administrator, from the Backup MRDB.

Network administrators and DBAs will return the Primary MRDB to service after all the "downtime" updates have been integrated in its files successfully. The goal is to ensure that the Primary MRDB is not placed back in service until it has been updated with the recent modifications that took place while it was out of service. When the Primary MRDB is ready to handle requests, the DBA could (a) change the address in the SC from the Backup MRDB to that of the Primary MRDB, thus redirecting traffic immediately to the Primary MRDB, or (b) wait for the Primary MRDB to reply to the next keep-alive message from the SC.

AUX-001740 [**Required: SC**] The SC shall give the SC administrator the ability to change, on demand, the address to which the SC LDAP updates should be directed.

AUX-001750 [**Required: SC**] When the Database address in the SC is reset to the Primary MRDB, or when the SC receives a successful response to the keep-alive message from the Primary MRDB, the SC shall do the following:

a. Stop sending LDAP Updates to the Backup MRDB.

b. Reestablish an LDAPv3 over TLS connection with the Primary MRDB.

c. Resume sending LDAP Updates to the Primary MRDB.

d. Continue sending keep-alive messages to the Primary and Backup MRDBs according to Timer Ta.

AUX-001760 [**Required: Backup MRDB**] During failover (when the Primary MRDB is out-of-service and the Backup MRDB stands in), authorized DISA personnel (craftspeople, network managers, DBA) shall be able to access the Backup MRDB and perform LDAP Search operations, LDAP Update operations, and LDIF file imports on it.

It is expected that the Backup MRDB will be capable of handling the LDAP Update traffic load during failover conditions.

3.3.5.2.5.1.2 Primary Master Down, Backup Master Down

Although unlikely, it is possible that the Backup MRDB would do one of the following:

- Be down already when the Primary MRDB fails.
- Experience a failure shortly after it starts to stand in for the Primary MRDB.

AUX-001770 [**Required: SC**] During failover mode to the Backup MRDB, if the SC does not receive a response from the Backup MRDB within 2 seconds of sending a keep-alive message or an LDAP Update request, then the SC shall retry sending the message to the Backup MRDB.

AUX-001780 [**Required: SC**] If no response is received from the Backup MRDB for the retry message within 5 seconds (i.e., both Primary and Backup MRDBs are now out of service), then the SC shall do the following:

a. Report alarms for a critical error to the network administrator.

b. Queue subsequent LDAP Update operations.

c. Initiate Ta and continue sending keep-alive messages to both Primary and Backup MRDBs until it receives notification that either the Primary or Backup MRDB has been restored to service.

AUX-001790 [**Optional: SC**] While both the Primary and Backup MRDB are down, the SC shall maintain a log of the LDAP Updates that it tried to send to the Primary and Backup MRDBs. The log shall contain the address of the destination Database, timestamps, target LDAP DN, and Update transaction.

The log will serve as a reference for audits.

3.3.5.2.5.2 LRDB Failover

Each theater is expected to have one or more LRDBs serving the HR or Commercial Cost Avoidance LDAP Search requests from the SCs or SSs. In that topology, the LRDBs are expected to act as potential backups for each other. If an LRDB (e.g., Database #1) fails, then the SC will reroute LDAP requests destined for Database #1 to another LRDB (e.g., Database #2), defined here as the "Secondary." The rerouting continues until Database #1 is returned to service.

AUX-001800 [**Required: SC, SS**] Each SC or SS that accesses LRDBs shall support the configuration of two DISA network IP addresses for those Routing DBs: one for a Primary LRDB and another for a Secondary LRDB (used when the Primary has failed).

As noted in Section 3.3.5.2.5, Failover, each SC and SS shall use an independent Timer Ta to schedule sending the keep-alive messages to its Primary and Secondary LRDBs.

3.3.5.2.5.2.1 Primary Local Down, Secondary Local Active

AUX-001810 [**Required: SC, SS**] If the SC or SS does not receive a response from the Primary LRDB within 0.5 seconds of sending a keep-alive message or an LDAP Search request, then the SC or SS shall send another keep-alive message or resend the same LDAP Search request.

AUX-001820 [**Required: SC, SS**] If no response is received from the Primary LRDB for the retry message within 0.5 seconds, then the SC or SS shall do the following:

a. Stop sending LDAP Search requests to the Primary LRDB.
b. Redirect the LDAP Search requests to the Secondary LRDB immediately.
c. Continue keep-alive messages with the Primary and Secondary LRDBs.
d. If the most recent status of the Secondary LRDB is "functional," then continue with step c of AUX-001790. Otherwise, the SC or SS shall utilize commercial number routing instead of performing Commercial Cost Avoidance, and utilize internal SS routing tables instead of performing HR.

AUX-001830 [**Required: SC, SS**] The SC or SS shall continue sending the LDAP Search operations to the Secondary LRDB until it receives a successful response to a keep-alive message from the Primary LRDB.

When the Primary LRDB is restored from "out-of-service" to "in-service," the Primary LRDB should not send a successful response to any keep-alive messages from SCs or SSs until it has been updated with the latest data from the MRDB. This should be ensured by the network personnel performing the necessary repairs on the Primary LRDB before returning the Primary Database back online.

AUX-001840 [**Optional: LRDB, MRDB, Backup MRDB**] The Primary LRDB shall be able to request a partial synchronization from the MRDB, specifying the start time as that time the Database went out of service. The MRDB (or Backup MRDB) shall support that request.

Network administrators or DBAs should return the Primary LRDB to service after all "downtime" updates from the MRDB have been integrated successfully in its files. The goal is to ensure that the Primary LRDB is not returned to service until it has been updated with the recent MRDB modifications that took place while it was out of service. When the Primary LRDB is ready to handle Search requests, the SC and SS administrators could (a) change the address in the SCs and SSs from the Secondary LRDB to that of the Primary LRDB, thus redirecting traffic immediately to the Primary LRDB or (b) wait for the Primary LRDB to reply to the next keep-alive message from each SC and SS.

AUX-001850 [**Required: SC, SS**] The SC and SS shall give the SC and SS administrators the ability to change the address, on demand, to which the SC and SS Search requests should be directed.

AUX-001860 [**Required: SC, SS**] When the LRDB address in the SC or SS is reset to the address of the Primary LRDB, or when the SC or SS receives a successful response to the keep-alive message from the Primary LRDB, the SC or SS shall do the following:

a. Stop sending LDAP Searches to the Secondary LRDB.
b. Resume sending LDAP Searches to the Primary LRDB.
c. Continue sending keep-alive messages to the Primary and Secondary LRDBs according to Timer Ta.

It is expected that the Secondary LRDB will be capable of handling the LDAP Search traffic load during failover conditions.

3.3.5.2.5.2.2 Primary Local Down, Secondary Local Down

Although unlikely, it is possible that the Secondary LRDB is out of service at the same time as the Primary LRDB. In that case, the following requirements will be followed.

AUX-001870 [**Required: SC, SS**] Following the failure of the Primary LRDB, if no response is received from the Secondary LRDB within 2 seconds of sending a keep-alive message or an LDAP Search request message, then the SC or SS shall retry sending the message to the Secondary LRDB.

AUX-001880 [**Required: SC, SS**] If no response is received from the Secondary LRDB for the retry message within 5 seconds, then the SC or SS shall do the following:

a. Report alarms for a critical error to the network administrator.
b. Stop sending LDAP requests to the LRDBs.

c. Start Timer Ta.

d. Maintain keep-alive messages with both Primary and Secondary LRDBs using Ta.

The failure of both Primary and Secondary LRDBs affects HR call routing and defeats the cost savings intended from Commercial Cost Avoidance. Therefore, it is important to return at least one LRDB back to service, or to have more than one Secondary LRDB provisioned for each SC or SS. After the DBs are restored, the DBAs will notify the SC and SS administrators so that their SCs and SSs can start sending their Search requests to the appropriate LRDB.

AUX-001890 [**Required: SC, SS**] When both the Primary and Secondary LRDBs are out-of-service, and the SC or SS receives a successful response to the keep-alive message from the Primary LRDB, the SC or SS shall do the following:

a. Stop sending LDAP Search requests to the Secondary LRDB.

b. Resume sending LDAP Search requests to the Primary LRDB.

c. Resume sending keep-alive messages to the Primary and Secondary LRDBs based on Ta.

AUX-001900 [**Required: SC, SS**] When both the Primary and Secondary LRDBs are out-of-service, and the SC or SS receives a successful response to the keep-alive message from the Secondary LRDB, the SC or SS shall do the following:

a. Stop sending LDAP Search requests to the Primary LRDB.

b. Resume sending LDAP Search requests to the Secondary LRDB.

c. Resume sending keep-alive messages to the Primary and Secondary LRDBs based on Ta.

3.3.5.2.6 Provisioning

In the following requirements, “bulk upload” refers to a method in which number records are uploaded into the LRDB or MRDB “in bulk,” rather than uploaded individually using LDAP Update operations (such as Add, Modify, and Delete). For an LRDB, the source of the data for the “bulk uploads” may be the MRDB or the Backup MRDB. For an MRDB, the source of the data for the “bulk uploads” may be a set of SCs containing number records, or it may be another database that is a copy of the MRDB (e.g., the Backup MRDB).

Bulk uploads will be used during the initial provisioning of the LRDB or MRDB (e.g., population of the MRDB from multiple SCs that already contain number records), or during full reloads of that Database (e.g., population of LRDB records from the MRDB, after a loss of data). An example of a “bulk upload” technique is transfer of LDAP Data Interchange Format (LDIF) files from an individual SC to the MRDB, using e-mail messages or FTP sessions. LDIF file transfer implies a manual export of LDIF data at the source end (e.g., SC) and manual import of LDIF data at the receiving end (e.g., MRDB). Other bulk upload techniques can also be used, if supported by the LRDB, MRDB, and SC vendors.

Commercial experience with bulk uploads for DBs containing millions of records has shown that the time needed to perform a bulk upload goes down as the size of the upload transactions (the data "chunks") used in the bulk upload goes up. In other words, the time needed for bulk uploading records is inversely proportional to the size of the upload transactions or "chunks" used to perform the bulk-upload.

It is therefore recommended that the MRDB and LRDB include as many Database records as possible within each "bulk upload" transaction to reduce the "bulk upload" provisioning time at the LRDB or MRDB. It is also recommended that a small number of high-volume transactions be used for "bulk uploads," instead of a large number of low-volume transactions.

AUX-001910 [**Required: LRDB**] The LRDB shall support a maximum bulk upload time of 16 hours for a Database size of 8 million records, using multiple bulk upload transactions in which each transaction contains a fraction of the 8 million records.

AUX-001920 [**Required: MRDB, Backup MRDB**] The MRDB and Backup MRDB shall be able to accept a bulk update of the full set of 8 million Database records (via LDIF file transfer or other methods) within a period of no more than 16 hours, using multiple bulk upload transactions in which each transaction contains a fraction of the 8 million records.

AUX-001930 [**Required: LRDB, MRDB, Backup MRDB**] In addition to supporting bulk uploads, the LRDB and MRDBs shall support user interfaces (e.g., a Web-based Graphical User Interface [GUI] and a text-based command line interface) that allow end users to configure and update the Database. The LRDB and MRDBs shall allow DISA to make these interfaces available to local DISA craftspeople, remote DISA craftspeople, and remote DISA Operations Systems (such as the RTS Element Management System [EMS]).

AUX-001940 [**Required: LRDB, MRDB, Backup MRDB**] The LRDB and MRDBs shall allow an authorized craftsperson, DBA, or remote DISA Operations System to access the LRDB and MRDBs for reading, writing, and updating record data.

AUX-001950 [**Required: LRDB, MRDB, Backup MRDB**] The LRDB and MRDBs shall allow an authorized craftsperson, DBA, or remote DISA Operations System to access the LRDB and MRDBs for configuring the following:

a. Department of Defense (DoD) public key infrastructure (PKI) certificates (used with TLS authentication) for both the Database itself and the various Database clients (i.e., SCs and SSs in that theater).

b. LDAP User Names and Passwords (used with LDAP Bind message authentication) for the various Database clients (SCs and SSs in that theater).

3.3.5.2.7 Synchronization Between Primary and Backup MRDBs

In each theater, the LRDBs are expected to act as backups for each other. The Primary MRDB also has one Backup MRDB. The purpose of this Backup MRDB is to provide a most recent

duplicate of the Primary MRDB in case of an outage, data loss, or catastrophic failure at the Primary MRDB. This allows SCs sending Database updates to "fail over" from the Primary to the Backup MRDB when the Primary MRDB is out of service.

AUX-001960 [**Required: MRDB, Backup MRDB**] The Primary MRDB shall support full data updates (full data backups) to the Backup MRDB during non-busy hours (based on the Primary MRDB's local time zone).

AUX-001970 [**Optional: MRDB**] The Primary MRDB shall support the performance requirements listed in this document (i.e., minimum operations per second and maximum processing time) during the "full data backup" process with the Backup MRDB. This means that the Primary MRDB shall be able to support bulk updates from SCs, LDAP Search operations from SCs, and LDAP Update operations from SCs, while simultaneously performing a full data backup with the Backup MRDB.

AUX-001980 [**Optional: MRDB, Backup MRDB**] The Primary MRDB shall support the performance of full data backups with the Backup MRDB on a configurable scheduled basis. The Primary MRDB shall support scheduled full data backup settable frequencies of every 6 hours, every 12 hours, and every 24 hours.

AUX-001990 [**Optional: MRDB, Backup MRDB**] The Backup MRDB shall be coupled with the Primary MRDB via redundant, physically diverse, high throughput TLS over IP connections, and shall function as a "hot standby" for the Primary MRDB. These master-to-master connections shall be secured using TLS with DoD PKI certificates, consistent with the requirements for securing exchange of LDAPv3 messages over TLS.

AUX-002000 [**Optional: MRDB, Backup MRDB**] The Primary and Backup MRDBs shall give DISA the ability to initiate a "full data backup" at any time, independent of when the last scheduled full data backup was performed.

3.3.5.2.8 Synchronization Between LRDB and MRDB

The requirements in this section apply to the LRDB and MRDB. In general, the LRDB and MRDB are located in physically separate sites.

AUX-002010 [**Required: LRDB, MRDB**] The LRDB shall support an interface to the MRDB, and the MRDB shall support an interface to the LRDB, to support Database synchronization for the Commercial Cost Avoidance and HR features.

AUX-002020 [**Required: LRDB, MRDB**] The Database synchronization interface between the LRDB and the MRDB shall be LDAPv3 over TLS over IP. This LDAPv3 interface shall be compliant with the following LDAP v3 RFCs:

RFC 2251, RFC 2252, RFC 2253, RFC 2254, RFC 2255, RFC 2256, RFC 2829, RFC 2830.

AUX-002030 [**Required: LRDB, MRDB**] The LDAPv3 Data schema used on the Database synchronization interface between the LRDB and MRDB shall include all of the following information fields:

a. Entry field containing an LDAP Distinguished Name containing the following:
   (1) User ID component containing the commercial number (e.g., UID=7038821234) of the end user.
   (2) Domain components "uc" and "mil" (dc=uc, dc=mil).
b. Attributes field containing the following attributes:
   (1) User ID field containing the commercial number of the end user.
   (2) SIP Alias field containing the full international format commercial called number of the end user followed by "@uc.mil."
   (3) sip User Name field containing the UID (i.e., commercial number) followed by "@uc.mil."
   (4) Directory Number field containing the full 10-digit DSN number of the end user.
   (5) LSCCCAID field containing the CCA-ID of the SC serving the end user.
   (6) SSCCAID field containing the CCA-IDs of the primary SS and the backup SS serving this SC, separated by a comma.
   (7) Object Class field containing "mobSLR."

AUX-002040 [**Required: LRDB, MRDB**] The encoding of the LDAPv3 messages and data schema used on the Database synchronization interface between the LRDB and MRDB shall follow the BER of ASN.1.

AUX-002050 [**Required: LRDB, MRDB**] The Database synchronization interface between the LRDB and MRDB shall be secured using TLS, consistent with the requirements for securing AS-SIP messages using TLS in Section 4, Information Assurance. This security shall provide mutual authentication between the LRDB and MRDB, message confidentiality for the Database synchronization messages, and message integrity for the Database synchronization messages.

AUX-002060 [**Required: LRDB, MRDB**] The Database synchronization interface between the LRDB and MRDB shall traverse the data firewalls at both the LRDB and MRDB sites.

AUX-002070 [**Required: LRDB, MRDB**] The Database synchronization interface between the LRDB and MRDB shall traverse the CE-Rs at both the LRDB and MRDB sites, using the DSCP for User Signaling traffic, and the associated CE-R queues.

AUX-002080 [**Required: MRDB**] The MRDB shall be capable of maintaining multiple Database synchronization interfaces to different LRDBs at the same time. Each individual Database synchronization interface shall support the previous requirements for the protocols, data schemas, and security mechanisms used between an individual LRDB and the MRDB.

Typically, Database synchronization methods are vendor-proprietary, and are not expected to have an effect on Database performance for this Routing Database implementation within DISA. The Primary and Backup MRDBs are expected to be the ultimate data sources available to the various LRDBs for synchronization purposes. The Database synchronization requirements call for a master-subordinate configuration, in which the MRDBs are the "masters" and the LRDBs are the "subordinates."

AUX-002090 [**Required: LRDB, MRDB, Backup MRDB**] The MRDBs shall be able to perform their Database synchronization with the LRDBs through a "push" model, in which data records are downloaded from one MRDB to the LRDBs on a programmable schedule.

a. Under normal operation, the data push shall be from the Primary MRDB to the various LRDBs.

b. Under MRDB failover operation, the data push shall be from the Backup MRDB to the various LRDBs, since the Primary MRDB is out-of-service.

AUX-002100 [**Required: LRDB**] The LRDB shall be able to support SC and SS Search requests during its synchronization process with the MRDB.

AUX-002110 [**Optional: LRDB, MRDB, Backup MRDB**] The MRDBs shall be able to perform their Database synchronization with the LRDBs through a pull model, in which data records are downloaded from one MRDB to the LRDB, based on a pull request from the LRDB (e.g., in case of data loss at the LRDB).

a. Under normal operation, the data pull shall be from the Primary MRDB to the LRDBs (as initiated by the LRDB).

b. Under failover operation, the data pull shall be from the Backup MRDB to the LRDBs (as initiated by the LRDB), since the Primary MRDB is out-of-service.

AUX-002120 [**Required: MRDB, Backup MRDB**] The MRDB shall maintain a status on each of the LRDBs that it is responsible for synchronizing. At minimum, the status information shall include or record the following:

a. Timestamp for the last update for each LRDB.

b. Type of update (full or incremental).

AUX-002130 [**Required: MRDB, Backup MRDB**] The Database synchronization process between the MRDB and LRDB shall be possible through full or incremental updates. Incremental updates deliver only the records that were modified or created since the last known update.

AUX-002140 [**Required: MRDB, Backup MRDB**] The MRDB shall perform full and incremental updates according to a settable schedule or on an on-demand basis.

It is expected that incremental synchronizations will take place more frequently than full database synchronizations as the size of the database grows. Typically, full synchronizations are

more appropriate in the case of a database reload after data loss, while incremental updates pose minimal effect on traffic and resources within the Database architecture.

AUX-002150 [**Optional: MRDB, Backup MRDB**] The MRDB (or Backup MRDB) shall be able to synchronize its data with two LRDBs simultaneously.

It is important to complete the synchronization of the MRDB with all LRDBs within a short time, in order for all Commercial Cost Avoidance and HR queries from the various clients (i.e., SCs and SSs) to receive consistent responses from all local DBs.

AUX-002160 [**Required: LRDB, MRDB, Backup MRDB**] Under normal operations (no Database failover scenarios and no Database scheduled maintenance), the simultaneous synchronization between the MRDB and every pair of LRDBs shall be completed within a period of no longer than 8 hours. The MRDB, Backup MRDB, and LRDB shall support the number of interfaces necessary to perform the synchronization within the required period.

AUX-002170 [**Optional: MRDB, Backup MRDB**] If the MRDB attempts a synchronization with an LRDB, and the target LRDB is out of service at the scheduled time (e.g., a communication error is received from the LRDB), then the MRDB shall attempt the synchronization again in 30 minutes from the original scheduled time. If this second attempt fails, then the MRDB shall reattempt the synchronization one last time 60 minutes after the original start time.

AUX-002180 [**Optional: MRDB, Backup MRDB**] If the MRDB's third and final attempt at synchronization with any LRDB fails, then the MRDB shall notify the DBA by issuing an alarm identifying 1) the address of the LRDB that failed to receive synchronization updates from the Primary or Backup MRDB and 2) the time of the last attempt.

If an LRDB was not available for synchronization, then the next scheduled synchronization is expected to take place during one of the following:

a. At regularly scheduled times, after the LRDB has been repaired and returned to service.
b. Per the LRDB administrator's request (as soon as the LRDB is repaired).

3.3.6 MRDB and LRDB Operations

3.3.6.1 Overview

The objective of a Routing Database operations plan is to preserve Database integrity and to provide high-quality service. Operations, administration, and maintenance guidelines are provided by the Routing Database vendors and should be followed as directed for robust performance.

This section addresses the majority of the requirements for the functional areas of the Routing DBs and Signaling Appliances (Master and Local DBs, SCs, and SSs) that support the

Commercial Cost Avoidance and HR features. Other sections containing related requirements are referenced throughout this section.

The functional areas are as follows:

- Trouble Detection and Reporting. The functions necessary to detect, send notification of, and log failure conditions.
- Performance Monitoring. Measurements and data collection on utilization, errors, and availability to improve capacity planning and detect traffic overload conditions.
- Routing Database Archival. The functions necessary to provision additional backup in the form of a static archive.
- Security Management. Access rights and logs.

The required approach to managing the Routing Database is using Simple Network Management Protocol (SNMP) and MIBs. The two applicable Internet Engineering Task Force (IETF) Standards are Standards 58 and 62. These two standards are composed of the following requirements.

AUX-002190 [**Required: MRDB, Backup MRDB, and LRDB**] Standard 58, Structure of Management Information Version 2 (SMIv2): RFC 2578, RFC 2579, and RFC 2580.

AUX-002200 [**Required: MRDB, Backup MRDB, and LRDB**] Standard 62, Simple Network Management Protocol Version 3 (SNMPv3): RFC 3411, RFC 3412, RFC 3413, RFC 3414, RFC 3415, RFC 3416, RFC 3417, and RFC 3418.

Much of the Configuration Management (CM) requirements are covered in Section 3.3.5, LRDB and MRDB. Provisioning a Routing Database, including bulk updates to initially load the database and configure security settings, is discussed in Section 3.3.5.2.6, Provisioning. Requirements for synchronization of data between a Primary and Backup MRDB are in Section 3.3.5.2.7, Synchronization Between Primary and Backup MRDBs. Requirements for synchronization between an LRDB and an MRDB are in Section 3.3.5.2.8, Synchronization Between LRDB and MRDB.

3.3.6.2 Trouble Detection and Reporting

This section discusses Alarms, Event Logs, and Audits used by operations personnel to detect and resolve trouble conditions.

3.3.6.2.1 Alarms

This section covers requirements for Alarms to be issued by the Routing Database or SC or SS when conditions exist on the LDAP interface between an SC or SS and a Routing Database that may be symptomatic of a hardware or software failure.

In addition to failures, alarms may be issued when there are resource or performance degradation issues caused; for example, by excessive traffic. Based on performance measurement thresholds configured by the network administrator and DBA, notifications and alarms are generated.

AUX-002210 The SC or SS shall support the generation and reporting of alarms for the following scenarios:

AUX-002210.a [Required: SC, SS]The SC or SS detects loss of connectivity with any of the LRDBs or MRDBs (e.g., no response to an LDAP Bind): the alarm message shall contain the identity of the affected Database, timestamp, and error type, if applicable.

AUX-002210.b [**Optional: SC, SS]** The number of LDAP error messages received from an LRDB exceeds a threshold during a 5-minute interval: the alarm message shall contain the identity of the affected Database, timestamp, and error types. The thresholds set by each network administrator will var]y depending on the volume of traffic each Database is expected to support.

AUX-002210.c [**Optional: SC, SS**] The number of LDAP error messages from the Primary or Backup MRDB exceeds a threshold during a 5-minute interval: the alarm message shall contain the identity of the affected Database, timestamp and error types. The thresholds set by each network administrator will vary depending on the volume of traffic each Database is expected to support.

AUX-002210.d [Required: SC, SS] The SC or SS determines that it should reroute LDAP Search requests to a Secondary LRDB; i.e., a failover (refer to Section 3.3.5.2, Routing Database, for detailed requirements on the conditions triggering these alarms).

AUX-002210.e [Required: SC, SS] The SC determines that it should reroute LDAP Update requests from the Primary MRDB to the Backup MRDB (failover); this indicates that the Primary MRDB is out of service and requires attention.

AUX-002210.f [Required: SC, SS] The SC does not receive responses to retry messages from the Backup MRDB (indicating that both the Primary and Backup MRDBs have failed).

AUX-002210.g [**Optional: SC, SS**] The SC or SS encounters a time-out on a Search request, attempts to send the Search twice more, and the response time still exceeds the set threshold.

AUX-002210.h [**Optional: SC, SS]** The SC encounters a time-out on an Update request, attempts to send the Update request twice more, and the response time still exceeds the set threshold.

AUX-002210.i [Required: SC, SS] The SC or SS receives an error response LDAP_INVALID_CREDENTIALS (49) on three consecutive Bind attempts within 30 seconds; this error response could signal an unauthorized access attempt to the database(s).

AUX-002210.j [**Optional: SC, SS**] The SC or SS receives an improperly formatted response from a Routing Database on the first attempt and two subsequent retries; this response could point to errors in the Database processing or Database data integrity.

AUX-002210.k [**Optional: SC, SS**] The SC attempts an Update (Modify or Delete) in which the pilot Search result shows that the CCA-ID of the SC does not match that of the target record, or is missing.

AUX-002220 The Primary MRDB, Backup MRDB, and LRDB shall support the generation and reporting of alarms for the following scenarios as described:

AUX-002220.a [Optional: MRDB, Backup MRDB, and LRDB] A Primary or Backup MRDB fails to synchronize with an LRDB at the scheduled time and/or on reattempts: the alarm message shall contain the identities or addresses of the Primary or Backup MRDB and the LRDB in question, and the time stamp of the attempt (refer to Section 3.3.5.2, Routing Database, for detailed requirements on the conditions triggering these alarms).

AUX-002220.b [**Optional: MRDB, Backup MRDB, and LRDB]** The average Routing Database LDAP response time for Search requests, measured over a 5-minute interval, exceeds a preset threshold (set by the network administrator).

AUX-002220.c [Optional: MRDB, Backup MRDB, and LRDB] The number of LDAP error responses returned on Bind requests because of invalid credentials, during a 5-minute interval, exceeds a threshold (set by the network administrator).

AUX-002220.d [**Optional: MRDB, Backup MRDB, and LRDB]** The average Routing Database LDAP response time for Bind requests, over a 5-minute interval, exceeds a threshold (set by the network administrator).

AUX-002220.e [Optional: MRDB, Backup MRDB, and LRDB] The Routing Database average CPU utilization for an individual processor or all processors in a given Database exceeds 90 percent for a 5-minute interval.

AUX-002220.f [**Optional: MRDB, Backup MRDB, and LRDB]** The number of LDAP requests that are not formatted properly from an SC or SS exceeds a preset threshold (set by the network administrator) during a 5-minute interval; this could point to errors in the SC or SS processing.

AUX-002230 [**Required: MRDB, Backup MRDB, and LRDB**] The Primary MRDB, Backup MRDB, and LRDB shall support Simple Network Management Protocol version 3 (SNMPv3) interfaces to remote network management systems for the reporting of alarms.

3.3.6.2.2 Logs

Logs capture events over a time interval. Logs can be useful for diagnostics and troubleshooting as well as other Network Management activities.

AUX-002240 [**Optional: MRDB, Backup MRDB, and LRDB**] The MRDB, Backup MRDB, and LRDB shall support the generation of logs that span settable periods (default 1 week). The MRDB, Backup MRDB, and LRDB shall allow the administrators to set that period.

AUX-002250 [**Optional: MRDB, Backup MRDB, and LRDB**] The MRDB, Backup MRDB, and LRDB shall support the memory requirements necessary to store log files that span a period of 6 months.

AUX-002260 [**Optional: MRDB, Backup MRDB, and LRDB**] The Database Management System (DBMS) governing the MRDB, Backup MRDB, and LRDB shall support the generation of a downtime log for each Database. The downtime log shall store an event record each time a Routing Database goes out of service or returns to service. Each event shall include the following:

a. Identity of the Database.

b. Date and time the Database failure or restoration occurred.

AUX-002270 [**Optional: MRDB, Backup MRDB, and LRDB**] The MRDB, Backup MRDB, and LRDB shall support the generation of an LDAP Error log documenting the LDAP error response messages returned to its clients. Each log record shall include the following:

a. Identity of the database.

b. Identity of the LDAP client receiving the error.

c. Type of error.

d. Date and timestamps for each message sent.

Database access is allowed only to pre-authorized entities. Therefore, unauthorized attempts should be reported. Access logs should record key access incidents and repeated unauthorized attempts.

AUX-002280 [**Optional: MRDB, Backup MRDB, and LRDB**] The MRDB, Backup MRDB, and LRDB each shall support the generation of a security access log documenting all access that requires credentials, both authorized and unauthorized access (e.g., all Bind responses in which an error response was returned because of invalid credentials). Each access log(s) record shall contain the following details:

a. Date and time of access.

b. User ID or system ID (e.g., SC ID).

c. Credentials received by the Database from the accessing entity.

d. Response sent back from Database.

It is not recommended or encouraged to perform non-standard or emergency "manual" updates to any Routing Database on a regular basis. However, if it does occur through an authorized craftsperson station or DBA station, then it is required to be sent directly to the master or backup Database (depending on which one is active at the time). For data integrity and auditing purposes, a non-standard update should be logged and promptly entered in the master Database.

AUX-002290 [**Optional: MRDB, Backup MRDB, and LRDB**] The MRDB, Backup MRDB, and LRDB shall support the creation of a manual update log. Each log record shall contain the following:

a. Time and date of manual update.

b. Source: IP address from which the update originated.

c. Authorization information to identify the administrator or craftsperson originating the manual update.

d. Distinguished Name of the Database record updated.

e. Attribute or entry updates made.

Each administrator could use the log to identify updates that originated from his or her theater and perform random checks to ensure that the updates are in effect. The MRDB DBA will be able to view the number of updates originating from each theater and perform the necessary checks to ensure that the MRDB is updated.

AUX-002300 [**Optional: MRDB, Backup MRDB, and LRDB**] The MRDB, Backup MRDB, and LRDB shall support logging the following events along with the time and date for each:

a. Synchronization attempt with another Routing Database.

b. Synchronization result for each attempt (successful and failed attempts).

c. Full data backups performed by DISA personnel on each Database.

AUX-002310 [**Optional: SC, SS**] The SC or SS shall support logging the following events:

a. Every failover to a Secondary LRDB and restoration to the Primary LRDB, along with the date and time of the failover or restoration and the original and alternate database addresses or identity.

b. For SCs only, every failover to a Backup MRDB and restoration to the Primary MRDB, along with the date and time of the failover or restoration, and the original and alternate database addresses or identity.

3.3.6.2.3 Audits

AUX-002320 [**Optional: MRDB, Backup MRDB, and LRDB**] The MRDB, Backup MRDB, and LRDB shall be capable of performing an audit request on demand or on a scheduled basis from authorized DBAs. The audit request shall contain one of the following actions:

a. Perform a partial comparison of entries in the MRDB and the LRDB for a range of Distinguished Names (DNs).

b. Perform a full comparison of all entries between the MRDB and the LRDB.

   While the Primary MRDB is out of service, updates are redirected to the Backup MRDB. For the purposes of audits, a separate log of those updates should be maintained by the Backup MRDB to be compared later to the actual data entries in both the Primary and Backup MRDBs.

AUX-002330 [**Optional: Backup MRDB**] The Backup MRDB shall maintain a log of all the updates received from the SCs when the Primary MRDB is out of service. The update log shall be available to authorized DBAs for viewing and auditing. Each update log record should contain the following:

a. Data and time of the update.

b. SC ID requesting the update.

c. DN of the record being updated, added, or deleted.

d. Set of attributes and values that are being updated.

3.3.6.2.4 Routing Database Archival

The data in the MRDB is critical to the Commercial Cost Avoidance and HR services. There are several measures that have been put in place to return the DBs to service as soon as possible if a Routing Database failure occurs or if the data becomes corrupted. In addition to the redundancy, synchronization, and failover requirements discussed in Section 3.3.5, LRDB and MRDB, this section recommends that a static archive be kept of the MRDB as another means of quickly restoring the data in a MRDB.

AUX-002340 [**Optional: MRDB, Backup MRDB**] The Primary and Backup MRDBs shall perform a partial or full update to the archive at least every 6 hours. The Primary and Backup MRDBs shall provide the capability to perform these updates automatically on a configurable schedule and manually on demand. The backup to the archive should be done while still meeting the MRDB throughput requirements in Section 3.3.5, LRDB and MRDB.

Archival backups could be transported physically (e.g., via courier) from the Primary MRDB and Backup MRDB locations to the archival backup site. However, that could cause recovery delays of at least 1 day in case that data is needed for a total reload of the database. Electronic backup to the archival backup site would consume much less time.

AUX-002350 [**Conditional: MRDB, Backup MRDB**] If archive backups are adopted, then the Primary and Backup MRDBs shall be able to transmit the archive backup files electronically to the hardware hosting the archive over a high-bandwidth connection (via a protocol such as FTP).

AUX-002360 [**Conditional: MRDB, Backup MRDB**] If archive backups are adopted, then the Primary and Backup MRDBs shall access the archival backup copies electronically via high-bandwidth connections to restore the Database. This shall be done manually by an authorized network administrator.

It is recognized that the archives will be, at most, 6 hours out of synch with the Primary and Backup MRDBs, but could nonetheless serve as the latest available copy of the Primary MRDB in case the Primary and Backup MRDBs undergo extensive damage.

3.3.6.2.5 Performance Monitoring

In addition to monitoring a Routing Database for failures, operations personnel need to monitor a Routing Database to ensure that it has been engineered with the resources needed to meet the traffic demands. The Routing Database needs to keep resource utilization and traffic measurements to help determine when additional capacity may be needed. Performance measurements are used to help determine when there is an impairment resulting in performance that is below expectations (e.g., slower response time). Some performance measurements have associated thresholds that if exceeded, will result in an alarm being generated. DBAs can tune the database performance and resources based on the reported measurements.

AUX-002370 [**Required: MRDB, Backup MRDB, and LRDB**] The MRDB, Backup MRDB, and LRDB shall be capable of sending traffic and performance measurements to the network administrator on a predetermined schedule (as set by the DBA) or when polled by the authorized DBA.

Visual-based tools can assist DBAs in their overall management role.

AUX-002380 [**Optional: MRDB, Backup MRDB, and LRDB**] The Database Management system for the MRDB, Backup MRDB, and LRDB shall support a visual interface or Graphical User Interface (GUI) to display the performance metrics of all the databases in all the theaters.

AUX-002390 [**Optional: MRDB, Backup MRDB, and LRDB**] The following measurements and statistics for each database shall be stored and be made available for retrieval at any time by the network administrators:

a. Disk utilization for the Database and log files, updated every 24 hours.

b. Average "total" CPU utilization in a 5-minute interval.

c. Average "individual" CPU utilizations in a 5-minute interval.

d. Number of TLS connections available between the Database and its clients (SCs, SSs, and other DBs) in a period of 1 hour.

e. Number of active TLS connections between the Database and its clients (SCs, SSs, and other DBs) in a period of 1 hour.

f. Number of active LDAP sessions between the Database and its clients in a period of 1 hour.

g. Number of Bind operations received in a 5-minute interval.

h. Number of Unbind operations received in a 5-minute interval.

i. Number of successful Binds processed in a 5-minute interval.

j. Average LDAP Bind time (Database time to respond successfully to a Bind request) measured in a 5-minute interval.

k. Number of LDAP Search request messages received in a 5-minute interval.

l. Number of LDAP Search response messages sent in a 5-minute interval.

m. Average LDAP Search response time (Database time to respond successfully to a Search request) in a 5-minute interval.

n. Number of Database entries returned to Database clients (SCs, SSs, and other DBs) in a 5-minute interval.

o. Number of LDAP Update request messages received in a 5-minute interval, with a breakdown for the number of (a) Update Add, (b) Update Delete, and (c) Update Modify.

p. Number of LDAP Update response messages sent in a 5-minute interval.

q. Average LDAP Update response time (Database time to respond successfully to an Update request) in a 5-minute interval.

r. Number of LDAP Error messages returned in a 5-minute interval.

s. Number of pending Database synchronizations (MRDB to LRDB; Backup MRDB to LRDB; MRDB to Backup MRDB); this may point to extended outages at the MRDB, the Backup MRDB, or the LRDB.

AUX-002400 [**Optional: SC, SS**] The following SC and SS measurements on Caching of Database Responses shall be available to the SC and SS administrators:

a. Percentage Cache Hit Rate: Percentage of Search requests handled by the cache, updated every 24 hours.

b. Cache Size: Actual data store in the memory cache (size of the full portion of the cache).

c. Age of Cache Records: Time stamp when oldest cache record was written into the cache.

d. Percentage Cache Miss Rate: Percentage of Search requests that were not served by the cache in a period of 1 hour (within that last hour).

e. Latency: Average latency to process cache requests (time difference between receipt of cache request and return of cache response), measured and updated in 5-minute intervals.

f. Up and Down times: Specifies the times that the cache was available (Up) or not available (Down), updated every 24 hours.

g. Active Connections: Average number of SC and SS connections to the cache, measured and updated in 5-minute intervals.

h. SC and SS products may support other query- and cache-related measurements different than the ones identified above.

AUX-002410 [**Optional: SC, SS**] SC and SS measurements on Caching of Database Responses shall be collected every 1 hour. Other intervals, including 5-min, 15-min, 30-min, and daily, shall also be allowed.

AUX-002420 [**Required: MRDB, Backup MRDB, and LRDB**] The Primary MRDB, Backup MRDB, and LRDB shall support Simple Network Management Protocol version 3 (SNMPv3) interfaces to remote network management systems for the reporting of performance monitoring measurements and statistics.

3.3.6.2.6 Security Management

This section discusses some of the security features that should be provided by a Routing Database. This includes authentication and authorization of operations personnel and the SCs and SSs that send LDAP messages to the Routing Database. Both remote and local accesses to the Routing DBs are included here.

The MRDB and LRDB perform different functions. The MRDB and its Backup MRDB are primarily "write" databases, in which updates on HR and Commercial Cost Avoidance routing are centrally aggregated and managed for distribution to the LRDBs. The latter, in turn, are responsible for all the "reads" or LDAP Search requests launched by the SCs and SSs to determine the correct routing paths for HR and CCA calls.

For both types, the "read" DBs and the "write" DBs, the DBs contain important information that should be made available only to authorized DISA personnel. DBAs are expected to implement a password policy for authorized personnel and different levels of access. DBAs also create user authorization lists for each database. Only entities with credentials that match entries on the authorization list will be allowed access.

AUX-002430 [**Required: MRDB, Backup MRDB, and LRDB**] The MRDB, Backup MRDB, and LRDB shall be configured with an "authorization list" that contains authorized users and their access levels. The list shall support user IDs and passwords for authorized personnel, as well as IP addresses for Database workstations, SCs, and SSs.

The DBs shall use DoD PKI certificates and negotiated TLS sessions in all their communications with Database workstations (both local and remote) SCs, and SSs.

AUX-002440 [**Required: MRDB, Backup MRDB, and LRDB**] The MRDB, Backup MRDB, and LRDB shall accept and process requests only from Database clients (SCs, SSs, and other DBs) with LDAP Bind requests containing credentials that match credentials on the "authorized" list.

AUX-002450 [**Required: MRDB, Backup MRDB, and LRDB**] The DBMS interfaces (e.g., craftsperson workstations) managing the MRDB, Backup MRDB, and LRDB shall not store, transmit, or display any LDAP client passwords in the clear.

AUX-002460 [**Required: MRDB, Backup MRDB, and LRDB**] The MRDB, Backup MRDB, and LRDB shall support the capability to provide remote, high bandwidth access to authorized craftsperson or administrator workstations. The DBAs shall be able to configure an authorization list in each MRDB, Backup MRDB, and LRDB, specifying the authorized craftsperson/DBA identities and the type of access or transactions allowed for each identity.

AUX-002470 [**Required: MRDB, Backup MRDB, and LRDB**] The MRDB, Backup MRDB, and LRDB shall support the capability to provide a visual GUI display for remote, high-bandwidth access to authorized craftsperson or administrator stations.

3.3.7 Hybrid Routing Requirements for Preventing PRI "Hairpin" Routes

This section provides requirements for SSs and DSN multifunction switches (MFSs) to support HR calls over T1.619A PRI interfaces. The requirements apply to SSs, SS MGs, and MFSs.

The goal of these requirements is to prevent PRI "hairpinning" of HR calls, when those calls are routed from the MFS to the SS MG (so that the SS can query the RTS Routing Database on those calls), and then routed back from the SS MG back to the MFS again for call completion. The reason that the SS returns the call to the MFS is one of the following:

- The Routing Database responds to the SS's HR query for the DSN number and indicates "Number Not Found."
- The Database responds to the SS's HR query for the DSN number, and indicates "Number Found," but provides no SC CCA-ID or SS CCA-ID values.

A routing "hairpin" would occur if the MFS routed the call to the SS MG on one ISDN PRI B-Channel, and the SS MG then routed the call back to the MFS on another ISDN PRI B-Channel. This would tie up two PRI B-Channels for the duration of each HR call that was originated on the TDM DSN, routed to an SS for access to the Routing Database, and then returned to the MFS for completion to a destination EO, Small End Office (SMEO), or PBX.

Since the goal is to not to tie up any PRI B-Channels for the duration of each TDM-originated-and-TDM-terminated HR call, a feature is needed that eliminates these routing "hairpins" on the

T1.619A PRI between the SS MG and the MFS. This section provides requirements for two features that eliminate these routing hairpins:

- ISDN PRI Two B-Channel Transfer (TBCT).
- DSN HR.

Both of these features are existing MFS PRI features (or enhancements to existing MFS PRI features) that are available on DISA MFSs today.

SSs and their MGs are required to support both of these features so that they will be interoperable with the various MFSs in the DISA TDM network today for HR calls. The MFSs are required to support at least one of these features, so that they support at least one mechanism for eliminating PRI routing hairpins on MFS-to-SS-to-MFS HR calls.

AUX-002480 [**Required: SS MG, MFS**] The short marking in this section is an abbreviated version of this longer marking: [**Required: SS, SS MG, MFS**]. The longer marking means that the requirement is applicable to the SS, the SS MG, and the MFS.

AUX-002490 [**Required: SS MG, MFS**] These network appliances shall not perform any T1.619A PRI routing hairpins on HR calls that are originated on the DISA TDM network, processed by the SS using the RTS Routing Database, and then terminated on the DISA TDM network. These network appliances shall use "routing hairpin elimination" features to prevent these routing hairpins from occurring on these HR calls.

AUX-002500 [**Required: SS MG**] The SS and its MG shall support both of the following "routing hairpin elimination" features on its T1.619A PRIs (the PRIs between the MG and the MFS):

- ISDN PRI TBCT (per the SS requirements in Section 3.3.7.1, SS and MFS Requirements for TBCT).
- DSN HR (per the SS requirements in Section 3.3.7.2, SS and MFS Requirements for DSN HR).

AUX-002510 [**Required: SS MG**] The SS and its MG shall support these features on both Routine and Precedence calls. The SS and its MG shall also allow these Routing and Precedence calls to be pre-empted by the PRI multilevel precedence and preemption (MLPP) feature when these "routing hairpin elimination" features are in use on these calls.

AUX-002520 [**Required: MFS**] The MFS shall support at least one of the following "routing hairpin elimination" features on its T1.619A PRIs (the PRIs between the MFS and the SS MG):

- ISDN PRI TBCT (per the MFS requirements in Section 3.3.7.1, SS and MFS Requirements for TBCT).
- DSN HR (per the MFS requirements in Section 3.3.7.2, SS and MFS Requirements for DSN HR).

AUX-002530 [**Required: MFS**] The MFS shall support these features on both Routine and Precedence calls. The MFS shall also allow these Routing and Precedence calls to be pre-empted by the PRI MLPP feature when these "routing hairpin elimination" features are in use on these calls.

AUX-002540 [**Required: MFS**] Any preexisting MFS restrictions that prevent the PRI TBCT feature from being used with Precedence calls or the PRI MLPP feature shall be removed for HR calls so that the aforementioned requirements can be met.

3.3.7.1 SS and MFS Requirements for TBCT

3.3.7.1.1 SS Requirements for TBCT

AUX-002550 [**Required: SS MG**] The SS and its MG shall support the ISDN PRI TBCT feature, per the following Telcordia requirements document:

- GR-2865-CORE, Generic Requirements for ISDN PRI Two B-Channel Transfer, Issue 3, March 2000.

AUX-002560 [**Required: SS MG**] The SS and its MG shall support these requirements for both Routine and Precedence calls. The SS and its MG shall also allow these Routine and Precedence calls to be pre-empted by the PRI MLPP feature when the TBCT feature is in use on these calls.

AUX-002570 [**Required: SS MG**] The SS and its MG shall also support these requirements on the DISA T1.619A PRI, even though the requirements were originally written for commercial U.S. National ISDN PRIs.

AUX-002580 [**Required: SS MG**] GR-2865-CORE describes TBCT operation on two sides on the ISDN PRI: the "network side" (the "Stored Program Control Switch [SPCS]") and the "user-side" (the "TBCT controller"). The SS and its MG shall follow the GR-2865-CORE requirements for the "user-side" of the PRI TBCT feature (the MFS operates as the "network-side").

AUX-002590 [**Required: SS MG**] The SS and its MG shall also support the "user-side" TBCT requirements for the "TBCT controller" in the following Telcordia document:

- SR-4994, 2000 Version of National ISDN Primary Rate Interface (PRI) Customer Premises Equipment Generic Guidelines, Issue 1, December 1999:
  - Section 11.5, PRI Two B-Channel Transfer.

The SR-4994, Section 11.5 "user-side" TBCT requirements are more specific than the GR-2865-CORE "user-side" TBCT requirements.

3.3.7.1.2 MFS Requirements for TBCT

The requirements in this section are Conditional for the MFS. If the MFS supports the ISDN PRI TBCT feature as a mechanism for eliminating PRI routing hairpins, then the following requirements apply.

AUX-002600 [**Conditional: MFS**] The MFS shall support the ISDN PRI TBCT feature, per Telcordia GR-2865-CORE.

AUX-002610 [**Conditional: MFS**] The MFS shall support these requirements for both Routine and Precedence calls. The MFS shall also allow these Routine and Precedence calls to be pre-empted by the PRI MLPP feature when the TBCT feature is in use on these calls.

AUX-002620 [**Conditional: MFS**] The MFS shall also support these requirements on the DISA T1.619A PRI, even though the requirements were originally written for commercial U.S. National ISDN PRIs.

AUX-002630 [**Conditional: MFS**] GR-2865-CORE describes TBCT operation on two sides on the ISDN PRI: the "network side" and the "user side." The MFS shall follow the requirements for the "network-side" of the PRI TBCT feature (the SS and its MG operate as the "user-side").

3.3.7.1.3 SS and MFS HR Call Flow Using TBCT

The following requirements apply when PRI TBCT is used between the SS (and its MG) and the MFS to prevent routing hairpins. The MFS is assumed to support the ISDN PRI TBCT feature in this case.

AUX-002640 [**Required: SS MG, MFS**] The SS, the SS MG, and the MFS shall support the entire following call flow for completion of HR calls and hairpin prevention using PRI TBCT. The call flow consists of both the following figures and the numbered steps that follow the figures. Figure 3.3-4 and Figure 3.3-5 show the first part of the SS and MFS HR call flow using TBCT.

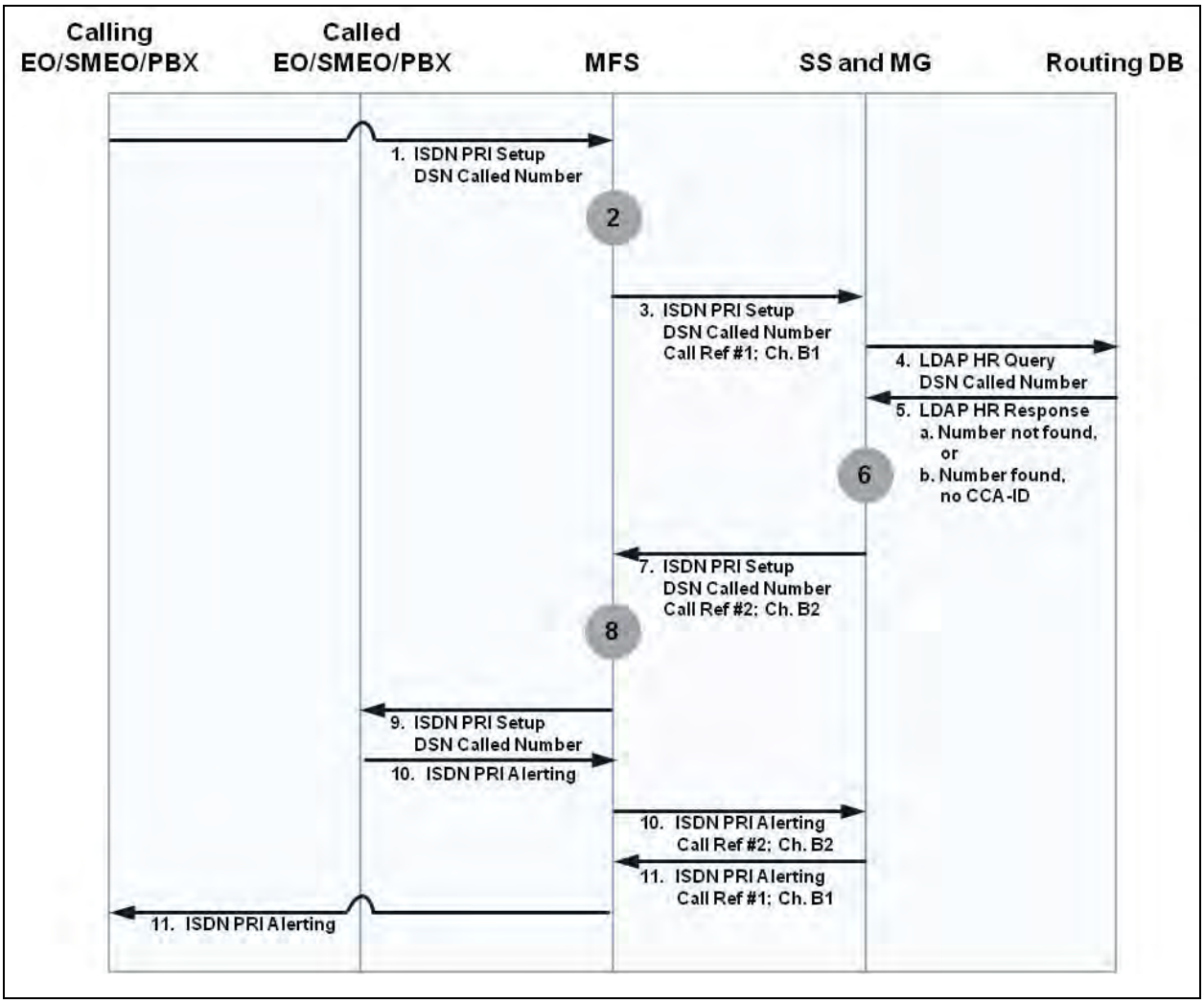


Figure 3.3-4. SS and MFS HR Call Flow Using TBCT – Part 1

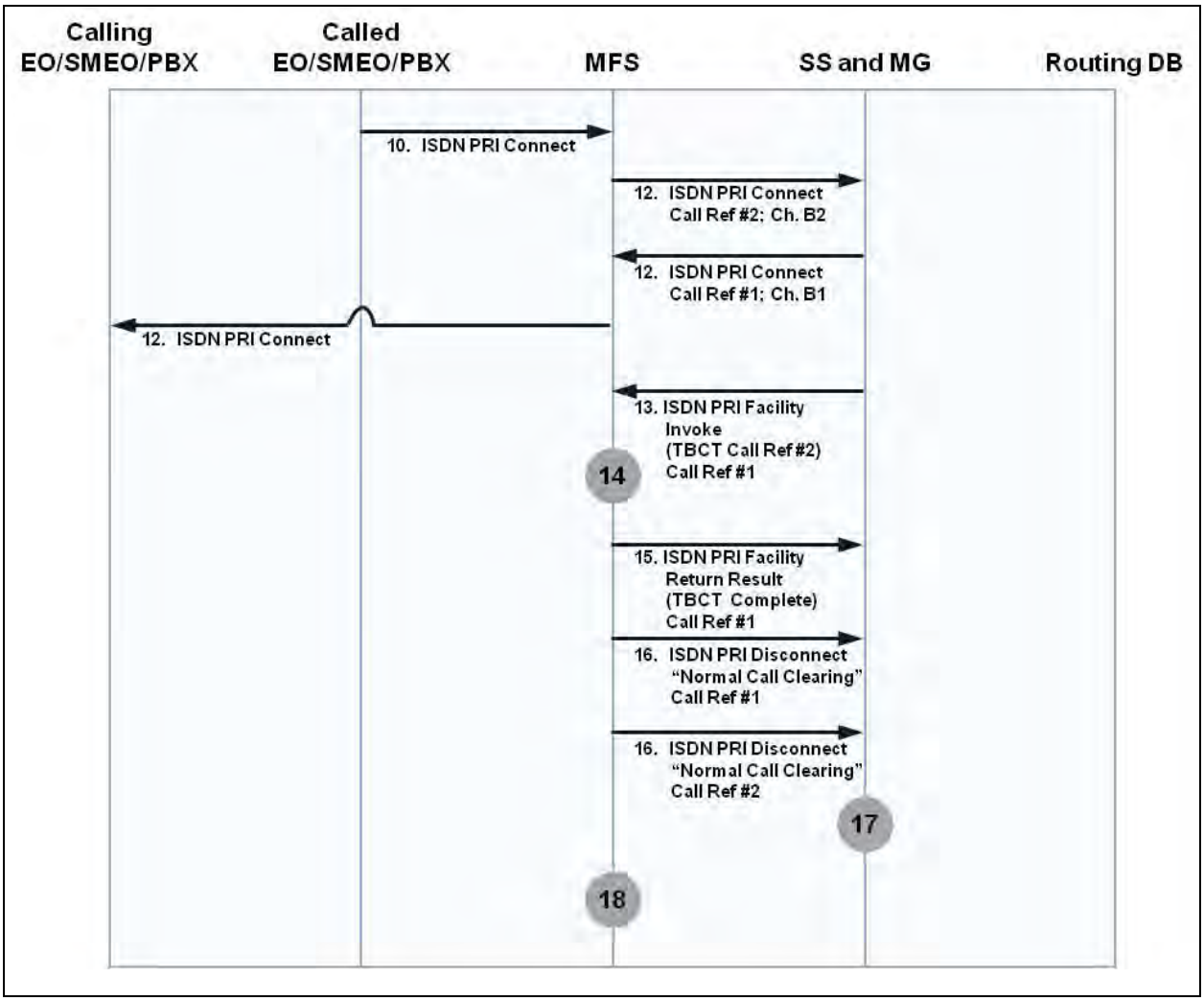


Figure 3.3-5. SS and MFS HR Call Flow Using TBCT – Part 2

1. The MFS receives an incoming call to a DSN number from a calling party on a line-side interface or a trunk-side interface that is different from the T1.619A PRI trunk group that connects the MFS and the SS MG.
2. The MFS checks its routing tables for the called DSN number, for the case in which the call arrived on a line-side interface or a trunk-side interface that is different from the T1.619A PRI connecting the MFS and the SS MG. The MFS then determines that the outgoing route for that number is the T1.619A PRI trunk group that connects the MFS and the SS MG.
3. The MFS routes the call request to the SS MG using this T1.619A PRI trunk group. This "first leg" of the call request is established using an ISDN SETUP message and uses one ISDN B-Channel and one ISDN call reference on that T1.619A PRI.
4. The SS MG accepts this call request from the MFS and directs the call request to the SS for further routing. The SS inspects the called number value and determines that an HR query to

the RTS Routing Database is required. The SS performs this HR query per the requirements in Section 3.3.2, SS to LRDB Interface: Database Queries for HR.

5. The RTS Routing Database responds to the HR query with one of the following two results:
   a. Number not found.
   b. Number found, but no SC CCA-ID or SS CCA-ID is available.
6. In both cases, the SS determines that the HR call needs to be returned to the SS MG, T1.619A PRI, and MFS for call completion, since the Database response indicated that the called number was not served by an SC on the UC network. The SS then returns the call to the SS MG.
7. The SS MG routes the call request back to the MFS using the same T1.619A PRI trunk group on which the call entered the MG. This "second leg" of the call request is established using a second ISDN SETUP message and uses a second ISDN B-Channel and a second ISDN call reference on that T1.619A PRI.
8. At this point, the MFS receives an incoming call to the called DSN number from the T1.619A PRI trunk group that connects the MFS and the SS MG. From the MFS standpoint, this is a completely separate call request from the previous call request that it directed to the SS MG, even though the two call requests have the same DSN called number.

   The MFS then checks its routing tables for the called DSN number, for the case in which the call arrived on a trunk-side interface that is the T1.619A PRI connecting the MFS and the SS MG.

   This means that the MFS must maintain two distinct outgoing routes for calls to the DSN called number: one for use when the call enters the MFS on a line-side interface or a trunk-side interface that is different from the MFS-to-SS-MG PRI, and another for use when the call enters the MFS on a trunk-side interface that is the MFS-to-SS-MG PRI.

   The MFS needs to maintain these two distinct outgoing routes independent of whether it supports PRI TBCT or DSN HR. The first outgoing route is used to route calls from the MFS toward the RTS Routing Database. The second outgoing route is used to route calls from the MFS to the destination EO, SMEO, or PBX in the DISA TDM network after the RTS Routing Database has processed the call.

   The second outgoing route is also used (and is needed) in the case in which an IP end user on an SC in the UC network calls the DSN number. The call is routed to the SS by AS-SIP trunks; the SS sends an HR query to the RTS Routing Database; the Database indicates "Number Not Found" (or "SC and SS CCA-ID" not found); the SS routes the call over to the DSN MFS for call completion; and the MFS routes the call to the destination EO, SMEO, or PBX. Note that there is no need to use either PRI TBCT or DSN HR in this case because the call originates on the UC network and completes on the DISA TDM network.

9. After checking its routing tables for the second call request to the DSN called number, the MFS determines that the outgoing route for that number is a route toward the destination EO, SMEO, or PBX on the DISA TDM network (which is different from the T1.619A PRI route back toward the SS MG). This destination EO, SMEO, or PBX may be directly accessible from the MFS, or it may be accessible from another MFS (or pair of MFSs) in the DISA TDM network. In the latter case, the MFS then has to route the second call request toward this destination via that other MFS in the network.
10. Once the second call request is routed to the destination EO, SMEO, or PBX, that EO/SMEO/PBX will return an ISDN ALERTING or PROGRESS message (indicating that the call is ringing), followed by an ISDN CONNECT message (indicating that the call is answered). The MFS providing TBCT receives these ISDN messages back from the destination EO, SMEO, or PBX, and then relays them to the SS MG using the second ISDN call reference on the T1.619A PRI between the MFS and the SS MG.
11. Once the SS MG receives an ISDN ALERTING or PROGRESS message from the MFS using the second ISDN Call reference, it relays that ISDN ALERTING or PROGRESS message back to the MFS using the first ISDN call reference. (The ISDN ALERTING message is analogous to the AS-SIP 180 Ringing response. The ISDN PROGRESS message is analogous to the AS-SIP 183 Session progress response.)
12. Once the SS MG receives an ISDN CONNECT message from the MFS using the second ISDN Call reference, it relays that ISDN CONNECT message back to the MFS using the first ISDN call reference. (The ISDN CONNECT message is analogous to the AS-SIP 200 OK response.)
13. Since the two PRI call legs are both "answered," the SS MG now requests TBCT by sending an ISDN FACILITY message to the MFS. This message contains a Facility Information Element that contains an Invoke component which contains the "TBCT" operation (the "enhancedExplicitEctExecute" operation), per GR-2865-CORE and SR-4994, Section 11.5.

    If the SS MG sends this FACILITY message using the first ISDN call reference, then the TBCT operation must contain a "link ID" parameter that contains the value of the second ISDN call reference.

    If the SS MG sends this FACILITY message using the second ISDN call reference, then the PRI TBCT operation must contain a "link ID" parameter that contains the value of the first ISDN call reference.

    (PRI TBCT requires at least one of the two call legs to be answered before the two call legs can be transferred together. For HR calls, it is simpler if both call legs are answered before the two call legs are transferred together, since an answer condition on one call leg immediately causes an answer condition on the other call leg.)
14. Upon receipt of the ISDN FACILITY message from the SS MG containing the "TBCT" operation, the MFS internally transfers the two call legs together. Specifically, the MFS

transfers the first call leg (established MFS-to-MG, using the first ISDN B-Channel and the first ISDN call reference) and the second call leg (established MG-to-MFS, using the second ISDN B-Channel and the second ISDN call reference) together, using an internal MFS transfer capability.

At this point, the signaling and media paths for the end-to-end call are completely within the DISA TDM network, and the two PRI call legs can be removed from the T1.619A PRI between the MFS and the SS MG.

15. The MFS returns a second ISDN FACILITY message to the SS MG containing a Facility Information Element containing a Return Result component. This Return Result component indicates the successful completion of the "TBCT" operation. The MFS sends this second ISDN FACILITY message to the SS MG using the same ISDN call reference on which the first MG-to-MFS ISDN FACILITY message was received.
16. The MFS then returns a first ISDN DISCONNECT message to the SS MG using the first ISDN call reference, and at the same time returns a second ISDN DISCONNECT message to the SS MG using the second ISDN call reference. Both ISDN DISCONNECT messages contain Cause Code #16, "Normal Call Clearing."

    If the MFS-to-MG DISCONNECT message sent on the first call reference is followed by the receipt of an MG-to-MFS DISCONNECT message on the same call reference, then the MFS has to be able to resolve the two competing DISCONNECT messages and still disconnect that call leg.

    If the MFS-to-MG DISCONNECT message sent on the second call reference is followed by the receipt of an MG-to-MFS DISCONNECT message on the same call reference, then the MFS has to be able to resolve the two competing DISCONNECT messages and still disconnect that call leg.
17. After receipt of the first ISDN DISCONNECT message from the MFS using the first ISDN call reference, the SS MG completes the disconnection of the MFS-to-MG call leg on its side of the T1.619A PRI.

    After receipt of the second ISDN DISCONNECT message from the MFS using the second ISDN call reference, the SS MG completes the disconnection of the MG-to-MFS call leg on its side of the T1.619A PRI.
18. Once the two call legs between the MFS and the SS MG have been disconnected, the SS and its MG are removed from the end-to-end answered call to the DSN called number. This end-to-end call is now completely within the DISA TDM network, and the signaling and media paths for that call are completely within the DISA TDM network.

3.3.7.2 SS and MFS Requirements for DSN HR

3.3.7.2.1 SS Requirements for DSN HR

AUX-002650 [**Required: SS MG**] The SS and its MG shall support the DSN HR feature. The details of DSN HR feature operation are in Section 3.3.7.2.3, SS and MFS HR Call Flow Using DSN HR.

The key differences between DSN HR and PRI TBCT are as follows:

- DSN HR uses a single ISDN call leg, single ISDN B-Channel, and single ISDN call reference between the SS MG and the MFS.
- DSN HR uses an ISDN DISCONNECT message with Cause Code #1, Unallocated (unassigned) number, in the SS-MG-to-MFS direction. There is no SS-MG-to-MFS SETUP message (establishing a second call leg) or SS-MG-to-MFS FACILITY message (transferring two call legs together) in this case.
- In DSN HR, MFS routing of the call request toward the destination EO, SMEO, or PBX is based on the receipt of the ISDN DISCONNECT message with Cause Code #1 from the SS MG, instead of receipt of a second ISDN SETUP message with the DSN called number from the SS MG.
- DSN HR requires that the MFS support an "Alternate Routing" capability, in which the primary MFS route for the DSN called number is the T1.619A PRI between the MFS and the SS MG, and the alternate MFS route for the DSN called number is the DISA TDM network route from that MFS to the destination EO, SMEO, or PBX.

Calls leave the MFS for the MG using the primary route and are "route advanced" to the alternate route (toward the destination EO/SMEO/PBX) upon receipt of the ISDN DISCONNECT message with Cause Code #1 from the MG. The "alternate route" may also be an ordered set of routes (secondary route, tertiary route, etc.) that lead to different TDM network paths from the "DSN HR" MFS toward the destination EO, SMEO, or PBX.

Alternate routes are typically used in cases in which the primary route is busy or out of order, and the call needs to be routed using an alternate route. In the DSN HR feature, alternate routes are also used when the call is offered to the primary route, and the primary route returns an indication that the call attempt has been rejected because the called number is unallocated/unassigned (ISDN DISCONNECT message, Cause Code #1).

- In DSN HR, the MFS-to-SS MG call leg is cleared by the ISDN DISCONNECT message that the SS MG sends to the MFS, using the single ISDN call reference on the single ISDN call leg. In PRI TBCT, the MFS is responsible for clearing both the ISDN call legs, using two separate MFS-to-MG ISDN DISCONNECT messages on two separate ISDN call references.

AUX-002660 [**Required: SS MG**] The SS and its MG shall support the DSN HR requirements for both Routine and Precedence calls. The SS and its MG shall also allow these Routine and

Precedence calls to be pre-empted by the PRI MLPP feature when the DSN HR feature is in use on these calls.

AUX-002670 [**Required: SS MG**] The SS and its MG shall support the DSN HR requirements on the DISA T1.619A PRI. The DSN HR feature is not applicable to commercial U.S. National ISDN PRIs.

3.3.7.2.2 MFS Requirements for DSN HR

The requirements in this section are all Conditional for the MFS. If the MFS supports the DSN HR feature as a mechanism for eliminating PRI routing hairpins, then the following requirements apply.

AUX-002680 [**Conditional: MFS**] The MFS shall support the DSN HR feature. The details of DSN HR feature operation are in Section 3.3.7.2.3, SS and MFS HR Call Flow Using DSN HR.

AUX-002690 [**Conditional: MFS**] The MFS shall support the DSN HR requirements for both Routine and Precedence calls. The MFS shall also allow these Routine and Precedence calls to be pre-empted by the PRI MLPP feature when the DSN HR feature is in use on these calls.

AUX-002700 [**Conditional: MFS**] The MFS shall support the DSN HR requirements on the DISA T1.619A PRI. The DSN HR feature is not applicable to commercial U.S. National ISDN PRIs.

3.3.7.2.3 SS and MFS HR Call Flow Using DSN HR

The following requirements apply when DSN HR is used between the SS (and its MG) and the MFS to prevent routing hairpins. The MFS is assumed to support the DSN HR feature in this case.

AUX-002710 [**Required: SS MG, MFS**] The SS, the SS MG, and the MFS shall support the entire following call flow for completion of HR calls and hairpin prevention using DSN HR. The call flow consists of both Figure 3.3-6 and the numbered steps that follow it.

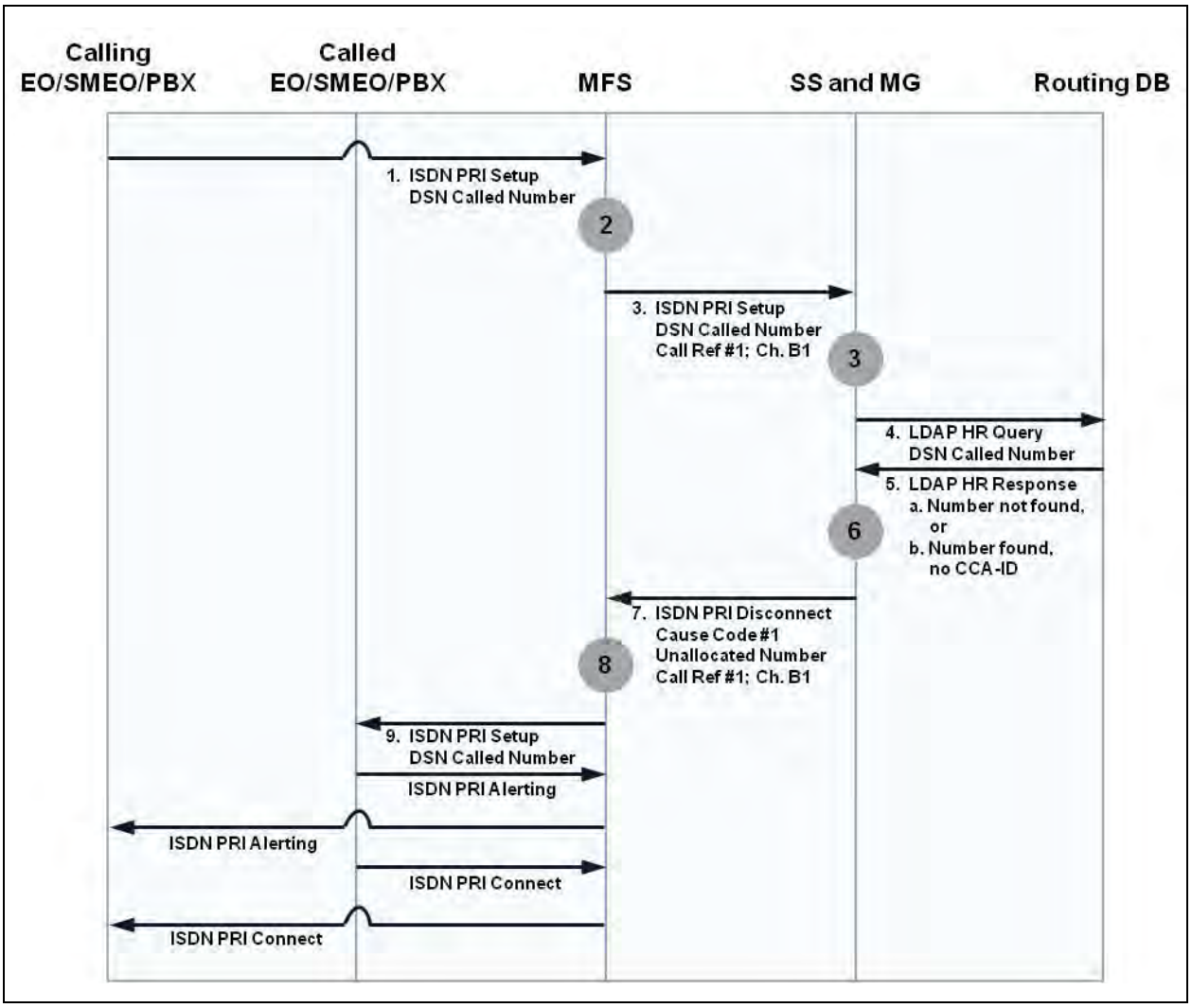


Figure 3.3-6. SS and MFS HR Call Flow Using DSN HR

Steps 1 through 6 in this call flow are identical to Steps 1 through 6 in the PRI TBCT call flow in Section 3.3.7.1.3, SS and MFS HR Call Flow using TBCT. The last three paragraphs from Step 8 in the TBCT call flow also apply.

1. The SS MG returns the call to the MFS by sending the MFS an ISDN DISCONNECT message containing Cause Code #1, unallocated (unassigned) number. The MG sends this ISDN DISCONNECT message on the SS-MG-to-MFS PRI, using the same ISDN call reference that the MFS used to send the previous ISDN SETUP message to the MG. The MG also disconnects from the MFS-to-MG call leg on its side of the T1.619A PRI.

   This ISDN DISCONNECT message removes the HR call request from the MFS-to-MG interface, and returns the call to the MFS for further routing. At this point, the SS and the SS MG are completely removed from the call request to the DSN called number.

2. Upon receipt of the ISDN DISCONNECT message with Cause Code #1, the MFS "DSN HR" feature uses the MFS "Alternate Routing" feature to route the call request toward the destination EO, SMEO, or PBX in the DISA TDM network.

   The "Alternate Routing" feature is set up so that the primary MFS route for the DSN called number is the T1.619A PRI between the MFS and the SS MG, and the alternate MFS route for the DSN called number is the TDM network route from that MFS toward the destination EO, SMEO, or PBX. The "alternate MFS route" may also be an ordered set of routes that represent different TDM network paths from the "DSN HR" MFS toward the destination EO, SMEO, or PBX.

   This destination EO, SMEO, or PBX may be directly accessible from the MFS, or it may be accessible from another MFS (or pair of MFSs) in the DISA TDM network. In the latter case, the MFS then has to route the call request toward this destination via the other MFS in the network.

   If the DSN HR feature was not used in the MFS, then the receipt of the ISDN DISCONNECT message with Cause Code #1 from the SS MG would result in rejection of the call request on the DISA TDM network, and the playback of a call denial announcement to the calling party (e.g., "Your call cannot be completed as dialed. Please check the number and try again."). The use of DSN HR in MFS allows call requests receiving these "DISCONNECT/Cause Code #1" treatments to be "route advanced" to other network routes using Alternate Routing, instead of being rejected and connected to a call denial announcement.

3. The MFS then routes the call request to the destination EO, SMEO, or PBX on the DISA TDM network. The call request is handled on the DISA TDM network from this point forward and may be answered, forwarded, diverted to an attendant, or rejected at the called party interface. The signaling and media paths for this call remain completely within the DISA TDM network, because the SS MG removed the UC network from the call request when it returned the ISDN DISCONNECT message to the MFS.

3.4 UC AUDIO AND VIDEO CONFERENCE SYSTEM

UC Conference System (UCCS) requirements in this section that are marked "AO" apply to systems that support conferences for only audio end instruments (i.e., voice phones). Requirements that are marked "VO" apply to systems that support conferences only for video end instruments (i.e., video terminals). Requirements for systems that support conferences for both audio and video end instruments are marked "A/V." Requirements that apply to all types of conference systems are marked "All UCCS."

NOTE: An audio/visual (A/V) conference system can be implemented as an integrated audio and video product, or as a combination of an audio conference system and a video conference system.

3.4.1 Introduction

This section addresses required functionality, performance, capabilities, and associated technical parameters for the UC audio and video conference system components of the DISN VoIP and Video over IP services. This section's focus is real-time conferencing functions and features that meet the operational needs of the Warfighter and the Government. The concept for including conference systems into the UC DISN voice and video assured services framework is depicted in Figure 3.4-1, UC Conference System Framework.

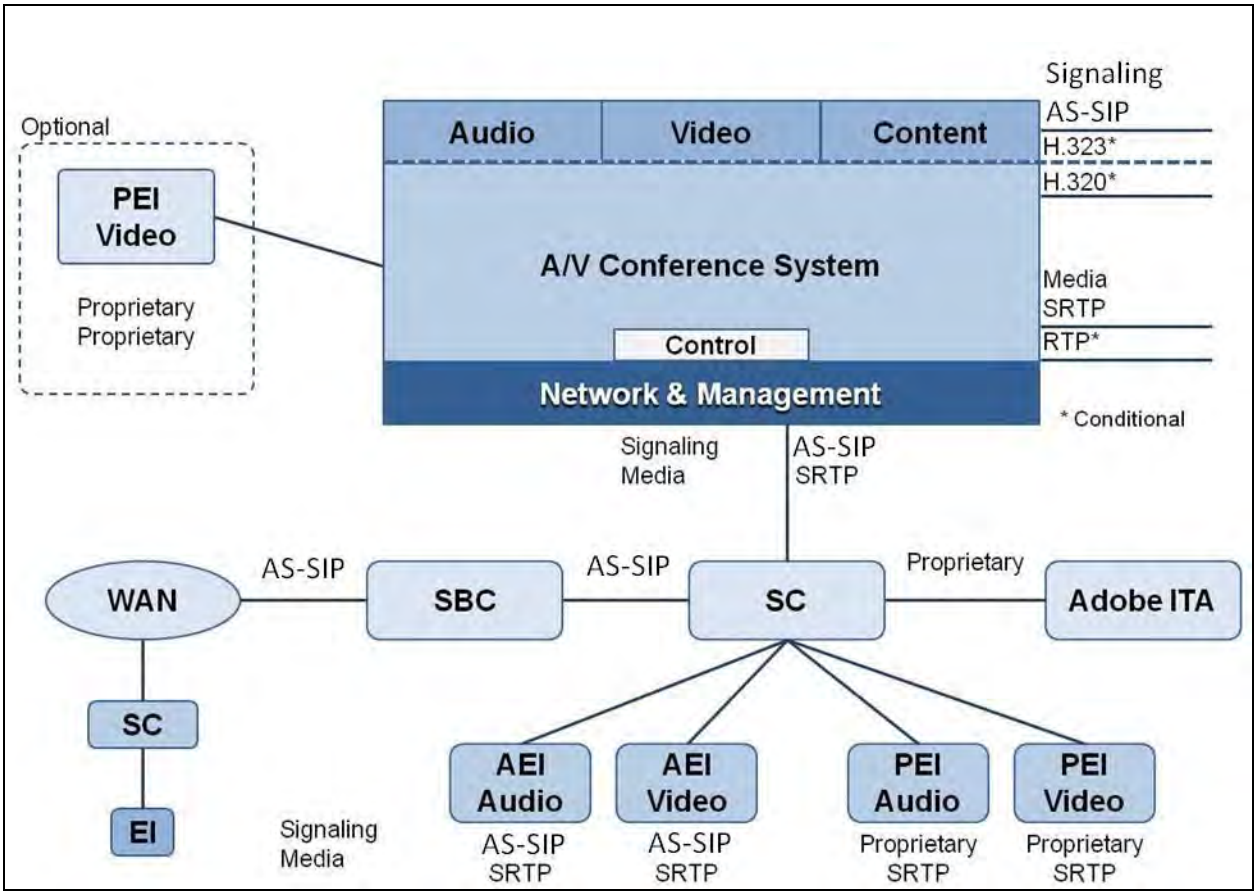


Figure 3.4-1. UC Conference System Framework

The conference system can be viewed as a peripheral device to the SC. At the vendor's option, it can be implemented as a standalone appliance; i.e., as its own System Under Test (SUT) or as an integrated part of the SC SUT. The primary difference between the two options is that a proprietary interface may be used when the network interface component is an integral part of the SC in the same SUT. When implemented as a standalone SUT, AS-SIP will be the required interface between the conference system and the SC. When made part of an existing APL SC, the SC will require a new APL certification. The acquisition agent working with the vendors will decide whether to acquire the conference system's network interface as a standalone appliance or as part of an SC. There are no hardware packaging requirements or restrictions on how the vendor chooses to implement the UCCS. A standalone audio conference system can be deployed,

a standalone video conference system can be deployed, an audio conference system product can be combined with a separate video conference system product, or an integrated audio/video product can be deployed. H.320 and H.323 gateway devices may be used, but are not required.

Note that Proprietary Video EIs (Proprietary Signaling, Proprietary Media/codecs) can be supported on the "line side" of Video Conference System in cases where the Proprietary Video EI and the Video Conference System are from the same vendor. It is assumed that these Proprietary Video EIs are connected directly to the Video Conference System over IP in this case, and that there is no SC in the signaling path between the Video EI and the Video Conference System. The Video Conference System can provide "normalization" from the proprietary protocol on the EI side to AS-SIP on the SC side, in this case.

Proprietary Video EIs and Video Conference Systems can also communicate through an SC using proprietary protocols, if the Video EI, Video Conference System, and SC all support the same proprietary protocol.

Proprietary Video EIs and Video Conference Systems can also communicate with each other through a set of SCs and SSs, but the SCs must provide "normalization" from the proprietary protocol to AS-SIP, in this case.

3.4.2 System Description

3.4.2.1 Overall System Description

The UCCS is intended to provide global real-time audio and video conferencing service capabilities for the DoD. Services include non-secure audio add on, video recording, archive and retrieval, bandwidth management, and seamless connectivity of users and resources. Furthermore, the conference system shall provide reservation and reservationless based scheduling conferencing management capabilities.

3.4.2.2 System Architecture

AUX-002720 [**Required: All UCCS**] The conference system shall provide, as a minimum, an Ethernet-based interface to the network.

3.4.2.3 Information Assurance

AUX-002730 [**Required: All UCCS**] The conference system shall meet the Information Assurance requirements of all applicable DISA Security Technical Implementation Guidelines (STIGs).

Section 3.4.5.1.6, Security Management, contains conference system security management requirements.

3.4.3 Service

This section describes the service requirements of the conference system.

3.4.3.1 Service Description

This subsection describes the service requirements for the conference system. The system provides a range of conferencing services that allow two or more locations to communicate by means of audio and/or video.

3.4.3.1.1 Registration

AUX-002740 [**Required: All UCCS**] All subscriber EIs and devices directly utilizing the conferencing system shall be required to register with the system in order to use conferencing services.

This registration requirement is not meant to exclude non-registered EIs and external parties from participating in a conference to which they have been invited by the registered subscriber that scheduled the conference.

Section 3.4.5.3, Registration System, contains conference services registration system requirements.

3.4.3.1.2 Point-to-Point Conferencing

AUX-002750 [**Required: All UCCS**] The conference system shall provide IP-based point-to-point conferencing. Point-to-point conferencing consists of two participants with fully interactive audio and/or video capabilities. The system shall support EIs that are registered with the system to initiate point-to-point, fully interactive audio and video capability communications. This capability shall be supported through conferencing services that enable the resolution of resource conflicts by calendaring and scheduling system application programming interfaces (APIs) with enterprise scheduling systems. It is desired that the UCCS shall provide real-time conferencing status capability; e.g., busy, online, offline.

AUX-002760 [**Required: All UCCS**] The conference system shall support IP-based solutions using AS-SIP, [**Optional**] H.323, and [**Optional**] dial-up ISDN H.320 endpoint support.

AUX-002770 [**Required: All UCCS**] The conference system shall support interactive conferences using IP and [**Optional**] ISDN transport. These conferences shall consist of Proprietary and AS-SIP EIs only, [**Optional**] H.323 EIs only, [**Optional**] H.320 EIs only, or [**Optional**] a combination of H.323 EIs, Proprietary and AS-SIP EIs, and H.320 EIs.

NOTE: ISDN transport applies only to conferences involving non-IP EIs.

3.4.3.1.3 Multipoint Conferencing

AUX-002780 [**Required: All UCCS**] The conference system shall provide multipoint conferencing. A multipoint conference consists of three or more EIs in a conference call and shall include the following functions and features.

AUX-002790 [**Required: All UCCS**] The conference system shall distribute fully interactive video and/or audio streams among multiple participants according to the channel bandwidth of each participant.

AUX-002800 [**Required: VO CS, A/V CS**] The conference system shall accommodate users on the same conference at different video rates, resolutions, and frame rates according to EI capability and not at the lowest common denominator level.

AUX-002810 [**Required: All UCCS**] The conference system shall provide interactive, multipoint conferences using IP transport and [**Optional**] ISDN transport. These conferences shall consist of Proprietary and AS-SIP EIs only, [**Optional**] H.323 EIs only, [**Optional**] H.320 EIs only, or [**Optional**] a combination of H.323 EIs Proprietary and AS-SIP EIs, and H.320 EIs.

NOTE: ISDN transport applies only to conferences involving non-IP EIs.

3.4.3.1.4 Video Performance

This section describes the criteria and metrics required to ensure audio/video quality during multi-party conferences as well as point-to-point calls.

For planning purposes, the conference system should be designed in accordance with the following guidelines.

Bit Error Rate. It is essential for the system to control bit error rate at the lowest possible level.

Packet Loss. The end-to-end network design guideline for packet loss percentage is less than 1 percent and may include the use of packet loss concealment.

NOTE: The 1 percent packet loss design guideline is also supported by industry standard document Telecommunications Industry Alliance (TIA)/Electronic Industries Alliance (EIA)/TSB116.

Latency. International Telecommunications Union – Telecommunication (ITU-T) Recommendation G.114 recommends that no more than 50 milliseconds be allocated for each of the national and international segments of network transmission. In the international case, there is one originating and one terminating national segment, as well as one international segment resulting in the end-to-end one-way delay limit of 150 milliseconds. In the domestic case, there is one originating and one terminating national segment, resulting in the end-to-end one-way delay limit of 100 milliseconds for domestic connections.

The end-to-end one-way delay guideline is as follows:

- Less than 150 milliseconds for international connections.
- Less than 100 milliseconds for domestic connections.

Jitter. Jitter buffers that temporarily store arriving packets in order to minimize delay variations shall be employed.

3.4.3.1.5 In-Conference Control

AUX-002820 [**Required: All UCCS**] The conference system shall provide in-conference control. In-conference control shall include the following functions and features.

AUX-002830 [**Required: VO CS, A/V CS**] The conference system shall provide a banner for each conference.

AUX-002840 [**Required: All UCCS**] The conference system shall provide notification of participants joining and leaving a conference, and provide an end-of-conference warning to all participants.

AUX-002850 [**Required: All UCCS**] The conference system shall provide the ability to extend conferences, without disruption, to conferences in progress.

AUX-002860 [**Required: VO CS, A/V CS**] The conference system shall support presentation capability for different screen layouts locally, manageable by each individual host.

AUX-002870 The conference system shall provide the following conferencing chair control functionality:

AUX-002870.a [**Required: VO CS, A/V CS**] Voice-activated switching.

AUX-002870.b [**Required: All UCCS**] Broadcast mode.

AUX-002870.c [**Required: All UCCS**] Lecture mode.

AUX-002870.d [**Required: VO CS, A/V CS**] Video switching with H.243 control.

AUX-002870.e [**Required: VO CS, A/V CS**] Continuous presence.

AUX-002870.f [**Required: All UCCS**] Add/Delete, Accept/Reject, Connect/Disconnect, Mute/Unmute, audio/video.

3.4.3.1.6 Transcoding

Transcoding converts audio and video media streams, allowing conference participants to communicate with each other even though their EIs are equipped with different encoding/decoding capabilities.

AUX-002880 [**Required: VO CS, A/V CS**] The conference system shall provide transcoding availability regardless of the data speeds; the number of concurrent video calls; and the number

of concurrent conferences, video sizes, frame rates, and conference modes (voice switching or continuous presence) without downgrading the conference to a lowest common denominator protocol.

AUX-002890 [**Required: VO CS, A/V CS**] The conference system shall provide automatic video transcoding without downgrading the conference to a lowest common denominator protocol.

AUX-002900 [**Required: AO CS, A/V CS**] The conference system shall provide automatic audio transcoding without downgrading the conference to a lowest common denominator protocol.

3.4.3.1.7 Variable Data Rates

AUX-002910 [**Required: VO CS, A/V CS**] The conference system shall provide support for variable data rates, the rate at which data (bits) is transmitted, usually expressed in bits per second (bps) per Conferencing Terminal Unit (CTU). The system shall support data rates of at least 64 kilobits per second (kbps) per CTU. The system shall provide speed matching and down speeding to facilitate adjustable data rates. The system shall provide bandwidth management of IP services in order to restrict the bandwidth used by active call connections to the bandwidth installed and available in the network access connections.

3.4.3.1.8 Audio Add-On

AUX-002920 [**Required: A/V CS**] The conference system shall provide audio add-on features for audio-only participants in video conferences and support an external VoIP audio conference connecting to the video conference session.

3.4.3.1.9 Interactive Graphics Exchange

AUX-002930 [**Optional: VO CS, A/V CS**] The UCCS shall provide content sharing capability for participants to interact during video teleconferencing (VTC) sessions that allow participants to view and display the same presentation material at the same time. The system shall provide a dedicated live video stream and a presentation video stream and still-frame graphics as specified in Section 3.4.3.3.1, Compression Algorithms and Audio/Video Protocols. The system shall provide Interactive Graphics Exchange with the following functions and features.

AUX-002940 [**Optional: VO CS, A/V CS**] The conference system shall provide a means to allow participants to interactively view images from external sources with all or any of the participants in the conference.

AUX-002950 [**Optional: VO CS, A/V CS**] The conference system shall provide real-time participation of any combination of EIs. The system shall provide still image exchange as specified in Section 3.4.3.3.1, Compression Algorithms and Audio/Video Protocols.

AUX-002960 [**Optional: VO CS, A/V CS**] Interactive graphics exchange capabilities shall include the following:

a. Point-to-point and multipoint conferencing services.

b. Interoperability with different vendor EIs and variable graphic resolutions.

c. Connections among participants using any video EIs, connection types, and at any rates.

3.4.3.1.10 Audio Conferencing

The conference system shall be able to support audio conferencing and provide the following functions and features.

AUX-002970 [**Required: A/V CS**] The system shall be capable of accepting audio-only participants into a conference call for both scheduled and ad hoc video conferences.

AUX-002980 [**Required: VO CS, A/V CS**] The system shall provide an interface to an external audio conferencing system to allow cascading between a multi-point VTC call with a multi-point audio call through the use of the interface to an external audio conferencing system.

AUX-002990 [**Required: AO CS, A/V CS**] The system shall provide internal conferencing capabilities for the support of audio-only participants.

3.4.3.2 Integrated Services

This subsection describes services that are to be integrated in a means that provides the customer a user-friendly presentation, request, and access.

3.4.3.2.1 Web Access to Conference System

AUX-003000 [**Required: All UCCS**] The conference system shall provide a Web-based portal for customer access to the UC conferencing services, features, and capabilities. As the conferencing services change, the Web-based portal shall reflect those changes. Additionally, the conferencing services Web portal shall provide the following:

AUX-003000.a [Required: All UCCS] An enterprise-wide service for the identification and other pertinent information about users, conferencing services, and resources, and makes it accessible from any place at any time.

AUX-003000.b [Required: All UCCS] Awareness of relevant, accurate information about the conferencing service to users at all levels (strategic, operational, and Tactical).

AUX-003000.c [Required: All UCCS] An integrated scheduling system that provides users the ability to schedule one or a combination of video and audio conference services in one Web interface.

3.4.3.2.2 Recorded Content Retrieval and Management

The following subsections describe the Video and Audio Conferencing Recorded Content Retrieval and Management services to be provided by the system.

3.4.3.2.2.1 Video Conferencing Recorded Content Retrieval

AUX-003010 [**Optional: VO CS, A/V CS**] The conference system shall provide a video conferencing recorded content request and retrieval system in accordance with (IAW) the following requirements.

AUX-003020 [**Optional: VO CS, A/V CS**] The system shall provide the user the ability to view and listen to the recorded video conferences using a Web browser to retrieve streaming video.

AUX-003030 [**Optional: VO CS, A/V CS**] The system shall provide a Web-based system for the meeting moderator to access the recorded video conference call.

AUX-003040 [**Optional: VO CS, A/V CS**] The system shall inform the meeting moderator of the recorded video conference access information immediately after the completion of the video conference.

AUX-003050 [**Optional: VO CS, A/V CS**] The system shall provide Web-based interfaces for users to search recorded content based on the combination of the following information: meeting topic, meeting date/time, keywords provided by meeting moderators, meeting leader name, meeting language, and meeting leader organization.

AUX-003060 [**Optional: VO CS, A/V CS**] The Web interface shall provide a link to the content retrieval launch page.

AUX-003070 [**Optional: VO CS, A/V CS**] The content retrieval launch page shall authenticate the users using PKI and prompt users to enter passwords defined by the meeting moderators during the meeting scheduling phase.

AUX-003080 [**Optional: VO CS, A/V CS**] The content retrieval launch page shall maintain a record of every content request. The record of each request shall include the name, email address, and E.164 number or IP address of the requester; the identification of the recording; and the date and time of the request.

AUX-003090 [**Optional: VO CS, A/V CS**] The content retrieval launch page shall allow users to choose which format of the supported streaming media formats to use when playing back the retrieved content.

AUX-003100 [**Optional: VO CS, A/V CS**] The system shall provide the end user controls during streaming to pause/resume and select segments to play.

AUX-003110 [**Optional: VO CS, A/V CS**] The content retrieval launch page shall allow users to download the stored content of a conference meeting, if this option is permitted by the meeting's moderator.

AUX-003120 [**Optional: VO CS, A/V CS**] The streaming shall comply with the Streaming Service Protocol Requirements described in Section 3.4.3.3.1, Compression Algorithms and Audio/Video Protocols.

AUX-003130 [**Optional: VO CS, A/V CS**] The system shall ensure the compatibility of stored content with the latest versions of media player clients.

3.4.3.2.2.2 Audio Conferencing Recorded Content Management

AUX-003140 [**Optional: AO CS, A/V CS**] The conference system shall provide a content management system IAW the following requirements.

AUX-003150 [**Optional: AO CS, A/V CS**] The content management system shall comply with DoD 5200.1R with clear marking and labeling.

AUX-003160 [**Optional: AO CS, A/V CS**] The content management system shall maintain recorded audio conferencing content ready for users to retrieve anytime for a period of 30 days after the completion of the conferences.

AUX-003170 [**Optional: AO CS, A/V CS**] The content management system shall archive recorded audio conferencing content into permanent storage after 30 days.

AUX-003180 [**Optional: AO CS, A/V CS**] The content management system shall allow users to request stored content from archive. The wait time to retrieve archived material shall be less than one working day.

AUX-003190 [**Optional: AO CS, A/V CS**] The archive material shall be kept at the same fidelity levels of the original recordings. Compression techniques that cause a loss of fidelity are not acceptable encoding schemes for archive material.

3.4.3.3 Interoperability

AUX-003200 [**Required: All UCCS**] This subsection describes the system's interoperability requirements. The system shall maximize the use of standards-based interfaces. The system shall use functions, protocols, and formats that are publicly available.

AUX-003210 [**Optional: VO CS, A/V CS**] For video equipment, the conference system shall adhere to Federal Telecommunications Recommendation 1080B-2002 (FTR-1080B).

3.4.3.3.1 Compression Algorithms and Audio/Video Protocols

AUX-003220 [**Required: VO CS, A/V CS**] The conference system shall support the following audio and video standards for video conferencing:

AUDIO PROTOCOLS	VIDEO PROTOCOLS
G.711	H.263-200
G.722	H.264
G.722.1	
G.723.1	
G.728	
G.729/G.729A	

AUX-003230 [Optional: VO CS, A/V CS] The conference system shall support the following video standards for video conferencing:

VIDEO PROTOCOLS
H.261
H.264 (SVC)

AUX-003240 [**Required: AO CS, A/V CS**] The conference system shall support the following audio standards for audio-only conferencing:

AUDIO PROTOCOLS
G.711
G.722
G.722.1
G.723.1
G.728
G.729/G.729A

AUX-003250 [**Required: All UCCS**] The conference system shall provide interoperability for all end point devices that support AS-SIP during call setup.

AUX-003260 [**Optional: All UCCS**] The conference system shall provide interoperability for all end point devices that support H.320 during call setup.

AUX-003270 [**Optional: All UCCS**] The conference system shall provide interoperability for all end point devices that support H.323 during call setup.

AUX-003280 The conference system, including any proprietary Video EIs, shall support the following:

AUX-003280.a [**Required: VO CS, A/V CS**] Sub-Quarter Common Intermediate Format (SQCIF).

AUX-003280.b [**Required: VO CS, A/V CS**] Quarter Common Intermediate Format (QCIF).

AUX-003280.c [**Required: VO CS, A/V CS**] Common Intermediate Format (FCIF, also called CIF).

AUX-003280.d [**Required: VO CS, A/V CS**] 4 Full Common Intermediate Format (4FCIF, also called 4CIF).

AUX-003280.e [**Optional: VO CS, A/V CS**] 16 Full Common Intermediate Format (16FCIF, also called16 Common Intermediate Format (16CIF)).

AUX-003280.f [**Optional: VO CS, A/V CS**] SD and HD video resolution formats for H.261, H.263, and H.264 codecs.

VIDEO FORMAT STANDARDS	VIDEO RESOLUTION
SQCIF	128 x 96
QCIF	176 x 144
SIF(525)	352 x 240
CIF/SIF(625)	352 x 288
4SIF(525)	704 x 480
4CIF/4SIF(625)	704 x 526
16CIF	1408 x 1152
DCIF	528 x 384
SD	720 x 480
HD(720p)	1280 x 720
HD (1080p)	1920 x 1080

AUX-003290 [**Required: VO CS, A/V CS**] The conference system shall ensure that the freeze-frame image feature is compliant with ITU-T H.239 and with H.261 Annex D.

AUX-003300 [**Required: VO CS, A/V CS**] The system's freeze-frame image size shall support 4FCIF (4CIF), VGA, SVGA, XGA, and WSXGA+ when using H.239.

AUX-003310 [**Optional: VO CS, A/V CS**] The system's freeze-frame image size shall support HD (720p) and HD (1080p) when using H.239.

AUX-003320 [**Required: VO CS, A/V CS**] The system's freeze-frame image size shall support 4FCIF (4CIF) when using H.261 Annex D.

3.4.3.3.2 H.320 and H.323 Protocols

AUX-003330 The conference system that supports H.323/H.320 protocols shall meet the following ISDN/PRI, H.323 V4, chair control, serial interfaces, content sharing VTC endpoint protocol requirements:

AUX-003330.a [**Optional: VO CS, A/V CS**] ISDN PRI on ISDN interfaces (including Alcatel-Lucent 5ESS PRI, GENBAND DMS PRI, and National ISDN PRI).

AUX-003330.b [**Optional: VO CS, A/V CS**] European E1 ISDN standards.

AUX-003330.c [**Optional: VO CS, A/V CS**] ISDN bonding up to 1.5 Mbps on T1 and 2 Mbps on E1 per International Organization for Standardization (ISO) 13871.

AUX-003330.d [**Optional: VO CS, A/V CS**] H.323/320 V4.

AUX-003330.e [**Optional: VO CS, A/V CS**] Far end camera control (FECC) H.281 and H.323 Annex Q.

AUX-003330.f [**Optional: VO CS, A/V CS**] Resource Availability Indicator (RAI)/Resource Availability Confirmation (RAC) for load balancing.

AUX-003330.g [**Optional: VO CS, A/V CS**] Chair control messages per H.246, H.242/H.243.

AUX-003330.h [**Optional: VO CS, A/V CS**] Direct, H.225 routed, and H.225-H.245 routed modes of H.323 gatekeeper operations.

AUX-003330.i [**Optional: VO CS, A/V CS**] Quality of Service (QoS) support using DSCP marking of IP packets.

AUX-003330.j [**Optional: VO CS, A/V CS**] Automatic downspeed to available ISDN/IP bandwidth.

AUX-003330.k [**Optional: VO CS, A/V CS**] Automatic rate detection to match incoming video calls.

AUX-003330.l [**Optional: VO CS, A/V CS**] V.35/RS-449/EIA-530 Data Terminating Equipment (DTE) and Data Circuit-Terminating Equipment (DCE) interfaces (The implementation shall use EIA-530 interfaces, and the use of V.35 and RS-449 interfaces shall be phased out where multiple interfaces are supported in equipment. RS-366 interfaces shall also be supported for dial signaling bypass devices).

AUX-003330.m [**Optional: VO CS, A/V CS**] H.239 for additional video channels or still images.

3.4.3.3.3 AS-SIP

The system shall ensure that all conferencing equipment meets the following protocol requirements:

AUX-003340 [**Required: All UCCS**] The AS-SIP audio and video signaling conferencing requirements are specified in AS-SIP Section 10, Audio and Video Conference Services.

AUX-003350 [**Optional: VO CS, A/V CS**] FECC H.281 and H.323 Annex Q.

AUX-003360 [**Optional: VO CS, A/V CS**] Chair control messages per H.246, H.242/H.243.

AUX-003370 [**Required: All UCCS**] QoS support using DSCP marking of IP packets.

AUX-003380 [**Required: VO CS, A/V CS**] Automatic downspeed to available IP bandwidth.

AUX-003390 [**Required: VO CS, A/V CS**] Automatic rate detection to match incoming video calls.

AUX-003400 [**Optional: All UCCS**] Support T.140 for text messages.

AUX-003410 [**Optional: VO CS, A/V CS**] H.261 Annex D for still images.

3.4.3.3.4 Video Mixing Modes

The conference system shall ensure that all video mixing modes meet the following standards.

AUX-003420 [**Required: VO CS, A/V CS**] Video Switching Mode. The system shall ensure that the system supports video switching according to H.243 and H.323. The design shall minimize the time to switch and the disruption of video when switching from one video source to another.

AUX-003430 [**Required: VO CS, A/V CS**] Video Mixing (Picture Composition or Continuous Presence Mode). The system shall ensure that the system supports video mixing functions according to H.243 and H.323. The system shall support enhanced continuous presence multiple video mixing to include the 7 plus 1 format.

3.4.3.3.5 In-Conference Chair Control

The conference system shall ensure that the system supports chair control standards as defined in H.230, H.246, H.242, H.243 and H.245, including standards supporting Broadcast and Lecture mode capabilities. The following shall be supported:

AUX-003440 [**Optional: VO CS, A/V CS**] H.320 chair control messages and procedures as defined in H.230, H.242, H.243 and H.245.

AUX-003450 [**Optional: VO CS, A/V CS**] H.323 multipoint conferencing units (MCUs) shall support chair control messages and procedures as defined in H.323 and as carried forward to H.323 from H.243.

AUX-003460 [**Optional: VO CS, A/V CS**] H.323 – H.320 gateways shall follow the H.246 message translation tables related to chair control functions.

3.4.3.3.6 Audio Conferencing

The conference system shall ensure audio systems support the following requirements:

AUX-003470 [**Required: AO CS, A/V CS**] Audio systems shall support in-dial and out-dial IAW the DISN World Wide Numbering Plan and the PSTN North American dialing plans.

TDM requirements include the following:

AUX-003480 [**Optional: AO CS, A/V CS**] The audio system's PSTN interfaces shall support T1/E1 (AT&T TR62411 or Telcordia TR-NWT-000170).

AUX-003490 [**Optional: AO CS, A/V CS**] The audio system's CAS interfaces shall support Alcatel-Lucent 5ESS and GENBAND DMS switches.

AUX-003500 [**Optional: AO CS, A/V CS**] The audio system's T1 PRI interfaces shall support Non-Facility Associated Signaling (NFAS) and D-channel backup, if the audio system supports more than two PRIs.

AUX-003510 [**Optional: AO CS, A/V CS**] The audio system's T1 interface shall support extended super frame (ESF) framing and with bipolar with eight-zero substitution (B8ZS)/ Alternate Mark Inversion (AMI) coding.

AUX-003520 [**Optional: AO CS, A/V CS**] The audio system's PSTN signaling module shall support ISDN PRI (5ESS, DMS, and National ISDN), and the PRI flavors of foreign countries such as Germany, Japan, and Korea.

AUX-003530 [**Optional: AO CS, A/V CS**] The audio system shall support the Dialed Number Identification Service (DNIS) feature where the original dialed numbers are presented as generic address parameters (GAPs).

AUX-003540 [**Optional: AO CS, A/V CS**] The audio system shall support the automatic number identification (ANI) feature and use it to identify a calling party, if applicable.

VoIP requirements include the following:

AUX-003550 [**Required: AO CS, A/V CS**] The audio system IP interfaces shall support static assignment of the IP address, mask, default router, and Domain Name Service (DNS) entries.

AUX-003560 [**Required: AO CS, A/V CS**] The audio system shall support multiple DNS entries. If the primary DNS server does not respond to a DNS request, then a secondary DNS server shall be queried.

AUX-003570 [**Required: AO CS, A/V CS**] The audio system shall support configurable transmission control protocol (TCP) ports for AS-SIP messaging.

AUX-003580 [**Required: AO CS, A/V CS**] The audio system shall be able to set the IPv4/IPv6 Precedence Field bits of the Type of Service (TOS) byte and DSCP bits for media streams and signaling streams.

AUX-003590 [**Required: AO CS, A/V CS**] The audio system shall support Network Time Protocol (NTP), version 3 [RFC 1305].

AUX-003600 [**Required: AO CS, A/V CS**] The audio system shall support SNMPv3 [RFC 3414].

AUX-003610 [**Required: AO CS, A/V CS**] The audio system shall support Secure Real-Time Transport Protocol (SRTP) and Secure Real-Time Transport Control Protocol (SRTCP) [RFC 3711].

AUX-003620 [**Required: AO CS, A/V CS**] The audio system shall support SRTCP and accurately report jitter, delay, and packet loss information to the far end using Real-Time Transport Protocol (RTP) Control Protocol Extended Reports (RTCP XR) [RFC 3611].

AUX-003630 [**Required: AO CS, A/V CS**] The audio system's AS-SIP signaling module shall support RFC 3261including loose route.

AUX-003640 [**Required: AO CS, A/V CS**] The audio system's AS-SIP signaling module shall allow AS-SIP URLs for both incoming and outgoing calls. This includes all alphanumeric characters allowed in legal SIP URLs.

AUX-003650 [**Required: AO CS, A/V CS**] The audio system's AS-SIP signaling module shall support Session Description Protocol (SDP) as defined in RFC 4566.

AUX-003660 [**Required: AO CS, A/V CS**] The audio system's AS-SIP signaling module shall implement user "hold" feature by using a=inactive or a= sendonly, or by sending a mid-call INVITE that includes a session description that is the same as in the original request, but the "c" destination addresses for the media streams to be put on hold are set to zero:c=IN IP4 0.0.0.0.

AUX-003670 [**Required: AO CS, A/V CS**] The AS-SIP signaling module shall support AS-SIP Digest Authentication [RFCs 3261 and 3310].

AUX-003680 [**Required: AO CS, A/V CS**] The AS-SIP signaling module shall be able to reject incoming INVITE messages when the message does not come from pre-provisioned proxies.

AUX-003690 [**Required: AO CS, A/V CS**] The AS-SIP signaling module shall support call transfer as specified in AS-SIP Section 9.6, Call Transfer.

AUX-003700 [**Required: AO CS, A/V CS**] Audio systems shall support electronic numbering (ENUM) service registration for SIP (AS-SIP) Addresses-of-Record [RFC 3764].

Voice medium requirements include the following:

AUX-003710 [**Required: AO CS, A/V CS**] The audio system shall support DTMF Generation/Recognition per Telcordia GR-181-CORE.

AUX-003720 [**Required: AO CS, A/V CS**] The audio system shall support G.711 μ/A law [pulse code modulation (PCM)] and G.729.

AUX-003730 [**Required: AO CS, A/V CS**] The audio system's total media processing time shall be less than 50 ms including delays from jitter buffer, transcoding, mixing, packetization, and algorithm look ahead.

AUX-003740 [**Required: AO CS, A/V CS**] The audio system shall support G.168 compliance echo canceller (EC) with 128 ms echo path.

AUX-003750 [**Required: AO CS, A/V CS**] The audio system shall support Audio and Video Transport (AVT) payload type 0 and 8. [G.711 a/mu law].

AUX-003760 [**Required: AO CS, A/V CS**] The audio system shall support AVT payload 18 [G.729].

AUX-003770 [**Required: AO CS, A/V CS**] The audio system shall be able to accept in-band DTMF tones.

AUX-003780 [**Required: AO CS, A/V CS**] The audio system shall be able to send DTMF specified by RFC 4733.

AUX-003790 [**Required: AO CS, A/V CS**] The audio system shall be able to conceal 1 percent of packet loss without appreciable quality degradation.

AUX-003800 [**Required: AO CS, A/V CS**] The audio system shall be able to tolerate 40 ms of jitter for audio without appreciable quality degradation.

AUX-003810 [**Required: AO CS, A/V CS**] The audio system shall implement adaptive jitter buffers instead of static fix jitter buffers.

AUX-003820 [**Required: AO CS, A/V CS**] All hardware shall meet Network Equipment Building System-3 (NEBS-3) requirements.

3.4.3.3.7 Reduced Maximum Transmission Unit IP Environment

AUX-003830 [**Required: VO CS, A/V CS**] This subsection addresses the Maximum Transmission Unit (MTU) requirements for an IP network environment. An MTU is the maximum size of an IP packet that will be accepted for transmission without fragmenting it into a smaller datagram. The MTU size shall be configurable to optimize video traffic. As a result of devices such as encryption units, the typical MTU size shall be changed to minimize the effect of fragmentation because of the additional overhead of the encryption.

AUX-003840 [**Required: All UCCS**] The conference system shall ensure that all conferencing services provide signaling and media streams, and are capable of configuring the MTU.

AUX-003850 [**Required: All UCCS**] The conference system shall ensure that all supporting services to video and audio services, including, but not limited to, reservation, monitoring, billing, administration, operator interface, and meeting control, are capable of working in the configurable MTU IP environment.

3.4.3.3.8 IPv6 Support

AUX-003860 [**Required: All UCCS**] The conference system shall comply with the IPv6 requirements contained in Section 5, IPv6.

3.4.3.3.9 AS-SIP Support

AUX-003870 [**Required: All UCCS**] The conference system shall comply with the AS-SIP requirements contained in AS-SIP 2013, Section 4, SIP Requirements for AS-SIP Signaling Appliances and AS-SIP EIs.

3.4.3.4 Assured Delivery

This subsection describes the set of capabilities which ensures that mission-critical calls are set up and remain connected.

3.4.3.4.1 Quality of Service

AUX-003880 [**Required: All UCCS**] The system or network device shall be able to set DSCPs on both signaling packets and media streams for both IPv4 and IPv6 as specified in Section 6.2.2, Differentiated Services Code Point.

3.4.3.4.2 Other Assured Delivery Features

3.4.3.4.2.1 Congestion Response

AUX-003890 [**Required: All UCCS**] The system shall provide measures to monitor bandwidth resource usage and to activate congestion management as needed within a timely fashion.

3.4.3.4.2.2 Accounting

AUX-003900 [**Required: All UCCS**] The system shall maintain a call summary of conference sessions. This will include the conference attendee identification, access methods, IP address, E.164 numbers, time and date of the call, call duration, and total number of participants. The summaries shall be maintained for 30 days or IAW Information Assurance security requirements.

3.4.3.4.2.3 Multilevel Precedence and Preemption

AUX-003910 [**Optional: All UCCS**] The system shall operate IAW the MLPP rules and procedures specified in Section 2.26.2, Multilevel Precedence and Preemption (inclusive as applies).

AUX-003920 [**Optional: All UCCS**] Preset Conferencing. Each conferee shall be dialed at its designated precedence level. Each conferee may have a different precedence level. The conference host must be dialed at the highest precedence level of any conferee.

AUX-003930 [**Optional: All UCCS**] Meet-Me Conferencing. When a priority session requests connection to a conference that is at conference maximum, then one of the lowest precedence conferees shall be preempted, selected through any deterministic method. (Conference maximum is the maximum number of conferees authorized for the same conference.) When a priority session requests connection to a conference that is not at conference maximum, but the system is at system maximum, then one of the lowest precedence conferees on another conference will be preempted, selected through any deterministic method. Note that the selection method shall not consider any ad hoc conferees for preemption, if an allocation of system resources dedicated to ad hoc conferences has been configured per requirement AUX-003880 in Section 3.4.4.2.1, Video Conference Capacity. (System maximum occurs when the maximum number of ports or resources are provisioned on the system.) Preempted conferees shall receive a preemption notification tone and be preempted. All remaining conferees on the system shall receive a conference disconnect tone (see Table 2.9-2, UC Information Signals).

AUX-003940 [**Optional: All UCCS**] Ad hoc Conferencing. When either party of a two-party session brings in a third party, an ad hoc conference is created at the highest precedence level of the dialed conferees. Thereafter, any party of an ad hoc conference can attempt to add an additional conferee at any time. If that party is dialed at a precedence level higher than any of the current conferees, then the conference precedence level shall be elevated to a higher precedence level. If an allocation of system resources dedicated to ad hoc conferences has been configured per requirement AUX-003880 in Section 3.4.4.2.1, and there are no ad hoc system resources available to add on a conferee, then a conferee from the lowest precedence ad hoc conference will be preempted so that the conferee can be brought into the higher precedence ad hoc conference. If an allocation of system resources dedicated to ad hoc conferences has not been configured, but the system is at system maximum, then one of the lowest precedence conferees on another conference will be preempted, selected through any deterministic method, so that the conferee can be brought into the higher precedence ad hoc conference.

AUX-003950 [**Optional: All UCCS**] Ad hoc Conferencing. When a higher precedence session (i.e., higher than the conference precedence level) is placed to any of the conferees, that conferee receives a preemption notification tone (see Table 2.9-2, UC Information Signals). The other remaining conferees shall receive a conference disconnect tone, as described in Table 2.9-2. This tone indicates to the other parties that one of the conference call participants is being preempted.

3.4.4 Service Performance

AUX-003960 [**Required: All UCCS**] This section provides the service performance criteria and metrics for the system. The service performance criteria shall apply during simultaneous operation of the respective EIs. The system shall design and implement redundancy, failover, and fault tolerance at the component, subsystem, and system levels to support achieving service

availability requirements in the presence of failures at the component, subsystem, and system levels. The system shall meet the requirements specified in Section 2.8, Product Physical, Quality, and Environmental Factors.

3.4.4.1 Quality

3.4.4.1.1 Video Conference Quality

For video conferencing services implemented and provided by the conference system, video quality requirements (that are based on commercial standards for supporting video conferencing) are as follows.

AUX-003970 [**Required: VO CS, A/V CS**] The conference system shall ensure that all video equipment used in designs can operate in the presence of minimal packet loss without degrading video quality below acceptable levels.

AUX-003980 [**Required: VO CS, A/V CS**] The conference system shall ensure that all video equipment used in the design provides adequate jitter buffer sizing to ensure an optimal end-to-end (E2E) video conferencing performance.

3.4.4.1.2 Audio Conference Quality

For audio conferencing services provided by the conference system, voice quality requirements are as follows.

AUX-003990 [**Required: AO CS, A/V CS**] The conference system shall ensure that the Mean Opinion Score (MOS) on the voice path meets the MOS requirements in Section 6, Network Infrastructure End-to-End Performance.

AUX-004000 [**Required: AO CS, A/V CS**] The conference system shall ensure that the implemented design possesses the adequate performance capacity and resources to support conference access processing requirements identified in Section 3.4.4.2, Capacity.

AUX-004010 [**Optional: AO CS, A/V CS**] The conference system shall ensure the time needed to compile polling statistics to adequately support the audio conference capability.

3.4.4.2 Capacity

AUX-004020 [**Required: All UCCS**] The conference system vendor shall provide documentation stating the conference system's capacity and scalability. Statements regarding capacity and scalability will be validated at DISA's discretion.

3.4.4.2.1 Video Conference Capacity

AUX-004030 [**Required: VO CS, A/V CS**] The number of concurrent conferences supported shall be limited only by available ports and the number of licenses acquired, and shall not depend on the access methods, features, or number of participants in each conference.

AUX-004040 [**Optional: VO CS, A/V CS**] The system shall have the capacity to support at least 1,000 concurrent 384 kbps video calls.

AUX-004050 [**Required: VO CS, A/V CS**] The system shall provide sufficient speed matching capacity to support that capability regardless of the access methods, algorithms, speeds, or the feature sets being used.

AUX-004060 [**Required: VO CS, A/V CS**] The system shall provide enough transcoding capacity to support that capability regardless of the access methods, algorithms, speeds, or feature sets being used.

AUX-004070 [**Required: VO CS, A/V CS**] The system shall provide sufficient H.323 gateway capacity to support that capability regardless of the access methods, algorithms, speeds, or feature sets being used.

AUX-004080 [**Required: VO CS, A/V CS**] The system shall provide enough H.239 capacity to support that capability regardless of the access methods, algorithms, speeds, or feature sets being used.

AUX-004090 [**Optional: VO CS, A/V CS**] The system shall provide enough H.261 Annex D capacity to support that capability regardless of the access methods, algorithms, speeds, or feature sets being used.

AUX-004100 [**Optional: VO CS, A/V CS**] The system shall support a minimum of 200 EIs for each multipoint conference.

AUX-004110 [**Required: A/V CS**] The system shall provide at least four audio added-on ports for each conference without the use of external audio systems or by cascading conference systems.

AUX-004120 [**Required: VO CS, A/V CS**] The system shall ensure that audio added-on does not compromise support for other capacity requirements.

AUX-004130 [**Optional: VO CS, A/V CS**] The system shall support the ability to configure allocation (0 to 100 percent, default 20 percent) of system ports/resources to be dedicated to ad hoc video conferences. Meet-me conferences shall not use resources allocated to ad hoc conferences, and vice versa.

3.4.4.2.2 Audio Conference Capacity

AUX-004140 [**Optional: AO CS, A/V CS**] The system shall be capable of scaling up to 2,500 concurrent audio calls.

AUX-004150 [**Optional: AO CS, A/V CS**] The system shall support up to 200 participants in a single conference session.

AUX-004160 [**Optional: AO CS, A/V CS**] The system shall be capable of scaling up to 500 concurrent conferences.

AUX-004170 [**Optional: AO CS, A/V CS**] The system shall be capable of scaling up to 500 or more conference control web sessions.

AUX-004180 [**Optional: AO CS, A/V CS**] The system shall be capable of scaling to support 10,000 or more reservations.

AUX-004190 [**Optional: AO CS, A/V CS**] The audio conference system shall support more than 50 concurrent recordings.

AUX-004200 [**Optional: AO CS, A/V CS**] The system shall support the ability toconfigure an allocation (0 to 100 percent; default 20 percent) of system ports and resources to be dedicated to ad hoc audio conferences. Meet-me conferences shall not use resources allocated to ad hoc conferences, and vice versa.

3.4.4.2.3 Registration, Admission, Status, and Routing Function

AUX-004210 [**Optional: All UCCS**] The conference system shall have the capability to provide bandwidth management, EI registrations, admissions, status, and routing functions. Furthermore, the system shall be capable of scaling to support at a minimum of 1,000 concurrent conference calls and 10,000 concurrent registrations of EIs.

3.4.4.2.4 Scalability

NOTE: Scaling can be provided by deploying multiple systems and provisioning or load sharing between systems.

The conference system should support a nominal growth of services without requiring major overhaul or major replacement of equipment.

AUX-004220 [**Required: VO CS, A/V CS**] The system architecture supporting the dedicated IP-based video services capability shall be able to scale to accommodate increased growth in dedicated IP-based video services EIs.

AUX-004230 [**Required: VO CS, A/V CS**] The system architecture supporting the dial-up video services capability shall be designed to support up to a 50 percent increase in dial-up video services.

AUX-004240 [**Optional: VO CS, A/V CS**] The system shall be able to scale to accommodate increased growth to support increases in connections to ISDN networks. Additional capacity in regards to this item shall be used only to support ISDN dial-up video traffic.

AUX-004250 [**Required: AO CS, A/V CS**] Audio add-on and audio conference service shall be able to scale to accommodate increased growth in call volume and EIs.

3.4.5 Service Management

This section describes service management. The conference system shall provide reservation, scheduling, and registration services. The conferencing system service applications shall integrate or provide interfaces with Government network services and management applications. The conference system shall provide management functions to ensure continuous operations and accessibility of services with a data feed into the Government network services systems. The equipment and software applications shall be configurable to allow alarm and log file transmissions to be selective with the activation of a specific feature set.

3.4.5.1 System Management

3.4.5.1.1 General System Management

AUX-004260 [**Required: All UCCS**] The conference system shall provide services management and monitoring for the Operation, Administration, Maintenance, and Provisioning (OAM&P) of conferencing services.

AUX-004270 [**Required: All UCCS**] The conference system shall provide a service monitor and management system to actively monitor elements and critical components within the system.

AUX-004280 [**Required: All UCCS**] Report data shall be in a form that is capable of being managed by the Government network services applications and network elements, which are based on commercial and industry standards. The data transmitted shall comply with industry standard management protocols and/or data formats. Such industry standard protocols for data exchange include, but are not limited to, Syslog, Common Object Request Broker Architecture (CORBA), SNMPv3, Transaction Language 1 (TL1), Java 2 Platform Enterprise Edition (J2EE), and Extensible Markup Language (XML).

AUX-004290 [**Required: All UCCS**] The conference system shall be responsible for managing and monitoring the following services and related resources. Furthermore, the system shall provide real-time, read-write continuous Network Management capabilities. The level of monitoring shall be sufficient to be able to track the status, through standard interfaces and

protocols, of individual discrete hardware and software components used to deliver the service to enable visibility of individual incidents affecting the service delivery:

a. Equipment and associated services.

b. Point-to-point and multipoint video services.

c. Audio services.

d. Reservation and scheduling.

e. Gateways and interfaces.

f. Conferencing center Web site.

g. Support systems.

AUX-004300 [**Required: All UCCS**] The conference system shall furnish and maintain a service monitor and management system with external interfaces or feeds into Government management application and monitoring systems. These interfaces shall provide the Government the capability to monitor the performance and status of video and audio services. These interfaces shall provide for the importing and exporting of video and audio management services and monitoring information. The Government shall have real-time access to all video and audio services management and monitoring data collected and stored by the system. These interfaces are further specified in Section 2.19.1, General Management.

AUX-004310 [Required: All UCCS] The conference system shall support the use of Simple Network Management Protocol version 3 (SNMPv3) for system management and monitoring.

AUX-004320 [Required: All UCCS] The conference system shall support a 10/100-Mbps Ethernet physical interface to the DISA VVoIP Element Management System (EMS). The interface shall work in either of the two following modes using auto-negotiation: IEEE, Ethernet Standard 802.3, 1993; or IEEE, Fast Ethernet Standard 802.3u, 1995.

AUX-004330 [Conditional: All UCCS] If the system will be deployed as a DISN asset, then local management traffic and VVoIP EMS management traffic shall use separate physical Ethernet interfaces. Redundant VVoIP EMS physical Ethernet interfaces may be used but are not required. Redundant local management physical Ethernet interfaces may be used but are not required.

3.4.5.1.2 Fault Management

AUX-004340 [**Required: All UCCS**] The conference system shall provide fault management for services and resources. The system shall provide the Government with all the fault information needed electronically to effectively manage all conferencing services.

AUX-004350 The fault management system shall include the following minimum requirements:

AUX-004350.a [**Required: All UCCS**] Power status shall be provided for individual shelf, rack, or controller units.

AUX-004350.b [**Required: All UCCS**] Functional/Fault/Online/Offline status.

AUX-004350.c [**Required: All UCCS**] Input/loss of input signal, or signal below working threshold.

AUX-004350.d [**Required: All UCCS**] Output/loss of output signal.

AUX-004350.e [**Required: All UCCS**] Input/output signal outside of specified range.

AUX-004350.f [**Required: All UCCS**] Intrusion detected.

AUX-004360 The fault management function shall perform the following:

AUX-004360.a [**Required: All UCCS**] Detect and identify faults. The fault management service provided shall monitor dedicated and dial-up video services resources, audio conferencing service status, support services status, and conduct alarm surveillance, maintain error logs, and analyze monitored or logged errors or events to anticipate faults:

(1) Faults shall be detected within 10 seconds of their occurrence.

(2) Faults shall be identified within 10 seconds of being detected.

(3) Faults shall be correlated within 10 seconds of identification.

(4) The Government shall be notified of service affecting faults within 10 seconds of fault correlation.

AUX-004360.b [**Required: All UCCS**] Isolate faults to include correlation of alarms. The fault management service provided shall initiate diagnostic testing and evaluate diagnostic results to determine the nature, severity, and specific cause(s) of the fault and isolate the fault to the video, audio, and support services at a component level.

AUX-004360.c [**Required: All UCCS**] Temporary corrective action when a fault occurs. The fault management service provided shall reroute a conference call or service request to other hubs, circuits, or equipment in the case of a fault, including through the use of redundancy and failover capabilities.

AUX-004360.d [**Required: All UCCS**] Correct faults. The fault management service provided shall implement corrective actions on faults to restore services to proper working order and complete resource/service restoration when the fault is with equipment or services provided by the conference system. This process shall incorporate backup and recovery capabilities to restore configurations and services to operational service.

3.4.5.1.3 Fault Management Information

AUX-004370 [**Required: All UCCS**] The conference system shall provide the Government with real-time monitoring of service-affecting events related to hardware and software components and subcomponents that compose the conference system. These service-affecting events impacting the scheduling and operation of system services include, but are not limited to, the following:

a. Outages for all conferencing services elements to be exported into the existing trouble tracking system.

b. Any hazardous condition, as specified in DISA Circular 310-55-1, that may cause loss of service.

AUX-004380 [**Required: All UCCS**] The conference system shall be able to update all service management thresholds, as required.

AUX-004390 [**Required: All UCCS**] The conference system shall maintain historical records of all fault alarm data and be able to export this data into the Government management application systems.

3.4.5.1.4 Performance Management

AUX-004400 [**Optional: All UCCS**] The conference system shall provide a performance management system. The performance management system shall monitor and control all service performance and the quality of the services and features supporting the conference system. Performance management shall perform the following functions.

AUX-004410 [**Optional: All UCCS**] Monitor, analyze, and characterize performance. The conference system shall monitor, analyze, and gather performance-related data to detect and characterize normal and degraded performance and be able to trend this data over time for metrics purposes. Section 3.4.4, Service Performance, defines normal performance requirements. The system shall provide notification if the service resources are being stressed with excess traffic loads.

AUX-004420 [**Optional: All UCCS**] Tune and control performance in areas of control: the conference system shall activate controls to tune all services performance to restore degraded resources/services to acceptable performance levels. If control actions will cause any user service disturbance, then these actions shall be approved by the Government before execution.

AUX-004430 [**Optional: All UCCS**] Maintain all services supporting the conference system through an operations database. The conference system shall maintain a database or be exportable to a Government network management tool supporting all conferencing services operational information, both real-time and historical, including, for example, traffic characterization data, performance data, and information on usage of resources/services. Historical records shall be kept of all performance data for a designated period of time.

AUX-004440 [**Optional: All UCCS**] Evaluate performance of services and features. The conference system shall continuously assess and monitor the performance of all conferencing services and features, according to the performance parameters identified in Section 3.4.4, Service Performance, to ensure that the performance levels of Government services and features meet the specification requirements of Section 3.4.3, Service, and Section 3.4.4, Service Performance.

3.4.5.1.5 Government Performance Management Information

This subsection describes Government performance management information requirements.

AUX-004450 [**Optional: All UCCS**] The conference system shall provide notification of events, exceptions, or measures related to the performance of services' resources, and associated service-affecting conditions to Government platforms as required. Performance degradation notification shall include, at a minimum, the following.

The conferencing services are composed of servers, applications and network services, appliances, and network devices responsible for supporting video services globally throughout the DoD community. The conferencing service is of a time-sensitive nature and one of the services that is being offered with the convergence of IP on the backbone.

There are two parts to the network management of this service: transport monitoring and video stream monitoring. First, the underlying network elements and servers need to be included in fault management and performance management activities at the physical layers and IP layers. Second, the video service needs to have instrumentation included that would be able to monitor the conferencing user's experience, in order to isolate problems and reveal if the video service is meeting specific service-level requirements.

AUX-004460 [**Optional: VO CS, A/V CS**] The performance management toolset should be able to collect information from the video device managers. The information it should collect would include, but not be limited to, the number of participants, duration of a session, video burst measurements, and capacity measurements.

3.4.5.1.6 Security Management

This subsection describes the security management requirements.

AUX-004470 [**Required: All UCCS**] Certification and Accreditation. The conference system shall ensure that all systems and subsystems in UC conferencing undergo Certification and Accreditation (C&A) IAW the DoD Information Assurance Certification and Accreditation Process (DIACAP) and associated audits.

AUX-004480 [**Required: All UCCS**] Best Security Practices. The conference system shall incorporate best security practices such as single sign-on, public key encryption (PKE), smart card, and biometrics in system security design of DoD information, but does not limit to certain security mechanisms.

AUX-004490 [**Required: All UCCS**] Enterprise Security Management. The conference system shall implement enterprise management of security devices and applications such as the following:

a. Firewalls and boundary protection.

b. Intrusion detection systems.

c. Operating systems, network devices, and applications security.

d. Vulnerability management.

AUX-004500 [**Required: All UCCS**] Security Configuration Specifications. The conference system shall comply with DoD reference documents such as STIGs or security recommendation guides from the DISA Facility Security Officer (FSO) that are pertinent to the UCCS or subcomponents.

3.4.5.2 Online Directory

AUX-004510 [**Required: VO CS; Optional: AO CS, A/V CS**] The system shall provide an online directory service to support scheduling that shall include general information about all registered DoD video and audio users including, but not limited to, a user's point of contact, location, supported data rates, organization name, unit capabilities, and software versions.

AUX-004520 [**Required: VO CS; Optional: AO CS, A/V CS**] The system shall update the online directory within 24 hours of learning of a new EI receiving service, a change in an existing EI's service status, or notification by DISA of any other change with regard to an EI.

AUX-004530 [**Required: VO CS; Optional: AO CS, A/V CS**] The system shall provide a secure Web interface that implements a public key enablement application, allowing registered users with a valid DoD PKI or External Certification Authority (ECA) certificate and Internet connectivity to access the online directory.

AUX-004540 [**Required: VO CS; Optional: AO CS, A/V CS**] The online directory shall support more than 1 million data entries and shall support more than 500 concurrent users at the same time.

AUX-004550 [**Required: VO CS; Optional: AO CS, A/V CS**] The online directory shall be Web-based using modern and open technologies and provide interfaces, such as XML, Simple Object Access Protocol (SOAP), Web Service Description Language (WSDL), and Universal Discovery Description Interface (UDDI), allowing external data sources from others to perform directory lookups, queries, and updates as specified by "Horizontal Fusion Standards and

Specifications," 3 November 2004, and DoD Joint Technical Architecture, Version 6, Volumes I and II, 3 October 2003.

AUX-004560 [**Required: VO CS; Optional: AO CS, A/V CS**] The online directory shall support the discovery service that provides processes for discovery of information content or services that exploit metadata descriptions of information technology resources stored in directories, registries, and catalogs (to include search engines) as specified by "Horizontal Fusion Standards and Specifications," 3 November 2004, and "DoD Joint Technical Architecture," Version 6, Volumes I and II, 3 October 2003. Directory services shall be designed to meet Protected Personal Information/Personally Identifiable Information protection requirements and Privacy Act requirements.

AUX-004570 [**Required: VO CS; Optional: AO CS, A/V CS**] The system shall provide an online directory service to allow authorized registered users to search system-wide for other authorized, registered service users in the directory and/or to update data entries.

3.4.5.3 Registration System

AUX-004580 [**Required: All UCCS**] The conference system shall include an automated registration system that current and prospective subscribers can access online using a standard Web browser.

AUX-004590 [**Required: All UCCS**] All data sent and recived by the automated registration system shall be encrypted using Secure Socket Layer (SSL)/TLS technology, as a minimum, with DoD PKI certificate authentication and validation.

AUX-004600 [**Required: All UCCS**] The automated registration system shall collect all data necessary to comply with provisioning requirements.

AUX-004610 [**Required: All UCCS**] The automated registration system shall collect all data necessary for connection approval by the program office.

AUX-004620 [**Required: All UCCS**] The automated registration system shall collect all data necessary to authorize users for access to operational systems including scheduling and reservations.

AUX-004630 [**Required: All UCCS**] The automated registration system shall collect all data necessary to support the operational requirements of UC conferencing services. Upon connection approval and completion of verification and interoperability tests, all data shall be available to the operational systems for the scheduling and activation of conferences.

AUX-004640 [**Required: All UCCS**] The automated registration system shall be the authoritative source of conference subscribers' data. The system shall provide the necessary tools to allow authorized users to maintain and update user and endpoint information.

AUX-004650 [**Required: All UCCS**] The automated registration system shall support Privacy Act statements as required by Information Assurance policy.

3.4.5.4 Scheduling System

AUX-004660 [**Required: All UCCS**] The primary component for requesting a conference shall be by an automated scheduling system that authorized users can access online using a standard Web browser. All data shall be encrypted using SSL/TLS technology, as a minimum, with DoD PKI certificate authentication and validation.

AUX-004670 [**Required: All UCCS**] The automated scheduling system shall resolve the availability of all requested participants and conferencing resources. The customer shall be able to schedule a conference immediately or schedule it for some time in the future. Immediate start requests for conferences shall be activated in less than 5 minutes of confirmation of available resources and participants. The system shall support scheduling conferences with the conference size larger than the number of initially invited or scheduled endpoints. A unique identification number shall be assigned to each conference event to facilitate conference control and management. E-mail notifications shall be provided to all conference participants to facilitate event coordination. E-mail content shall be editable as a configuration feature. The system shall support encrypted e-mail for notifications. Scheduled conference information also shall be available through the scheduling Web interface.

AUX-004680 [**Required: All UCCS**] The original requester shall serve as the conference manager for all conferences. The system shall have the capability to assign other system users to act as surrogates for the original requester. This may include peers and/or workflow superiors. Conference management and control shall include the ability to make changes to a scheduled or active conference. Supported changes to active conferences shall include, but not be limited to, the addition or deletion of participants, early termination of a conference, and extension of the conference beyond the originally scheduled end time. Additions, deletions, and extensions of conferences shall occur without interruption to the existing conference, other than preemptive precedence calls. Additions and extensions to conferences shall be executed in less than 5 minutes of confirmation of available resources. Deletions and terminations of conferences shall be executed in less than 5 minutes of the request by the conference manager. The system shall support scheduling of recurring conferences.

3.4.5.5 Accounting and Billing

AUX-004690 [**Required: All UCCS**] The conference system shall provide an Accounting Management function. The Accounting Management function shall do the following:

> **AUX-004690.a** [**Required: All UCCS**] Provide accounting information to the Government regarding all conferencing services provided.

AUX-004690.b [**Required: All UCCS**] Provide all conferencing services data to the Government at a level of detail that allows the Government to bill conferencing services customers based on usage.

AUX-004700 [**Required: All UCCS**] The Accounting Management function shall enable charges to be established for the use of dedicated and dial-up conferencing services resources.

AUX-004710 [**Required: All UCCS**] The conference system Accounting Management function shall provide for the collection, aggregation, storage, and reporting of all conferencing service usage data. The accounting management function shall consist of systems to activate and monitor customer accounts and to collect, aggregate, and report on usage data.

AUX-004720 The conference system shall provide the capability to perform the following Accounting Management functions:

AUX-004720.a [**Required: All UCCS**] Collect usage data from a Call Detailed Record (CDR) (i.e., at the level of the authorization code).

AUX-004720.b [**Required: All UCCS**] Aggregate and combine data for generating reports as specified by the Government.

AUX-004720.c [**Required: All UCCS**] conference records per individual customer's account.

AUX-004720.d [**Required: All UCCS**] Ensure continuous (24x7) monitoring, processing, and recording for all video services-related events and customer activity data.

AUX-004720.e [**Required: All UCCS**] Maintain a database of various conference reports per individual customer account, including conference detail summary, completion summary, and exception reports.

AUX-004720.f [**Required: All UCCS**] Archive data for possible later retrieval by the Government (e.g., in response to customer inquiries or to audit the data).

AUX-004730 [**Required: All UCCS**] The conference system shall provide the capability to transmit usage data to the EMS. The frequency of data transfer shall be determined by the Government based on volume of data collected. The system shall maintain all accounting data for at least one billing cycle.

3.5 GENERAL MASS NOTIFICATION WARNING SYSTEM (MNWS)

See UC Framework 2013, Section 3.4.2, for a description of the MWNS.

The MNWS shall provide the following functionality:

AUX-004740 [**Required**] Alert activation. The MNWS shall provide dissemination of alert notifications to target authorized subscribers by means of multiple notification devices, including, but not limited to, the following:

a. Personal devices. Includes networked desktop popups, PKI signed emails, text messaging, pagers, voice telephone calls, and other existing communication infrastructure such as UC/VoIP systems.

b. Mass notification devices. Includes Giant Voice system; indoor voice systems; Land Mobile Radios (LMRs); and integration with AM/FM/TV broadcast systems, fire/evacuation systems, and social networks.

AUX-004750 [**Required**] Tracking and reporting. The MNWS shall track and report alert delivery in real time, track and report subscriber responses to alert notifications in real time, and report on the operational status of delivery devices and services.

AUX-004760 [**Required**] Database. MNWS shall establish and maintain a comprehensive database of subscribers served by the installation's MNWS.

AUX-004770 [**Required**] Group Management. The MNWS shall offer unfettered flexibility to place target subscribers into groups that can then be targeted for specified alerts. The types of groups that can be created include, but are not limited to, groups based on organization, rank, roles and responsibilities, location, device delivery preference, phone number, and IP address. In addition, the groups can be static ("rosters") or dynamic (based on subscriber data attributes).

AUX-004780 [**Required**] Permission Management. Access to MNWS functions, assets, and resources are governed by the permissions assigned to each operator and subscriber. The MNWS shall be capable of assigning permissions on a group-wide role basis such that each member of the group receives identical permission to MNWS functions, assets, and resources.

AUX-004790 [**Required**] Delivery Device Management. The MNWS shall ensure operational status of delivery devices, provide appropriate data to delivery devices in order for delivery devices to send the desired alerts to the correct set of designated target subscribers, and track performance of delivery devices in conjunction with alert notifications.

AUX-004800 [**Required**] Self-service. The MNWS shall support the ability for subscribers to update their personal information to ensure up-to-date contact information for purposes of emergency alert notification.

AUX-004810 [**Required**] The MNWS shall be Section 508 compliant and provide effective alerting to members of the special needs community.

AUX-004820 [**Required**] The MNWS shall comply with all pertinent DoD information assurance and security requirements including, for example, CAC-enabled devices, PKI servers, and prohibition on group passwords:

a. The MNWS shall archive all alerts that are sent in order to maintain an audit trail in compliance with all DoD information assurance requirements, including logins, failed logins, data updates, and alert activations.

b. In the case of OCONUS deployments, the MNWS shall meet host nation requirements for emergency systems.

AUX-004830 [**Required**] The MNWS shall be capable of delivering installation-wide alert notification to all targeted personnel at a minimum of within 10 minutes, per DoD Instruction (DoDI) 6055.17 requirements or, as needed, at a faster delivery time per the specific needs of the installation.

AUX-004840 [**Required**] The MNWS service shall be capable of delivering regional alert notification to all targeted personnel at least within 10 minutes, per DoDI 6055.17 requirements or, as needed, at a faster delivery time per the requirements of the specific region.

AUX-004850 [**Required**] The MNWS service shall scale to support Command-wide alert notifications involving over 500,000 subscribers at over 100 installations.

AUX-004860 [**Required**] The MNWS service shall be capable of delivering Command-wide alert notification to all personnel within 10 minutes per DoDI 6055.17 requirements or, as needed, at a faster delivery time per the requirements of the Command.

AUX-004870 [**Required**] The MNWS shall provide a high availability service having a complete set of redundant primary and standby platforms, and this redundant configuration shall have an availability of 99.95 percent.

AUX-004880 [**Required**] The MNWS shall support the use of standard and open protocols including the Common Alerting Protocol (CAP) and XML in order to interface with various event sources and delivery devices.

AUX-004890 [**Required**] The MNWS shall meet all applicable STIGs and have current and applicable information assurance C&A.

AUX-004900 [**Required**] The MNWS shall provide supervision and a monitoring capability of MNWS components and of delivery systems, and provide operators with notification of a failure of an MNWS component or delivery system within 200 seconds of the occurrence of the failure.

AUX-004910 [**Required**] The MNWS shall be IPv6 compliant per the requirements in Section 5, IPv6.

3.5.1 Standby MNWS Platform

AUX-004920 [**Required**] An MNWS system shall have both a primary MNWS platform and a standby MNWS platform.

NOTE: In this context, a "platform" refers to a complete working instance of MNWS equipment and may consist of a number of distinct physical boxes or elements including, for example, application servers and database servers.

AUX-004930 [**Required**] The standby MNWS platform shall be deployed at a geographically diverse location from the primary MNWS platform.

AUX-004940 [**Required**] The standby MNWS platform shall fully replicate the hardware, software, database, and connectivity to event sources and delivery devices of the primary MNWS platform.

AUX-004950 [**Required**] The standby MNWS platform shall maintain standby connections with the complete set of event sources and delivery devices to which the primary MNWS platform is connected.

AUX-004960 [**Required**] When the standby MNWS platform loses contact with the primary MNWS platform and is unable to reestablish connectivity within a pre-configured time interval (default = 60 seconds), then the standby MNWS platform shall notify a predefined list of operators that the standby MNWS platform has lost connectivity to the primary MNWS platform. The standby MNWS platform shall periodically attempt to reconnect with the primary MNWS platform.

NOTE: The operators contacted by the standby MNWS platform confirm the status of the primary MNWS platform. If the primary MNWS platform is operational, then the operators keep the standby MNWS platform in standby status and address the loss of connectivity between the primary MNWS platform and standby MNWS platform. If the operators determine that the primary MNWS platform has failed, then the operators notify the standby MNWS platform that it is now the acting primary MNWS platform, and the standby MNWS platform replaces the primary with respect to all operations and functionality.

NOTE: When the primary MNWS platform fails, then the existing sessions of all operators and subscribers logged into the primary MNWS platform will fail. It is recommended that the client software and Web-based user interface automatically redirect a login request to the standby MNWS platform in the event that the client software or Web-based user interface is unable to reach the primary MNWS platform. Once an authorized operator has notified the standby MNWS platform that the standby MNWS platform has temporarily assumed the role of the primary MNWS platform, then subscriber attempts to log in to the standby MNWS platform will succeed.

AUX-004970 [**Required**] When the primary MNWS platform comes back up and a connection is reestablished between the primary MNWS platform and the standby MNWS platform (temporarily acting as the primary MNWS platform), then the primary MNWS platform shall

resynchronize its database to the database of the standby MNWS platform and reestablish connections with the complete set of event sources and delivery devices.

AUX-004980 [**Required**] When the two MNWS platforms are fully synchronized, the designated operators direct the fail-back to the primary MNWS platform. Operators currently using the standby MNWS platform are notified of the pending fail-back prior to execution of fail-back. Upon fail-back, the standby MNWS platform will once again continuously synchronize with the primary MNWS platform.

3.5.2 [Optional] Mobile MNWS Platform

AUX-004990 [**Optional**] The vendor shall offer a mobile instance of the MNWS software designed to run on a ruggedized laptop or equivalent mobile platform.

AUX-005000 [**Optional**] The mobile MNWS platform shall periodically synchronize its database with the active MNWS platform (i.e., the primary MNWS platform unless the primary is currently failed over to the standby MNWS platform).

AUX-005010 [**Optional**] The communication between the mobile MNWS platform and the primary MNWS platform or the mobile MNWS platform and the standby MNWS platform shall be secured using Secure HTTP employing a two-way exchange of certificates or an alternative security protocol providing at least equivalent authentication, confidentiality, and integrity mechanisms.

AUX-005020 [**Optional**] The mobile MNWS platform shall have at least a Federal Information Processing Standards (FIPS) 140-2 Level 1 compliant encrypted hard drive, and it is of particular importance that the subscriber database on the mobile MNWS platform be encrypted.

AUX-005030 [**Optional**] In the event that the primary MNWS platform and standby MNWS platform are both inaccessible or inoperative, then the mobile MNWS platform shall interface remotely with the telephony, e-mail, and Short Message Service (SMS) in order to deliver alert notifications. Recommended network connectivity methods for the mobile MNWS platform include LAN, 802.11b/g/n, broadband, and satellite.

AUX-005040 [**Optional**] The communication between the mobile MNWS platform and the external delivery devices and services, specifically telephony alerting services, MNWS Simple Message Transfer Protocol (SMTP) server, and SMS aggregators, shall be secured using Secure HTTP employing a two-way exchange of certificates or an alternative security protocol providing equivalent or better authentication, confidentiality, and integrity mechanisms.

AUX-005050 [**Optional**] The controller at the mobile MNWS platform is required to generate the alerts to the various remote delivery devices. There is no requirement that operators on remote computers be able to access the mobile MNWS platform.

AUX-005060 [**Optional**] The mobile MNWS platform shall track alert delivery progress and collect alert responses.

3.5.3 MNWS Database

AUX-005070 [**Required**] The MNWS shall maintain a comprehensive database of subscribers including all contact information necessary for the MNWS to send alert notifications to the subscribers.

NOTE: A representative but non-exhaustive list of the types of information maintained for each subscriber includes personal information such as name, usernames, group profiles identifying the groups to which the subscriber belongs for alert notification purposes, organizational affiliations, rank, categories of roles and responsibilities, a list of preferred and mandatory delivery devices and the contact information necessary to reach the subscriber via each delivery device, location, and categories of alerts applicable to the subscriber. In addition, subscriber information shall include a Date Eligible for Return From Overseas (DEROS) expiration date so that subscribers can be automatically removed from the alert notification set when they leave the theater.

AUX-005080 [**Required**] The MNWS database shall integrate with the relevant existing subscriber databases such as the Military Personnel Data System (MilPDS) and the Civilian Personnel Data System (CivPDS) in order to periodically synchronize subscriber data, including subscriber attributes and contact details, and to ensure accurate and up-to-date targeting of the appropriate subscriber population.

AUX-005090 [**Required**] The frequency with which the MNWS synchronizes its database with other relevant existing DoD databases shall be configurable. At a minimum, it is anticipated that synchronization will occur on a daily basis unless the local Command specifies otherwise.

AUX-005100 [**Required**] The MNWS shall support the Lightweight Directory Access Protocol (LDAP) and shall be capable of accessing databases that support LDAP.

AUX-005110 [**Required**] MNWS system access to the existing subscriber databases shall be read-only.

AUX-005120 [**Required**] Operators having the requisite authorization shall be able to define any number of subscriber attributes and contact information fields for the MNWS subscriber database including user attributes and contact details, organizational hierarchy, groups, and distribution lists.

AUX-005130 [**Required**] Operators having the requisite authorization shall be able to manually add subscribers to the database, update the contact information, update the mandatory and preferred delivery devices for a given subscriber and other fields of a subscriber record, and remove subscribers from the MNWS database.

AUX-005140 [**Required**] The MNWS shall be capable of storing database tables in an external, installation-provided database server.

3.5.4 Notifications Across MNWSs

AUX-005150 [**Required**] An MNWS shall be able to convey alerts to other MNWSs to support cross-organizational alert notifications, multiple installation alert notifications, regional alert notifications, and Command-wide alert notifications. In addition, an MNWS belonging to one service shall have the capability to convey alerts to one or more MNWSs belonging to one or more different services, and Combatant Command (COCOM) MNWSs shall be able to cascade appropriate alerts to their Service component MNWSs.

AUX-005160 [**Required**] Connections between MNWSs shall be secured using Secure HTTP employing a two-way exchange of certificates or an alternative security protocol providing at least equivalent authentication, confidentiality, and integrity mechanisms.

AUX-005170 [**Required**] MNWSs that share notifications shall exchange distribution lists of subscriber groups and associated targeting details including location and organizational affiliation.

AUX-005180 [**Required**] Operator roles and permissions will dictate whether an operator can share a notification with a particular peer MNWS, the nature of the alerts that the operator is allowed to share with a peer MNWS, and the target groups belonging to the peer MNWS that the operator is authorized to alert.

AUX-005190 [**Required**] An MNWS that publishes an alert to a second MNWS shall collect alerting tracking data and subscriber responses from the second MNWS.

3.5.5 MNWS Operator

AUX-005200 [**Required**] Operators authorized to perform group management tasks shall be able to create groups, assign individual subscribers to new or existing groups, assign groups of subscribers to new or existing groups, remove subscribers and groups from existing groups, and delete groups without deleting the subscribers and groups composing the deleted group:

a. Operators authorized to perform group management tasks shall be able to define Static subscriber groups composed of a selected list of subscribers (“roster”) that may include nested static groups.

b. Operators authorized to perform group management tasks shall be able to define Dynamic subscriber groups composed of lists of subscribers based on data queries on their database attributes.

AUX-005210 [**Required**] Operators having the requisite authorization shall be able to assign preferred and mandatory delivery devices to be used when alerting a subscriber or a group.

AUX-005220 [**Required**] Operators having the requisite authorization shall be able to generate predefined alert notification scenarios for subscribers and groups. These scenarios include the content of the alert, multiple response options for the subscriber to choose from, target

subscribers and mass communication devices, and preferred and mandatory personal delivery devices to be used when alerting the target subscriber(s) and/or group(s).

AUX-005230 [**Required**] Operators having the requisite authorization shall be able to manually activate predefined alert scenarios to trigger alert notification. The operator shall be able to specify the timing of the alert (e.g., immediately, at a certain time, on a recurring basis).

AUX-005240 [**Required**] Operators having the requisite authorization shall be able to create and activate alerts on the fly:

a. When an operator creates an alert on the fly, then the operator designates the target subscribers and/or groups, the preferred and mandatory delivery devices, the contents of the alert message, and the timing of the alert (e.g., immediately, at a certain time).

AUX-005250 [**Required**] Operators having the requisite authorization shall be able to target subscribers for alert notification based on organizational structure, distribution lists, physical location [over a Geographical Information System (GIS) map or by specifying zone code(s) or location name(s)], individual name, dynamic database query, roles and responsibilities, phone number, IP address, etc.

AUX-005260 [**Required**] Operators having the requisite authorization shall be able to block or remove subscribers or groups from a pre-built alert notification scenario or from a pending alert notification.

AUX-005270 [**Required**] Operators having the requisite authorization shall be able to define scheduled activation of test alerts.

AUX-005280 [**Required**] Operators having the requisite authorization shall be able to track the delivery of events and subscriber multiple responses.

AUX-005290 [**Required**] For any given alert, operators having the requisite authorization shall be able to retrieve and display the count of targeted recipients, the actual number of recipients, and the number of recipients who acknowledged receipt of the alert.

AUX-005300 [**Required**] For any given alert, operators having the requisite authorization shall be able to retrieve and display the count of targeted recipients and view the coverage of existing contact details per the selected notification devices against the count of targeted recipients prior to activating the alert.

AUX-005310 [**Required**] Operators having the requisite authorization shall be able to geo-target alert notification by selecting geographic areas, perimeters, and locations on electronic maps.

3.5.6 Web Interface for Operators and Subscribers

AUX-005320 [**Required**] The MNWS shall have a Web-based operator interface for operators to publish and track alerts and perform administrative tasks including, but not limited to, the management of subscribers, delivery devices and pre-built alert scenarios:

AUX-005320.a [**Required**] The operator Web-based interface shall be role and permission based, and only those capabilities allowed by the operator's authorization will be available.

AUX-005320.b [**Required**] All operator activities, including failed logins, shall be centrally audited. At a minimum, the audit trail shall record the following details per action: login-id, object type, action taken, and source IP address. Web-based audit reports shall be available only to authorized operators. Audit trail reports shall be exportable.

AUX-005330 [**Required**] The MNWS shall have a Web-based subscriber interface for subscribers ("self-service") to view alerts and view and update their personal information including their contact information and device preferences relating to event notification.

AUX-005340 [**Required**] Using the Web-based subscriber interface, a subscriber shall be able to view the alerts to which he or she is subscribed as well as the list of all the alerts for which the subscriber is eligible but not subscribed. The subscriber shall be able to opt-in to types of alerts for which the subscriber is eligible but not subscribed and opt-out of non-mandatory types of alerts for which the subscriber is subscribed.

AUX-005350 [**Required**] The Web-based user interface shall work on personal computers running DoD-approved operating systems and on DoD-approved Web browsers.

AUX-005360 [**Required**] The Web-based session between the browser and the MNWS Web server shall be secured using Secure HTTP. The MNWS Web server is required to authenticate itself to the operator or subscriber using its server certificate.

AUX-005370 [**Required**] Operators shall authenticate to the MNWS Web server using username and strong password. The session times out after a configurable period of inactivity, and the operator shall establish a new Web-based session with the MNWS Web server.

AUX-005380 [**Required**] Subscribers shall authenticate to the MNWS Web server either using a Common Access Card (CAC) or LDAP Windows authentication or using an authentication method that is at least as secure as either of the two previous methods.

3.5.7 Client Software for Subscribers

AUX-005390 [**Required**] The MNWS shall provide client software that runs on subscriber computers, the purpose of which is to furnish alert notifications.

AUX-005400 [**Required**] When an alert occurs that is intended for the subscriber, then the client software shall provide an audio alert accompanied by a persistent visual display of the alert message on the computer until the alert is canceled; no user action will be required to receive desktop notifications.

AUX-005410 [**Required**] When the client software receives multiple concurrent alerts, then the alert notifications are displayed vertically and horizontally on the desktop in a tiered fashion.

AUX-005420 [**Required**] If a subscriber logs into the computer and runs the client software after one or more alerts have been sent but while the alert or alerts are still active, then the client software provides an audio alert accompanied by a persistent visual display of the currently active alert message(s) on the computer until the subscriber responds to the alert(s).

AUX-005430 [**Required**] When the client software displays an alert on the computer, the subscriber shall be presented with response options enabling the subscriber to select a response option. When the subscriber selects a response option, the client software shall transmit the subscriber response to the MNWS server. The MNWS server stores the subscriber response, and the subscriber response is accessible to authorized operators.

AUX-005440 [**Required**] The connection between the MNWS client and MNWS server shall be secured using Secure HTTP. The MNWS server is required to authenticate itself to the client using its server certificate. The subscriber shall authenticate to the MNWS server using a CAC card or Active Directory Windows authentication or using an authentication method that is at least as secure as either of the two previous methods.

AUX-005450 [**Required**] The MNWS service shall furnish warning notification applications for mobile devices commonly used by subscribers (e.g., warning notification apps for iPhone, Android, Blackberry, iPads):

> **AUX-005450.a** [**Required**] The applications shall provide audio and visual warning notifications to the user of the mobile device.
>
> **AUX-005450.b** [**Required**] The applications shall provide for user response.
>
> **AUX-005450.c** [**Required**] The applications shall use device location (subject to all applicable privacy rules) to perform real-time, location-based alert targeting and tag user alert responses with real-time location information.

3.5.8 Event Sources

AUX-005460 [**Required**] For any particular event, operators having the requisite authorization shall be able to define that, upon notice of occurrence of the particular event by an event source, the MNWS is to implement one of the following behaviors:

a. The MNWS shall automatically trigger alert notification to target subscribers.
b. The MNWS shall test the event data against a predefined rule set, and, if the event conforms to the requirements of the rule set, then the MNWS shall trigger alert notification to target subscribers.
c. The MNWS shall test the event data against a predefined rule set, and, if the event conforms to the requirements of the rule set, then the event shall be reported to the authorized operators who in turn will decide the action to be taken.

3.5.8.1 External IP-Enabled Event Sources

AUX-005470 [**Required**] The MNWS shall support automatic activation by IP-enabled external sources (such as the National Weather Service, local and regional security forces Really Simple Syndication [RSS], and local and state emergency Common Alerting Protocol [CAP] feeds).

AUX-005480 [**Required**] The MNWS shall monitor external sources for new events. If an event from an external source meets predefined emergency criteria, then the default action is for the MNWS to inform operators of the event. The operators qualify the event and, when appropriate, initiate an alert to the pertinent target subscribers.

3.5.8.2 Internal IP-Enabled Event Sources

AUX-005490 [**Required**] The MNWS shall be capable of interfacing with internal IP-enabled event sources such as fire alarms, video surveillance, data collection systems, and chemical detectors.

AUX-005500 [**Required**] The MNWS shall monitor IP-enabled internal sources for new events. For any given IP-enabled internal event source, either the MNWS queries the event source to determine when an event occurs or the event source notifies the MNWS that an event has occurred, in which case the MNWS shall authenticate the alert before acting on it.

AUX-005510 [**Required**] For each IP-enabled internal event source, the MNWS shall specify either that the MNWS trigger an alert upon detection or notification of an event from the given source or that the MNWS process the event information from the given source against a predefined rule set such that an alert is triggered only when the event meets the criteria set forth in the rule set.

3.5.9 SMTP Delivery

AUX-005520 [**Required**] The MNWS shall include an SMTP server that sends outbound e-mail alerts to the installation's host SMTP servers which, in turn, employ SMTP relay to deliver the e-mail alerts to the set of target subscribers.

AUX-005530 [**Required**] The MNWS SMTP server shall do the following:

a. Send PKI-signed e-mail alerts to subscribers via host SMTP servers using SMTP relay.
b. Send e-mail alert cancellation messages to either a subset of subscribers or all subscribers as appropriate via host SMTP servers using SMTP relay.
c. Receive incoming e-mail responses (selecting one of multiple response options) from subscribers via host SMTP servers.

AUX-005540 [**Required**] The MNWS shall do the following:

a. Report e-mail alert delivery events.

b. Report on the operational status of the MNWS SMTP server.

AUX-005550 [**Required**] The MNWS SMTP server shall authenticate to the host SMTP server before sending outbound alert messages.

AUX-005560 [**Required**] The host SMTP server shall authenticate to the MNWS SMTP server before the MNWS server will accept inbound messages from the host SMTP server. Alternatively, incoming SMTP traffic may be routed directly to the MNWS SMTP server by designated multiplexer (MX) record.

3.5.10 External Delivery Systems and Services

3.5.10.1 Telephony Alerting Service

AUX-005570 [**Required**] The MNWS shall be capable of interfacing with external commercial telephone alerting services (i.e., "dialers") for the following purposes:

a. Sending telephony alerts to a set of target subscribers.

b. Canceling alerts to specific recipients or to all recipients.

c. Obtaining reports of event alert delivery and subscriber responses.

d. Obtaining reports of the operational status for the telephony alerting service.

AUX-005580 [**Required**] The connection between the MNWS and the external telephone alerting service shall be secured using Secure HTTP employing a two-way exchange of certificates or an alternative security protocol providing equivalent or better authentication, confidentiality, and integrity mechanisms.

AUX-005590 [**Required**] In order to instruct the telephony alerting service to send phone alerts, the MNWS shall provide the minimum set of data items necessary for telephony alert dissemination including user names, phone numbers, and (optionally) PINs for user authentication to the telephony alerting service.

AUX-005600 [**Required**] The telephony alerting service shall anonymize and then delete the contact information provided by the MNWS once the alert notification has been disseminated.

3.5.10.2 Short Message Service (SMS) Aggregation Service

AUX-005610 [**Required**] The MNWS shall be capable of interfacing with SMS aggregation services for the following purposes:

a. Sending text message alerts to a set of target subscribers.

b. Sending text messages canceling alerts to specific recipients or to all recipients.

c. Obtaining reports of event alert delivery and obtaining subscriber responses to text alerts (selecting one of multiple response options).

d. Obtaining reports of the operational status for the SMS aggregation service.

AUX-005620 [**Required**] The connection between the MNWS and the SMS aggregation service shall be secured using Secure HTTP employing a two-way exchange of certificates or an alternative security protocol providing equivalent or better authentication, confidentiality, and integrity mechanisms.

AUX-005630 [**Required**] In order to instruct the SMS aggregation service to send text alerts, the MNWS shall provide the minimum set of data items necessary including user names and SMS addresses (e.g., mobile phone numbers).

AUX-005640 [**Required**] The MNWS shall be capable of sending at least 10,000 SMS messages per minute.

3.5.10.3 Existing IP-Enabled Alert Delivery Devices

AUX-005650 [**Required**] The MNWS shall integrate with the existing IP-enabled alert delivery devices at the installation including telephony alerting systems associated with existing IP PBXs, IP-enabled Large Voice systems, LMRs, and digital displays.

AUX-005660 [**Required**] The MNWS shall be able to create RSS feeds that are delivered to RSS aggregators such as enterprise Web portals deployed at the installation.

AUX-005670 [**Required**] The MNWS shall support, at a minimum, XML, CAP, and RSS over secure HTTP in order to integrate with existing IP-enabled alert delivery devices.

AUX-005680 [**Required**] The MNWS shall interface with existing IP-enabled alert delivery devices for the following purposes:

a. Sending alerts to a set of target recipients.

b. Canceling an alert to a recipient or to all recipients.

c. Reporting event alert delivery and subscriber responses.

d. Reporting on the operational status of a delivery device.

3.5.10.4 Installed Unified Communication (UC) Systems

AUX-005690 [**Required**] The MNWS shall interface with installed UC systems in order to deliver alert notifications in the form of voice calls and instant messages, and by means of other collaboration products or capabilities available on the UC system that prove useful for disseminating alerts to the target subscribers.

NOTE: It is recognized that the MNWS will most likely need to employ different protocols and interface to a different set of APIs for each UC system. However, in each case, the communication between the MNWS and the UC system shall provide for authentication, authorization, integrity, and confidentiality.

AUX-005700 [**Required**] The MNWS shall do the following:

a. Send alerts to sets of recipients or devices.

b. Cancel a specific alert to a recipient or to all recipients.

c. Report on event alert delivery and subscriber responses.

d. Obtain the operational status for the UC system and the various functional components the MNWS is relying on to deliver the alerts.

e. In the event of a theater-wide alert, the MNWS shall have the capability to instruct the UC systems to initiate up to 10,000 simultaneous "99" phone calls theater-wide.

f. MNWS shall be compatible with the Installation Information Infrastructure Modernization Program (I3MP) selected system.

AUX-005710 [**Optional**] The UC system shall provide a panic button that enables subscribers to send real-time alerts to the MNWS. There shall be no indication or response in the subscriber's environment to the use of the panic button. The use of the panic button is by its very nature a secret act. The MNWS shall immediately notify authorized operators as to the specific panic button that has been activated, and the MNWS runs any pre-built alert notification scenarios designed for this event.

AUX-005720 [**Optional**] The UC system shall support remote viewing of Web cameras by UC display devices and by authorized operators logged into the MNWS.

AUX-005730 [**Optional**] The UC system shall support remote viewing of UC device cameras by authorized operators logged into the MNWS.

NOTE: This would occur only in the context of an emergency event.

3.5.10.5 Non-IP Delivery Systems

AUX-005740 [**Required**] The MNWS shall interface with the legacy non-IP delivery systems located at an installation such as non-IP Giant Voice systems, public address (PA) systems, and non-IP land mobile radio systems.

AUX-005750 [**Required**] The MNWS shall interface with the non-IP delivery systems for the following purposes:

a. Sending alerts.

b. Canceling alerts.

c. Reporting on alert delivery status.

d. Reporting on the status of the non-IP delivery system.

AUX-005760 [**Required**] The MNWS shall connect to the non-IP delivery devices using legacy physical interfaces such as the following:

a. Serial interface (RS-232, RS-485).

b. Dry contacts.

c. Audio-out.

d. Dual-Tone Multifrequency (DTMF).

3.5.10.6 Integration With Giant Voice Systems

AUX-005770 [**Required**] The MNWS shall be able to connect with an installation's IP and non-IP Giant Voice systems:

a. In case of IP-based integration, the Giant Voice system and the APIs on both systems shall comply with all required information assurance certifications.

b. In case of non-IP integration, the requirements of Section 3.5.10.5, Non-IP Delivery System, shall apply.

AUX-005780 [**Required**] The MNWS integration with Giant Voice systems shall not replace the existing Giant Voice activation method, but rather augment it for unified notification scenarios.

AUX-005790 [**Required**] The MNWS integration with Giant Voice systems shall enable authorized operators to specify the message to be activated, including pre-recorded voice/tone and text-to-speech:

a. If a Giant Voice system supports activation of specific zones/speakers, then authorized MNWS operators shall have the ability to activate specific zones/speakers of the Giant Voice system.

AUX-005800 [**Required**] The MNWS integration with Giant Voice systems shall comply with the Unified Facilities Criteria (UFC) requirements for Mass Notification Systems (MNS) integration.

3.5.10.7 Integration With Indoor Voice Systems

AUX-005810 [**Required**] The MNWS shall be able to connect with an installation's IP and non-IP Indoor Voice systems:

a. In case of IP-based integration, the Indoor Voice system and the APIs on both systems shall comply with all required information assurance certifications.

b. In case of non-IP integration, the requirements of Section 3.5.10.5, Non-IP Delivery System, shall apply.

AUX-005820 [**Required**] The MNWS integration with Indoor Voice systems shall not replace the existing Indoor Voice activation method, but rather augment it for unified notification scenarios.

AUX-005830 [**Required**] The MNWS integration with Indoor Voice systems shall enable authorized operators to specify the message to be activated, including pre-recorded voice/tone and text-to-speech:

a. If an Indoor Voice system supports activation of specific zones/speakers, then authorized MNWS operators shall have the ability to activate specific zones/speakers of the Indoor Voice system.

b. Authorized MNWS operators shall have the ability to activate the strobe lights (if available).

AUX-005840 [**Required**] The MNWS integration with Indoor Voice systems shall comply with the UFC requirements for MNS integration.

3.5.10.8 Integration With Fire Alarm Systems

AUX-005850 [**Required**] The MNWS shall be able to connect with an installation's IP and non-IP Fire Alarm systems:

a. In case of IP-based integration, the Fire Alarm system and the APIs on both systems shall comply with all required information assurance certifications.

b. In case of non-IP integration, the requirements of Section 3.5.10.5, Non-IP Delivery System, shall apply.

AUX-005860 The MNWS integration with Fire Alarm systems shall not replace the existing Fire Alarm activation method, but rather augment it for unified notification scenarios

AUX-005870 The MNWS integration with Fire Alarm systems shall enable authorized operators to specify the message to be activated, including pre-recorded voice/tone and text-to-speech:

a. If a Fire Alarm system supports activation of specific zones/speakers, then authorized MNWS operators shall have the ability to activate specific zones/speakers of the Fire Alarm system.

b. Authorized MNWS operators shall have the ability to activate the strobe lights (if available).

AUX-005880 The MNWS integration with Fire Alarm systems shall comply with the UFC requirements for MNS integration and with National Fire Protection Association (NFPA) 72, National Fire Alarm and Signaling code.

3.6 E911 MANAGEMENT SYSTEM

Standalone E911 Management Systems are UC appliances that enable a reliable user location to be provided to emergency response dispatch centers when a 911 call is made from a UC EI.

3.6.1 Scope, Assumptions, and Terms

As illustrated in Figure 3.6-1, E911 Management System Architecture for UC E911 Services, E911 Management Systems are intended to support wireline E911 service, including support for UC subscribers using softphones and subscribers connected via wireless LAN interfaces, such as Institute of Electrical and Electronics Engineers (IEEE) 802.11b/g/n.

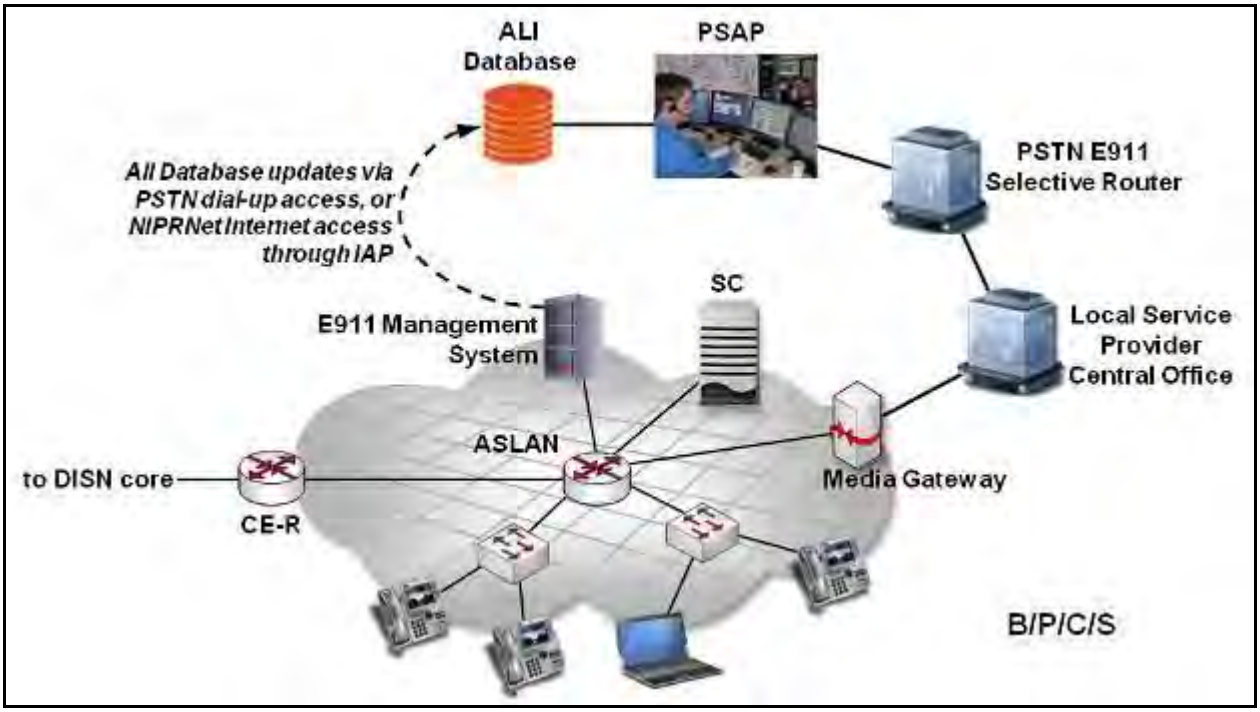


Figure 3.6-1. E911 Management System Architecture for UC E911 Services

Public Safety Answering Point (PSAP) is the term used in these requirements for any emergency response dispatch center that is a terminating point for a 911 call, including those operated by a DoD Component.

The term Automatic Location Identification (ALI) database is used for any database of location information queried by a PSAP to determine the location of a 911 caller, regardless of who operates the database or of the database's implementation details.

As shown in Figure 3.6-2, Illustrative ALI Database Records, each record in an ALI database is assumed to include, at a minimum, a location—composed of a street address and Emergency Response Location (ERL)—and an associated Emergency Location Identification Number (ELIN). An ERL identifies a specific physical location, area, or zone at the street address to which an emergency responder can be sent; e.g., the northeast quadrant of the third floor. An ELIN is a 10-digit telephone number that uniquely identifies the location (i.e., each ELIN is associated with one and only location).

NOTE: It is possible to have multiple ELINs assigned to a given ERL. Multiple ELINs per ERL allows for concurrent callbacks to multiple 911 callers from the same location.

Location Name	Street Address	ERL	ELIN
Joint Base ABC	123 Main St. Salem IL	3FL NE	618-555-1212
Joint Base ABC	123 Main St. Salem IL	3FL SE	618-555-1213
Joint Base ABC	123 Main St. Salem IL	3FL SW	618-555-1214
Joint Base ABC	123 Main St. Salem IL	3FL SW	618-555-1227
Joint Base ABC	123 Main St. Salem IL	3FL SW	618-555-1241
etc.			

Figure 3.6-2. Illustrative ALI Database Records

A PSAP attempts to match the calling party number received with an ELIN in the ALI database. If there is a match, then the associated street address/ERL information is used as the location of the 911 caller. Properly constructed and maintained ALI databases enable reliable location information to be determined based on the calling party number.

These requirements assume that a default response or behavior can be configured in the E911 Management System for circumstances when a precise location for an EI cannot be determined. One possible approach is to define and maintain a Default Location ALI database entry for each SC. The Default Location, and associated ELIN, would identify a location to which emergency responders can be sent in these circumstances.

Base/post/camp/station (B/P/C/S) 911 services supported by E911 Management Systems should comply with Federal, state, and local 911 regulations for the regions where these systems are deployed. This compliance may require additional capabilities beyond what is required in this section. For example, state and local agencies serving a B/P/C/S location may impose certain rules regarding the format of location and ELIN data stored in their ALI databases.

3.6.2 General E911 Management System

AUX-005890 [**Required: E911 Management System**] The E911 Management System shall support signaling interfaces to UC SC products from at least two different vendors, and shall use these interfaces for signaling with those SCs.

NOTE: A system that interoperates with only a single SC can be certified as part of the SC, but, since it has not demonstrated multivendor interoperability, it cannot be certified as a standalone product.

AUX-005900 [**Conditional: E911 Management System**] If the UC SC product supports one or more proprietary signaling interface for E911 Management System interconnection, then the E911 Management System shall support at least one of these interfaces, per the SC vendor's proprietary interface specifications.

AUX-005910 [**Conditional: E911 Management System**] If the UC SC product supports one or more standardized signaling interface for E911 Management System interconnection, then the E911 Management System shall support at least one of these interfaces, per standardized interface specifications identified by the SC vendor.

3.6.3 Automatic Location Identification (ALI) Information

AUX-005920 [**Required: E911 Management System**] The E911 Management System shall maintain, for each SC to which it interfaces, an appropriate set of location data and corresponding ELINs that identify the physical locations of each of the EIs served by the SC.

NOTE: The level of detail in the location data depends on the B/P/C/S or enclave's E911 wiremap and the approach chosen by the 911 administrator for mapping physical locations to ERLs.

AUX-005930 [**Required: E911 Management System**] The E911 Management System shall also maintain any additional data items required by the ALI databases supporting the PSAPs serving the B/P/C/S or enclave. These PSAPs are responsible for handling 911 calls from the EIs served by the SCs to which the E911 Management System interfaces.

NOTE: Sources for the ALI data maintained by the E911 Management System may include the SCs with which it interfaces, SC service provisioning systems, and direct manual entry.

AUX-005940 [**Required: E911 Management System**] The E911 Management System shall be capable of exporting, to a file, ALI data in .csv or National Emergency Number Association (NENA), Version 2.0 or later, formats.

AUX-005950 [**Conditional: E911 Management System**] If the B/P/C/S or enclave requires that ALI data be provided in a proprietary format, then the E911 Management System shall be capable of exporting, to a file, the ALI data in the required proprietary format.

AUX-005960 [**Conditional: E911 Management System**]If the E911 Management System supports direct, secure electronic transfer of ALI data to a target ALI database (or to an intermediary application or service that in turn updates the ALI database), and the B/P/C/S or enclave supports and allows such a transfer, then a direct electronic export of ALI data shall be allowed in lieu of exporting the data to a file.

AUX-005970 [**Required: E911 Management System**] The E911 Management System shall be capable of exporting ALI data:

a. On a periodic, scheduled basis.
b. In response to a configurable event (i.e., the creation of a new ERL and ELIN in the system).
c. In response to an administrator's request, on an ad hoc basis.

3.6.4 End Instrument Location at Registration

AUX-005980 [**Conditional: E911 Management System**] If the SC provides notification of EI registrations, then the E911 Management System shall do all of the following when notified of an EI registration:

a. Determine the physical location of the EI, based on IP address assigned to the EI and any additional information provided by the SC at registration notification.

b. Determine the ERL assigned to that location.

c. Keep an internal record of the EI registration that includes the ELIN for the ERL assigned to the EI's location.

d. Acknowledge receipt of the registration notification to the SC, and include the EI's ELIN in that acknowledgement.

AUX-005990 [**Conditional: E911 Management System**] If the EI directly provides notification of registration, then the E911 Management System shall do all of the following when notified of an EI registration:

a. Determine the physical location of the EI, based on IP address assigned to the EI and any additional information provided by the EI at registration notification.

b. Determine the ERL assigned to that location.

c. Keep an internal record of the EI registration that includes the ELIN for the ERL assigned to the EI's location.

How the E911 Management System determines the physical location of a registered EI is not specified in these requirements. It is allowed to use network endpoint discovery techniques, it may reference an internally maintained mapping of IP addresses to locations/zones, or it may use some other approach provided that the B/P/C/S or enclave fully supports the approach used.

The message flow at EI registration is shown in Figure 3.6-3, Message Flow at EI Registration.

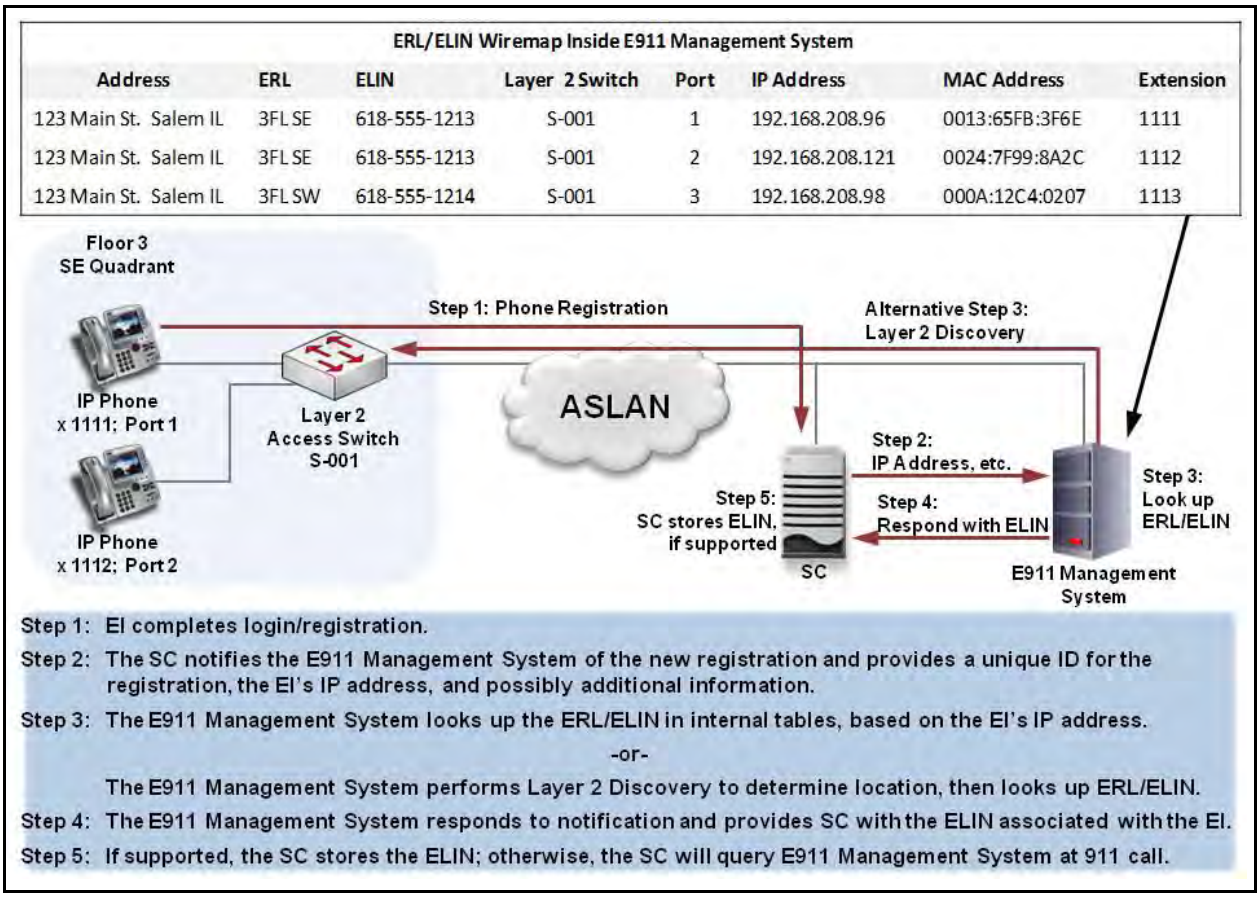


Figure 3.6-3. Message Flow at EI Registration

AUX-006000 [**Required: E911 Management System**] When the E911 Management System is unable to determine the location of a registered EI, it shall perform the configured default behavior for this circumstance.

NOTE: The ELIN associated with an EI, as determined by the E911 Management System, will be used by the SC as the calling party number in the event that a 911 call is made from that EI while it is registered with the SC. The SC shall maintain the ELIN received in the notification acknowledgement or it shall query the E911 Management System for the ELIN as part of processing a 911 call. The 911 call flows are illustrated in Figure 3.6-4.

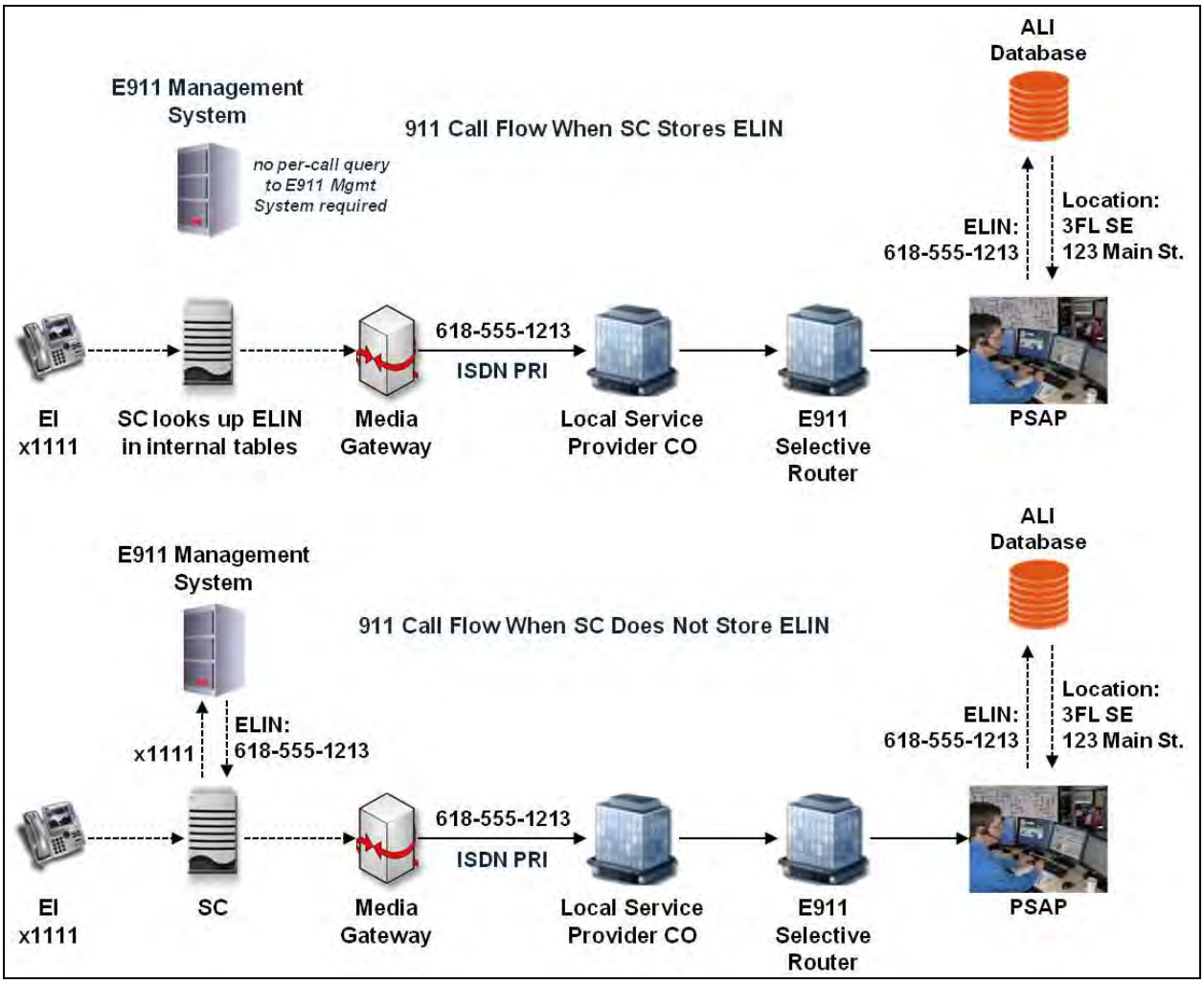


Figure 3.6-4. 911 Call Flows

3.6.5 Support for ELIN Query at 911 Call

AUX-006010 [**Required: E911 Management System**] When queried by an SC processing a 911 call from a registered EI, the E911 Management System shall provide the SC with the ELIN associated with that EI in its internal record.

3.6.6 SC Interfaces With E911 Management Systems

SCs are not required to support interfaces to standalone E911 Management Systems. The burden is on the E911 solution to interface to the SC.

If an SC does support interfaces to E911 Management Systems, then the requirements in this section apply. Furthermore, the requirements in this section apply only to SCs that are connected to an active E911 Management System.

AUX-006020 [**Conditional: SC**] If the SC proides notification of EI registrations to the E911 Management System, then the SC shall notify the E911 Management System whenever an EI registers with the SC and provide the EI's IP address and a unique identifier for the registration to the E911 Management System with the registration notification.

AUX-006030 [**Optional: SC**]The SC shall provide additional information, such as the EI's Move, Add, Change (MAC) address, to the E911 Management System with EI registration notification.

AUX-006040 [**Conditional: SC**] If the SC supports receiving and storing, at the EI level, an ELIN provided by an E911 Management System in a response message to a registration notification, then the SC shall do the following:

a. Receive the ELIN provided and store it as part of the information maintained for that EI with respect to the registration process.

b. Populate the Calling Party Number information element in the ISDN PRI setup message that is sent over the commercial PRI from the SC's MG to the PSTN, with that ELIN, if a 911 call is made from that EI.

   If the E911 Management system does not respond to an EI's registration notification, or does not provide a valid ELIN in its response, and a 911 call is made from that EI, then the SC shall populate the Calling Party Number information element with the ELIN configured to identify the Default Location for that SC.

AUX-006050 [**Conditional: SC**] If the SC supports querying an E911 Management System during 911 call processing in order to determine the ELIN for the EI from which the 911 call was made, then the SC shall do the following:

a. Request the E911 Management System to provide the ELIN for that EI, based on the unique identifier for that EI provided at registration notification.

b. The SC shall receive the ELIN provided by the E911 Management System, and populate the Calling Party Number information element in the ISDN PRI setup message, that is sent over the commercial PRI from the SC's MG to the PSTN, with that ELIN.

   If the E911 Management system does not provide a valid ELIN within a configurable time period, then the SC shall use the ELIN that was configured to identify the Default Location for that SC as the Calling Party Number information element.

AUX-006060 [**Required: SC**] If a 911 call is made from an unregistered EI, then the SC shall populate the Calling Party Number information element in the ISDN PRI setup message that is sent over the commercial PRI from the SC's MG to the PSTN, with an ELIN provided by the E911 Management System (either at EI registration or when the 911 call is made) per the default behavior configured in the E911 Management System for this circumstance.

3.6.7 On-Site Notification of 911 Call

AUX-006070 [**Conditional: E911 Management System, SC**] If the E911 Management System supports notification of a 911 call to a configurable entity within the B/P/C/S or enclave other than a PSAP, such as a front desk or security command center, and the SCs to which the E911 Management System interfaces support notifying the E911 Management System when processing a 911 call, then the E911 Management System shall provide a notification message to a configured non-PSAP entity when a 911 call is made.

NOTE: This requirement does not specify how the notification is done, nor does it specify what the content of notification message is. Allowed notification methods include automated voice call, email, and text messaging. A solution that is integrated with a front desk or security command center monitoring system would be expected to support screen pop-ups or other messaging mechanisms provided by the monitoring system. An integrated solution may also support 911 call monitoring from a front desk or security command center.

3.6.8 IPv6 Support

AUX-006080 [**Required: E911 Management System**] Conformant with Section 5, IPv6, the E911 Management System shall support dual IPv4 and IPv6 stacks (i.e., support both IPv4 and IPv6 in the same IP end point) as described in RFC 4213.

AUX-006090 [**Required: E911 Management System**] The E911 Management System shall meet all of the IPv6 protocol requirements for Network Appliances and Simple Servers (NA/SS) products in Section 5, IPv6, including the requirements in Table 5.2-4, UC Network Appliances and Simple Servers (NA/SS).

3.6.9 Information Assurance

AUX-006100 [**Required: E911 Management System**] E911 Management Systems shall meet the Information Assurance requirements of all applicable DISA STIGs.

3.6.10 OAM&P

AUX-006110 [**Required: E911 Management System**] The E911 Management System shall allow an administrator to read, add, delete, and modify the ERL/ELIN entries maintained in the system.

AUX-006120 [**Conditional: E911 Management System**] If the E911 Management System interfaces with SCs, then it shall allow an administrator to configure authentication credentials so that the system can authenticate the SCs to which it interfaces, and the SCs can authenticate the E911 Management System.

AUX-006130 [**Conditional: E911 Management System**] If the E911 Management System supports direct, secure electronic transfer of ALI data to a target ALI database, then the E911 Management System shall allow an administrator to configure the address of an ALI database, along with authentication credentials, so that the system can authenticate the ALI database and the ALI database can authenticate the E911 Management System.

Note that, in this requirement, "target ALI database" means the database proper, or any intermediary application or service that in turn updates the target ALI database.

3.7 CUSTOMER PREMISES EQUIPMENT

3.7.1 General Description

A wide variety of customer premises equipment (CPE) manufactured and sold by many sources was connected to the line (subscriber) side of a DSN switching system. Such varieties include industry "American National Standards Institute – European Telecommunications Standards Institute (ANSI-ETSI) Standards" based digital and analog devices, and non-standards based proprietary digital devices. During the transition period between TDM and IP-based technologies, some locations may have a requirement to interface the legacy CPE to an SC. As a result, most SC vendors provide an optional Integrated Access Device (IAD) to permit the use of CPE until it is replaced.

The CPE devices may include answering machines, voice mail systems, automated call distributors, proprietary telephone sets, standards-based telephone sets, facsimile machines, voice-band modems, ISDN Network Termination 1 (NT1) devices and Terminal Adapters (TAs), and certain devices that are deemed mandatory for local or host nation telecommunications network compliance (i.e., 911 emergency service).

3.7.2 Requirements

All CPE devices are required to meet the following requirements:

AUX-006140 [**Conditional**] If a CPE device supports MLPP, then that device shall do so in accordance with the requirements listed in Section 2.25.2, Multilevel Precedence and Preemption, and shall not affect the DSN interface features and functions associated with line supervision and control.

AUX-006150 [**Required**] All DSN CPE, at a minimum, must meet the requirements of Part 15 and Part 68 of the Federal Communications Commission (FCC) Rules and Regulations, and the Administrative Council for Terminal Attachments (ACTA).

AUX-006160 [**Conditional**] If a CPE device supports autoanswer, then that device shall have an "autoanswer" mode feature allowing the autoanswer mode to be set to a "time" more than the equivalency of four ROUTINE precedence ring intervals, in accordance with Section 2.25.2, Multilevel Precedence and Preemption, before "answer" supervision is provided.

AUX-006170 [**Conditional**] If a CPE device is required to support precedence calls above ROUTINE precedence, then that device shall respond properly to an incoming alerting (ringing) precedence call cadence, as described in Section 2.9.1.2.1, UC Ringing Tones, Cadences, and Information Signals.

AUX-006180 [**Conditional**] If a CPE device can "out dial" DTMF and/or dial pulse (DP) digits (automatic and/or manual), then that device shall comply with the requirements as specified in Telcordia Technologies GR-506-CORE, LSSGR: Signaling for Analog Interfaces, Issue 1, June 1996, paragraph 10. That device shall also be capable of outpulsing and interpretation of DTMF digits on outgoing and two-way trunks as specified in Telcordia Technologies GR-506-CORE, LSSGR: Signaling for Analog Interfaces, Issue 1, June 1996, paragraph 15, and Table 3.7-1.

Table 3.7-1. DTMF Generation and Reception From Users and Trunks

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

AUX-006190 [**Conditional**] If a CPE device contains a modem or facsimile machine, then that modem or facsimile machine shall be compatible with ITU and Telcordia standards, as applicable.

AUX-006200 [**Conditional**] If a CPE device contains a facsimile device, then that facsimile device, at a minimum, shall meet the requirements in accordance with applicable DoD Information Technology (IT) Standards Registry (DISR) standards.

AUX-006210 [**Conditional**] If Configuration Management and/or Fault Management is provided by the CPE device so that it can be managed by the Advanced DSN Integrated Management Support System (ADIMSS) or other management systems, then the management information for that CPE device shall be provided by one or more of the following serial or Ethernet interfaces:

a. Serial interfaces shall be in accordance with one of the following standards:

   (1) ITU-T Recommendation V.35.

   (2) TIA-232-F.

   (3) EIA-449-1.

   (4) TIA-530-A.

b. Ethernet interfaces shall be in accordance with IEEE 802.3-2002.

AUX-006220 [**Conditional**] If a CPE device supports 911 and E911 emergency services, then, at a minimum, the 911 and the E911 (tandem) emergency services shall have the capability to "hold" (prevent) the originating subscriber or caller from releasing the call, via the "switch supervision interaction for line and trunk control by the called party" feature, in accordance with Telcordia Technologies GR-529-CORE. Additionally, the FCC regulations regarding 911 and E911 must be considered.

3.8 DoD SECURE COMMUNICATIONS DEVICES

3.8.1 General Description

This section describes the requirements that will be used to certify DoD Secure Communications Devices (DSCDs) when directly connected to or otherwise traversing the DSN, PSTN, or DRSN Gateway to or from the DSN.

This section applies to the secure mode operation of any DSCD that either directly connects to the DSN, the PSTN, or the DRSN Gateway or traverses these networks in the course of conducting a secure communications session, regardless of where the telephone call originates or terminates. The certification test environment for DSCDs shall include configurations that realistically simulate fixed networks (i.e., DSN, DRSN via the DSN Gateway, PSTN) and deployed networks, such as digital voice exchange (DVX) systems and other configurations as defined by the Executive Agent for Theater Joint Tactical Networks, or any combination thereof.

3.8.2 Requirements

The JITC will validate all the features and capabilities of a DSCD device, including voice, data, and facsimile transmission.

AUX-006230 [**Required: STE Enabled DSCD, FNBDT/SCIP Enabled DSCD**] The enabled DSCD shall be only those that are type approved by the National Security Agency (NSA) and are listed on the NSA Secure Product Web site. Each DSCD must support at least one NSA-approved secure protocol. If the DSCD supports more than one secure protocol, then it must meet all the requirements for at least one of the secure protocols and must minimally support the other protocols that are provided on the DSCD.

AUX-006240 [**Required: STE Enabled DSCD, FNBDT/SCIP Enabled DSCD**] The DSCD devices that use a two-wire analog or basic rate interface (BRI) shall meet the EI requirements as specified in Section 3.7, Customer Premises Equipment. The DSCD devices that use an IP interface shall meet the EI requirements as specified in Section 2, Session Control Products, of UCR 2013. DSCD devices that support DSN trunk interfaces [PRI or IP (AS-SIP)] shall meet the interface requirements defined in the following:

a. Section 2, Session Control Products, MG Support for ISDN PRI Trunks, of UCR 2013, for PRI.

b. AS-SIP 2013 document for AS-SIP.

AUX-006250 [**Required: STE Enabled DSCD, FNBDT/SCIP Enabled DSCD**] A DSCD device that supports one of the required signaling modes shall interoperate with and establish secure sessions with other compatible devices with at least an 85 percent secure call completion rate.

AUX-006260 [**Required: STE Enabled DSCD, FNBDT/SCIP Enabled DSCD**] The DSCD shall be capable of using the protocol(s) provided to establish a secure session within 60 seconds and must maintain secure communications for the duration of the secure portion of the call.

AUX-006270 [**Required: STE Enabled DSCD, FNBDT/SCIP Enabled DSCD**] The DSCD shall operate in a network that has an E2E latency of up to 600 milliseconds.

AUX-006280 [**Required: STE Enabled DSCD, FNBDT/SCIP Enabled DSCD**] The DSCD shall achieve and maintain a secure voice connection with a minimum MOS of 3.0.

AUX-006290 [**Required: STE Enabled DSCD, FNBDT/SCIP Enabled DSCD**] Once connected to the rekey center, the DSCD shall obtain a new key and properly process that new key with a 95 percent rekey completion rate.

AUX-006300 [**Conditional: STE Enabled DSCD, FNBDT/SCIP Enabled DSCD**] If the DSCDs can establish secure sessions on a Continuously Variable Slope Delta (CVSD) switch and terminate on a CVSD switch without ever traversing or otherwise interacting with the DSN, DRSN, or PSTN, then that DSCD must do so with a 50 percent completion rate.

AUX-006310 [**Conditional: FNBDT/SCIP Enabled DSCD**] If the DSCDs can establish secure sessions on IP networks using Future Narrowband Digital Terminal (FNBDT)/Secure Communications Interoperability Protocol (SCIP), then that DSCD shall satisfy all the DSCD end point requirements described in NSA documents SCIP-215 and SCIP-216.

AUX-006320 [**Required: STE Enabled DSCD, FNBDT/SCIP Enabled DSCD**] The DSCD devices shall support a minimum data rate and facsimile transmission rate of 9.6 kbps.

3.9 UC COLLABORATION PRODUCT

3.9.1 Description

This section describes the Minimum Essential Requirements (MERs), Contitional Requirements, and Optional Requirements for the Collaboration Product (CP). The CP supports collaboration between IP-based end users using VVoIP sessions, Presence/IM/Chat sessions, and other collaborative sessions such as Whiteboard Sharing, Document Sharing, and virtual meetings.

This section focuses on the MERs, Conditional Requirements, and Optional Requirements for VVoIP sessions and Presence/IM/Chat Sessions provided by CPs. Other collaborative sessions provided by CPs are outside the scope of this section.

The requirements in this section assume that the high-level architecture for the CP contains the following functions or components:

- CP Clients (Collaboration software which runs on end-users' computers or smartphones).
- CP Server (Provides VVoIP and Presence/IM/Chat services to the CP Clients).
- CP MG (Gives the CP Clients and CP Server access to the DSN and the PSTN).
- CP SBC (Gives the CP Clients and CP Server access to an SC in the UC Network).

These requirements also assume that the System Under Test (SUT) for the CP contains at least two ~~all four~~ of these functions or components: the CP Clients and the CP Server. For VVoIP collaboration sessions, the role of the CP Client is similar to the role of the EI in the UC Network, and the role of the CP Server is similar to the role of the SC in the UC Network.

Most of the CP MG and the CP SBC requirements are Contitional, the rest of the CP MG and the CP SBC requirements are Optional.

The Conditional CP MG requirements are Conditional on CP support for TDM calls entering and leaving the CP enclave, via TDM interfaces (e.g. ISDN PRIs) from the CP MG to the DSN and/or the PSTN.

The Conditional CP SBC Requirements are Conditional on CP support for VVoIP calls entering and leaving the CP enclave, via an AS-SIP interface from the CP SBC to a Session Controller.

All the requirements in this section apply to the CP as a whole. In some cases, the CP requirements are marked as "[**Required: CP Client**]," "[**Required: CP Server**]," "[~~**Required**~~**Conditional: CP MG**]," or "[~~**Required**~~**Conditional: CP SBC**]", to show which CP function the requirement applies to.

3.9.2 Voice and Video Collaboration Product Requirements

3.9.2.1 Point-to-Point Voice Calls Between Collaboration Product Clients

AUX-006330 [**Required: CP**] The CP shall support the establishment of point-to-point Voice over IP (VoIP) calls between CP Clients that are served by the CP Server. The CP shall allow one CP Client to set up a point-to-point VoIP call with another CP Client. The CP shall allow the first CP Client to call the second CP Client by entering the second Client's phone number, by entering the second Client's username, or by looking up the second Client in a User Directory on the CP Server.

3.9.2.2 Add Voice Call to Existing Collaboration Session

AUX-006340 [**Required: CP**] When two CP Clients have an existing Collaboration session established through the CP Server (e.g., a Presence/IM/Chat session, a whiteboard session, or a document sharing session), the CP shall allow either one of the CP Clients to add a VoIP call

with the other CP Client to that existing session. The CP shall also allow either of the CP clients to later drop the VoIP call from that session, returning the session to its original type (e.g., Presence/IM/Chat, whiteboard, or document sharing).

3.9.2.3 Point-to-Point Video Calls Between Collaboration Product Clients

AUX-006350 [**Required: CP**] The CP shall support the establishment of point-to-point Video over IP calls between CP Clients that are served by the CP Server. The CP shall allow one CP Client to set up a point-to-point Video over IP call with another CP Client. The CP shall allow the first CP Client to call the second CP Client by entering the second Client's phone number, entering the second Client's username, or looking up the second Client in the User Directory on the CP Server.

3.9.2.4 Add Video Call to Existing Collaboration Session

AUX-006360 [**Required: CP**] When two CP Clients have an existing Collaboration Session established through the CP Server (e.g., a Presence/IM/Chat session, a whiteboard session, or a document sharing session), the CP shall allow either one of the CP Clients to add a Video over IP call with the other CP Client to that existing session. The CP shall also allow either of the CP clients to later drop the Video over IP call from that session, returning the session to its original type (e.g., Presence/IM/Chat, whiteboard, or document sharing).

3.9.2.5 Proprietary Client ⇔ Server Signaling and Client ⇔ Client Media

AUX-006370 [**Required: CP Client, CP Server**] For VoIP sessions between CP Clients, the CP Client and the CP Server shall support the establishment and tear-down of the VoIP sessions, using signaling messages that are proprietary to the CP.

AUX-006380 [**Required: CP Client, CP Server**] For Video over IP sessions between CP Clients, the CP Client and the CP Server shall support the establishment and tear-down of the Video over IP sessions, using signaling messages that are proprietary to the CP.

AUX-006390 [**ConditonalRequired: CP Server, CP MG**] For If Voice calls that traverse the CP MG, then the CP Server and the CP MG shall support the establishment and tear-down of the VoIP sessions between the Server and the MG, using signaling messages that are proprietary to the CP.

AUX-006400 [**ConditonalRequired: CP Server, CP SBC**] For If Voice calls that traverse the CP SBC, then the CP Server and the CP SBC shall support the establishment and tear-down of the VoIP sessions between the Server and the SBC, using signaling messages that are proprietary to the CP.

AUX-006410 [**ConditonalRequired: CP Server, CP SBC**] For If Video calls that traverse the CP SBC, then the CP Server and the CP SBC shall support the establishment and tear-down of

the Video over IP sessions between the Server and the SBC, using signaling messages that are proprietary to the CP.

Support for AS-SIP signaling over TLS within the CP (i.e., between one product component and another) is not required. Support for commercial SIP signaling over TLS within the CP is allowed but is not required. Since different product vendors generally support different versions of commercial SIP signaling, commercial SIP signaling is treated as proprietary signaling here.

AUX-006420 [**Required: CP Client**] For VoIP sessions between CP Clients, the Clients shall support the exchange of VoIP media packets, using media protocols that are proprietary to the CP. Support of industry-standard media protocols is also allowed.

AUX-006430 [**Required: CP Client**] For Video over IP sessions between CP Clients, the Clients shall support the exchange of Video over IP media packets, using media protocols that are proprietary to the CP. Support of industry-standard media protocols is also allowed.

AUX-006440 [**ConditonalRequired: CP Client, CP MG**] For If Voice calls that traverse the CP MG, then the CP Client and the CP MG shall support the exchange of VoIP media packets, using media protocols that are proprietary to the CP. Support of industry-standard media protocols is also allowed.

AUX-006450 [**ConditonalRequired: CP Client, CP SBC**] For If Voice calls that traverse the CP SBC, then the CP Client and the CP SBC shall support the exchange of VoIP media packets, using media protocols that are proprietary to the CP. Support of industry-standard media protocols is also allowed.

AUX-006460 [**ConditonalRequired: CP Client, CP SBC**] For If Video calls that traverse the CP SBC, thenthe CP Client and the CP SBC shall support the exchange of Video over IP media packets, using media protocols that are proprietary to the CP. Support of industry-standard media protocols is also allowed.

Support for SRTP-based media within the CP (i.e., between one product component and another) is allowed, but is not required. Examples of SRTP-based media are G.711 over SRTP and G.729 over SRTP for VoIP sessions, and H.263 over SRTP and H.264 over SRTP for Video sessions. The SRTP-based media within the CP can be either industry-standard media (such as the aforementioned G.7XX and H.26X media), or non-standard media that is proprietary to the CP.

3.9.2.6 Local Directory Service for Collaboration Product Users

AUX-006470 [**Required: CP**] The CP shall provide a Local Directory Service (LDS) for the CP users (the end users of the CP Clients and the CP Server). The LDS shall allow the CP users to look up information about each other based on the users' Name, Phone Number, and E-mail Address values.

AUX-006480 [**Required: CP**] The CP LDS shall support the following functions:

AUX-006480.a [**Required: CP]** The CP shall support a Directory Look-Up function that shall allow a user assigned to a CP to look up the telephone numbers of other users assigned to (i.e., served by) that CP. This function is referred to as "white pages" service, and it should not be confused with the CP routing tables, which are used for handling collaboration requests.

AUX-006480.b [**Required: CP**] For security reasons, the Directory Look-Up function shall be available only from a user's CP Client and not from other user devices outside the CP.

AUX-006480.c [**Required: CP**] The CP shall allow the system administrator to update the "white pages" directory database in response to subscriber data changes (i.e., subscriber adds, modifications, or removals). The CP shall update the white pages data automatically whenever ~~the~~ a subscriber's information is updated.

3.9.2.7 IPv6 Support

The source for the IPv6 Support Requirements for CP Clients and CP Servers is Section 5, IPV6.

AUX-006490 [**Required: CP Client**] The CP Client shall meet all of the IPv6 protocol requirements for End Instrument (EI) products in Section 5, IPv6, including the requirements in Table 5.2-3, UC EIs. This includes EI Conditional Requirements, when the Condition specified for the EI also applies to the CP Client.

AUX-006500 [**Required: CP Server**] The CP Server shall meet all the IPv6 protocol requirements for Network Appliances and Simple Servers (NA/SS) products in Section 5, IPv6, including the requirements in Table 5.2-4, UC Network Appliances and Simple Servers (NA/SS). This includes NA/SS Conditional Requirements, when the Condition specified for the NA/SS also applies to the CP Server.

3.9.2.8 QoS for Video over IP and VoIP Sessions

AUX-006510 [**Required: CP Client, CP Server; Conditonal:~~,~~ CP MG, CP SBC**] The CP Client, CP Server, CP MG (if included), and CP SBC (if included) shall provide Quality of Service (QoS) for VoIP sessions and Video over IP Sessions, through the setting of Differentiated Services Code Points (DSCPs) in VVoIP signaling streams and VVoIP media streams.

AUX-006520 [**Optional: CP Client, CP Server, CP MG, CP SBC**] CP support for the VVoIP Signaling and Media DSCPs, specified in Section 6.3.2 and Table 6.3.2, Traffic Conditioning Specification, is optional but not required. Examples of VVoIP Signaling and Media DSCPs follow:

- User Signaling DSCP 40 (Base 10).
- Non-Assured Voice DSCP 46 (Base 10).

- Broadcast Video DSCP 24 (Base 10).

CP support for Table 6.3.2 DSCPs associated with Priority and Precedence is not required.

3.9.2.9 Information Assurance

AUX-006530 [**Required: CP]** The CP and its components shall meet the Information Assurance requirements of all applicable DISA STIGs.

NOTE: The number of STIGs that would apply to a vendor's CP is dependent on the architecture of the CP System Under Test (SUT) that the vendor submits for certification. For example, when the CP supports VVoIP services, the DISA VVoIP STIG would apply.

3.9.2.10 SNMP v3 Alarms for Remote Monitoring

AUX-006540 [**Required: CP Server; Conditional: ~~,~~ CP MG, CP SBC**] The CP Server, CP MG (if included), and CP SBC (if included) shall support generation and transmission of Simple Network Management Protocol (SNMP) version 3 (SNMPv3) alarms for remote monitoring.

AUX-006550 [**Required: CP Server; Conditional: ~~,~~ CP MG, CP SBC**] The CP Server, CP MG (if included), and CP SBC (if included) shall generate alarm messages that are distinguishable from administrative log messages.

AUX-006560 [**Required: CP Server; Conditional: ~~,~~ CP MG, CP SBC**] The CP Server, CP MG (if included), and CP SBC (if included) shall detect their own fault (alarm) conditions.

AUX-006570 [**Required: CP Server; Conditional: ~~,~~ CP MG, CP SBC**] The CP Server, CP MG (if included), and CP SBC (if included) shall generate alarm notifications.

AUX-006580 [**Required: CP Server; Conditional: ~~,~~ CP MG, CP SBC**] The CP Server, CP MG (if included), and CP SBC (if included) shall send the alarm messages in Near-Real Time (NRT). More than 99 percent of alarms shall be detected and reported in NRT. NRT is defined as event detection and alarm reporting within 5 seconds of the event, excluding transport time.

AUX-006590 [**Required: CP Server; Conditional: ~~,~~ CP MG, CP SBC**] The CP Server, CP MG (if included), and CP SBC (if included) shall send the alarm messages in SNMPv3 format.

3.9.3 Conditional and Optional Voice and Video Collaboration Product Requirements

3.9.3.1 Voice Call Features (Call Forwarding, Call Transfer, Call Hold, Three Way Calling, Calling Number Delivery)

The Voice Call Feature requirements in the following text are Optional for CPs.

3.9.3.1.1 Call Forwarding

Call Forwarding (CF) allows for incoming calls to a given end user (or user Directory Number [DN]) to be redirected to another user (or user DN), contingent upon feature activation and possibly other conditions. The forwarded-to user may be another CP end user, a UC end user, or a DSN end user, subject to the restrictions of the user activating the feature. Calls forwarded to users who have a call forwarding feature already activated may be forwarded again.

Three types of CF features are applicable for UC CPs:

- Call Forwarding Variable (CFV).
- Call Forwarding Busy Line (CFBL).
- Call Forwarding – Don't Answer – All Calls (CFDA).

AUX-006600 [**Optional: CP Client, CP Server, CP MG, CP SBC**] Reminder Ring for all call forwarding features, as specified in accordance with (IAW) Telcordia Technologies GR-217-CORE, GR-580-CORE, and GR-586-CORE, shall be supported.

In the following requirements, references to a "user's DN" or a "user-specified DN" can be interpreted to mean "a user's address" or a "user-specified address." This applies because the CP may assign the CF features to the user's address instead of to the user's DN, and may support call forwarding to user addresses (such as the Usernames of other CP end users), in addition to supporting call forwarding to a user's DSN and COM numbers.

3.9.3.1.1.1 Call Forwarding Variable

When the CFV feature is active for a given user's DN, calls intended for that DN are redirected to a user-specified DN (e.g., a DSN number or commercial number). A user can activate and deactivate CFV for their DN, and can specify the desired terminating DN during each activation. Users cannot answer calls at a DN for which CFV is active, but can originate calls at that DN.

AUX-006610 [**Optional: CP Client, CP Server, CP MG, CP SBC**] CFV shall be supported IAW Telcordia Technologies GR-580-CORE.

3.9.3.1.1.2 Call Forwarding Busy Line

When Call Forwarding Busy Line (CFBL) is configured for a given DN, calls intended for that DN are redirected to a configured DN when the former DN is busy.

AUX-006620 [**Optional: CP Client, CP Server, CP MG, CP SBC**] CFBL shall be supported IAW Telcordia Technologies GR-586-CORE.

3.9.3.1.1.3 Call Forwarding – Don't Answer – All Calls

Calls to DNs configured with CFDA that are not answered after a user-specified number of ringing cycles are redirected to a configured DN.

NOTE: If the DN to which unanswered calls are forwarded is busy, then the original DN continues to ring until the originator of the call abandons it or the call is answered.

AUX-006630 [**Optional: CP Client, CP Server, CP MG, CP SBC**] CFDA shall be supported IAW Telcordia Technologies GR-586-CORE.

3.9.3.1.2 Call Transfer

AUX-006640 [**Optional: CP Client, CP Server, CP MG, CP SBC**] The CP shall support two types of call transfers for voice calls: normal and explicit.

- A normal call transfer is a transfer of an incoming voice call from a CP end user to another party (another CP end user, a DSN phone number, or a COM phone number).
- An explicit call transfer is the CP end user's transfer of two existing calls together, when both of these calls were originated by the CP end user.

The methods used to provide Normal Call Transfer and Explicit Call Transfer at the CP Client, CP Server, CP MG, and CP SBC are up to the CP vendor.

3.9.3.1.3 Call Hold

AUX-006650 [**Optional: CP Client, CP Server, CP MG, CP SBC**] The CP shall support the Call Hold feature for Voice calls. Call Hold shall support the following capabilities:

- End user can place an active voice call on hold.
- End user can retrieve a held voice call, making it an active voice call again.
- End user can have multiple voice calls on hold at the same time.
- Notifications from the CP to the end user that their held call is still on hold. (e.g., when a user's active call ends and the user's held call is still on hold, the CP should notify the user that the held call is still established and is still on hold).

The methods used to provide the Call Hold, Call Retrieve, and Hold Notification capabilities at the CP Client, CP Server, CP MG, and CP SBC, are up to the CP vendor.

3.9.3.1.4 Three-Way Calling

AUX-006660 [**Optional: CP Client, CP Server, CP MG, CP SBC**] The CP shall support the Three-Way Calling feature for Voice calls. Three-Way Calling shall support the following capabilities:

- End user can place an active voice call on hold, launch an outgoing voice call, and merge the two voice calls together into a three-way call.
- End user can place an active voice call on hold, answer an incoming voice call, and merge the two voice calls together into a three-way call.
- Place a three-way call on hold and retrieve a three-way call from hold.

AUX-006670 [**Optional: CP Client, CP Server, CP MG, CP SBC**] If the CP uses SIP for voice call establishment, then the product shall support the Three-Way Calling feature consistent with the following sections of Request for Comment (RFC) 5359:

- Section 2.10, Three-Way Conference – Third Party Is Added.
- Section 2.11, Three-Way Conference – Third Party Joins.

Aside from the RFC 3539 requirement, the methods used to provide the Three-Way Calling capabilities at the CP Client, CP Server, CP MG, and CP SBC, are up to the CP vendor. In addition, the location of the audio mixer/audio bridge that combines the audio media for each Three-Way Call is up to the CP vendor. For example, this mixer/bridge can be located in the CP Client, CP Server, CP MG, or CP SBC.

3.9.3.1.5 Calling Number Delivery

AUX-006680 [**Optional: CP Client, CP Server, CP MG, CP SBC**] The CP shall support the Calling Number Delivery feature for Voice calls. Calling Number Delivery shall support the following capabilities:

- Delivery of the calling party's number to the CP end user on incoming voice calls to that user from other CP end users, from UC network and DSN end users, and from PSTN end users.
- Delivery of "Calling Number Private" indications to the CP end user on incoming voice calls to that user in which the calling party's identity is marked "Private."
- Delivery of "Calling Number Unavailable" indications to the CP end user on incoming voice calls to that user in which the calling party's identity is not available.

AUX-006690 [**Optional: CP Client, CP Server, CP MG, CP SBC**] The CP shall determine the calling number provided to the called party based on the dialing plan used by the calling party:

- If the incoming call is from another CP end user, then the calling number shall be delivered to the called party in a format that allows the called party to "call back" the calling party at a later time. A calling party address (such as a Calling Party Username) can be used instead of a calling party number in this case.
- If the incoming call is from a UC network or DSN user, then the calling number shall be delivered to the called party in a 10-digit DSN number format.
- If the incoming call is from a PSTN (commercial) user, then the calling number shall be delivered to the called party in a national or international calling number format.

Aside from the above requirements, the methods used to provide the Calling Number Delivery capabilities at the CP Client, CP Server, CP MG, and CP SBC, are up to the CP vendor.

3.9.3.1.5.1 Calling Name Delivery

AUX-006700 [**Optional: CP Client, CP Server, CP MG, CP SBC**] The CP shall support the Calling Name Delivery feature for Voice calls. Calling Number Delivery shall support the following capabilities:

- Delivery of the calling party's name to the CP end user on incoming voice calls to that user from other CP users, from UC network and DSN end users, and from PSTN end users.
- Delivery of "Calling Name Private" indications to the CP end user on incoming voice calls to that user in which the calling party's identity is marked "Private."
- Delivery of "Calling Name Unavailable" indications to the CP end user on incoming voice calls to that user in which the calling party's identity is not available.

Aside from the aforementioned requirements, the methods used to provide the Calling Name Delivery capabilities at the CP Client, CP Server, CP MG, and CP SBC, are up to the CP vendor.

3.9.3.2 Outgoing Voice Calls to DSN and COM Numbers (via CP MG or SBC)

All of the requirements in this section are conditional on CP support for outgoing vocie calls to DSN and Commercial (COM) numbers, via the CP MG and/or the CP SBC.

AUX-006710 [~~**Optional**~~**Conditional: CP Client, CP Server, CP MG, CP SBC**] The CP shall support the establishment of point-to-point VoIP calls from CP end users to DSN numbers, and point-to-point VoIP calls from CP end users to ~~Commercial (~~COM~~)~~ numbers.

- The CP shall route voice calls to DSN numbers to either a DSN PRI on the CP MG, or to an AS-SIP "trunk group" on the CP SBC, depending on the value of the called DSN number.
- The CP can also route a voice call to a DSN number to another end user served by that CP, if that DSN number is associated with that other end user in the CP's internal routing tables.
- The CP shall route voice calls to COM numbers to either a PSTN PRI on the CP MG, or to an AS-SIP "trunk group" on the CP SBC, depending on the value of the called COM number.
- The CP can also route a voice call to a COM number to another end user served by that CP, if that COM number is associated with that other end user in the CP's internal routing tables.

AUX-006720 [~~**Optional**~~**Conditonal: CP Client, CP Server, CP MG, CP SBC**] The CP shall support outgoing Voice call requests from CP end users, containing the following:

- Called addresses that are DSN numbers from the DSN numbering plan.
- Called addresses that are E.164 numbers from the E.164 numbering plan.

AUX-006730 [~~Optional~~**Conditonal: CP Client, CP Server, CP MG, CP SBC**] When a Voice call's called address includes a DSN number from the DSN numbering plan, the CP shall determine whether the called DSN number is local to the CP or external to the CP.

If the called DSN number is local to the CP, then the CP shall complete the Voice call request to the destination end user on that CP.

If the called DSN number is external to the CP, then the CP shall route the session request outside of the CP, using one of the following:

- A DSN PRI on the CP MG (i.e., a PRI connected to a DSN EO).
- An AS-SIP "trunk group" on the CP SBC (i.e., an AS-SIP "trunk group" that is linked with another UC network element such as an SC or an SC SBC).

AUX-006740 [~~Optional~~**Conditional: CP Client, CP Server, CP MG, CP SBC**] When a Voice call's called address includes an E.164 number from the E.164 numbering plan, the CP shall determine whether the called E.164 number is local to the CP or external to the CP.

If the called E.164 number is local to the CP, then the CP shall complete the Voice call request to the destination end user on that CP.

If the called E.164 number is external to the CP, then the CP shall route the session request outside of the CP, using one of the following:

- A PSTN PRI on the CP MG (that is, a PRI connected to a PSTN EO).
- An AS-SIP "trunk group" on the CP SBC (i.e., an AS-SIP "trunk group" that is linked with another UC network element such as an SC or an SC SBC).

AUX-006750 [~~Optional~~**Conditional: CP MG**] For outgoing Voice calls, the CP MG shall support access to DSN EOs and PSTN EOs using the following types of ISDN PRIs:

- North American ISDN PRI.
- European (ETSI) ISDN PRI.

AUX-006760 [~~Optional~~**Conditional: CP MG**] For North American PRIs, the CP MG shall support both the Facility Associated Signaling (FAS) **[Conditional]** and Non-Facility Associated Signaling (NFAS) **[Optional]** options.

AUX-006770 [~~Optional~~**Conditonal: CP SBC**] For outgoing Voice calls, the CP SBC shall support access to UC SCs and UC SC SBCs using AS-SIP trunk groups, per the SBC AS-SIP requirements in Section 2.17, SBC, and the AS-SIP 2013 document.

3.9.3.3 Incoming Voice Calls from DSN and COM Numbers (via CP MG or SBC)

All of the requirements in this section are conditional on CP support for incoming vocie calls from DSN and COM numbers, via the CP MG and/or the CP SBC.

AUX-006780 [~~**Optional**~~**Conditional: CP Client, CP Server, CP MG, CP SBC**] The CP shall support the establishment of point-to-point VoIP calls to CP end users from DSN numbers, and of point-to-point VoIP calls to CP end users from COM numbers.

- The CP shall accept calls to DSN numbers from a DSN PRI on the CP MG, and from an AS-SIP "trunk group" on the CP SBC.
- The CP can also accept a call to a DSN number from another end user served by that CP, if that DSN number is associated with an end user in the CP's internal routing tables.
- The CP shall accept calls to COM numbers from a PSTN PRI on the CP MG, and from an AS-SIP "trunk group" on the CP SBC.
- The CP can also accept a call to a COM number ~~to~~ from another end user served by that CP, if that COM number is associated with an end user in the CP's internal routing tables.

AUX-006790 [~~**Optional**~~**Conditional: CP Client, CP Server, CP MG, CP SBC**] The CP shall support incoming Voice call requests to ~~the~~ CP end users, containing the following:

- Called addresses that are DSN numbers from the DSN numbering plan.
- Called addresses that are E.164 numbers from the E.164 numbering plan.

AUX-006800 [~~**Optional**~~**Conditional: CP Client, CP Server, CP MG, CP SBC**] When a Voice call's called address includes a DSN number from the DSN numbering plan, the CP shall determine whether the called DSN number is local to the CP or external to the CP.

If the called DSN number is local to the CP, then the CP shall complete the Voice call request to the destination end user on that CP.

If the called DSN number is external to the CP, then the CP may route the session request back outside the CP, using one of the following:

- A DSN PRI on the CP MG.
- An AS-SIP "trunk group" on the CP SBC.

In these cases, it is recommended that the route which the call leaves the CP on be different from the route which the call entered the CP on (e.g., if the call came in on a DSN PRI, then the call should go out on an AS-SIP trunk group).

AUX-006810 [~~**Optional**~~**Conditional: CP Client, CP Server, CP MG, CP SBC**] When a Voice call's called address includes an E.164 number from the E.164 numbering plan, the CP shall determine whether the called E.164 number is local to the CP or external to the CP.

If the called E.164 number is local to the CP, then the CP shall complete the Voice call request to the destination end user on that CP.

If the called E.164 number is external to the CP, then the CP may route the session request back outside the CP, using one of the following:

- A PSTN PRI on the CP MG.
- An AS-SIP "trunk group" on the CP SBC.

In these cases, it is recommended that the route which the call leaves the CP on be different from the route which the call entered the CP on (e.g., if the call came in on an AS-SIP trunk group, then the call should go out on a PSTN PRI).

AUX-006820 [~~**Optional**~~**Conditional: CP MG**] For incoming Voice calls, the CP MG shall support access from DSN EOs and PSTN EOs using the following types of ISDN PRIs:

- North American ISDN PRI.
- European (ETSI) ISDN PRI.

AUX-006830 [~~**Optional**~~**Conditional: CP MG**] For North American PRIs, the CP MG shall support both the Facility Associated Signaling (FAS) and Non-Facility Associated Signaling (NFAS) options.

AUX-006840 [~~**Optional**~~**Conditional: CP SBC**] For incoming Voice calls, the CP SBC shall support access from UC SCs and UC SC SBCs using AS-SIP trunk groups, per the SBC AS-SIP requirements in Section 2.17, SBC, and the AS-SIP 2013 document.

3.9.3.4 Video Call Features (Call Forwarding, Call Transfer, Call Hold, Three-Way Calling, Calling Number Delivery)

The Video Call Feature requirements in the following text are Optional for CPs.

AUX-006850 [**Optional: CP**] The CP shall support the following features for video calls, as an extension of the requirements for these features for voice calls in Section 3.9.3.1, Voice Call Features:

- Call Forwarding.
- Call Transfer.
- Call Hold.
- Three-Way Calling.
- Calling Number Delivery.

Section 3.9.3.1, Voice Call Features, requirements are extended to Video calls by replacing the term "Voice call" with the term "Video call" in each of these requirements.

AUX-006860 [**Optional: CP Client, CP Server**] On video call requests to CP end users, the CP Client and the CP Server shall not allow the automatic enabling of the user's video camera:

- When the video call request is negotiated (i.e., when the video call type is negotiated or when the video codec is negotiated).
- When the video call is accepted (i.e., when the video call is answered).

After the video call request is negotiated and accepted, the CP Client and the CP Server shall allow the called user to enable ~~his~~ their video camera, once the called user takes a positive action to enable that camera (i.e., the user selects an "Enable camera" option in ~~his~~ their Client application).

3.9.3.5 Outgoing Video Calls to DSN Numbers (via SBC)

All requirements in this section are conditional and CP support for outging video calls to DSN numbers via the CP SBC.

AUX-006870 [~~Optional~~Conditional: CP Client, CP Server, CP SBC] The CP shall support the establishment of point-to-point Video over IP calls from CP end users to DSN numbers.

- The CP shall route video calls to DSN numbers to an AS-SIP "trunk group" on the CP SBC.
- The CP can also route a video call to a DSN number to another end user served by that CP, if that DSN number is associated with that other end user in the CP's internal routing tables.

AUX-006880 [~~Optional~~**Conditional: CP Client, CP Server, ~~CP MG,~~ CP SBC**] The CP shall support outgoing Video call requests from CP end users containing called addresses that are DSN numbers from the DSN numbering plan.

AUX-006890 [~~Optional~~**Conditional: CP Client, CP Server, ~~CP MG,~~ CP SBC**] When a Video call's called address includes a DSN number from the DSN numbering plan, the CP shall determine whether the called DSN number is local to the CP or external to the CP.

If the called DSN number is local to the CP, then the CP shall complete the Video call request to the destination end user on that CP.

If the called DSN number is external to the CP, then the CP shall route the session request outside the CP, using an AS-SIP "trunk group" on the CP SBC (that is, an AS-SIP "trunk group" that is linked with another UC network element such as an SC or an SC SBC).

AUX-006900 [~~Optional~~**Conditional: CP SBC**] For outgoing Video calls, the CP SBC shall support access to UC SCs and UC SC SBCs using AS-SIP trunk groups, per the SBC AS-SIP requirements in Section 2.17, SBC, and the AS-SIP 2013 document.

3.9.3.6 Incoming Video Calls from DSN Numbers (via SBC)

All of the requirements in this section are conditional on CP support for incoming video calls from DSN numbers via the CP SBC.

AUX-006910 [~~**Optional**~~**Conditional: CP Client, CP Server, ~~CP MG,~~ CP SBC**] The CP shall support the establishment of point-to-point Video over IP calls to CP end users from DSN numbers.

- The CP shall accept video calls to DSN numbers from an AS-SIP "trunk group" on the CP SBC.
- The CP can also accept a video call to a DSN number from another end user served by that CP, if that DSN number is associated with an end user in the CP's internal routing tables.

AUX-006920 [~~**Optional**~~**Conditional: CP Client, CP Server, ~~CP MG,~~ CP SBC**] The CP shall allow incoming Video call requests to the CP end users containing called addresses that are DSN numbers from the DSN numbering plan.

AUX-006930 [~~**Optional**~~**Conditional: CP Client, CP Server, ~~CP MG,~~ CP SBC**] When a Video call's called address includes a DSN number from the DSN numbering plan, the CP shall determine whether the called DSN number is local to the CP or external to the CP.

If the called DSN number is local to the CP, then the CP shall complete the Video call request to the destination end user on that CP.

If the called DSN number is external to the CP, then the CP may route the session request back outside the CP using the AS-SIP "trunk group" on the CP SBC.

AUX-006940 [~~**Optional**~~**Conditional: CP SBC**] For incoming Video calls, the CP SBC shall support access from UC SCs and UC SC SBCs using AS-SIP trunk groups, per the SBC AS-SIP requirements in Section 2.17, SBC, and the AS-SIP 2013 document.

3.9.3.7 High Availability (Five 9s) for Collaboration Products

AUX-006950 [**Optional: CP**] The CP shall have a product availability state of 0.99999 (a nonavailability state of no more than 5 minutes per year). The CP vendor shall provide an availability model for the product, showing all availability calculations and showing how the overall availability will be met. The product components shall have no single point of failure that could cause an outage of more than 96 VoIP and Video over IP subscribers.

AUX-006960 [**Optional: CP**] The CP shall meet the following maximum downtime requirements:

1. IP (10/100 Ethernet) network links (CP Server to CP MG connections, CP Server to CP SBC connections, and CP SBC connections to external SCs and SC SBCs): No more than 35 minutes of downtime per year.

2. IP End User connections (CP Client to CP Server connections): No more than 12 minutes of downtime per year.

3.9.3.8 Emergency Service (911) for Voice Calls

The Emergency Service feature provides a three-digit telephone number (e.g., 911 in the US) that gives the end user emergency service access to an Emergency Service Bureau. The emergency call access is one way only, originating from the end user's CP Client within the CP and terminating to the ESB.

Possible call routes from the CP Client to the ESB are as follows. Another term for an ESB in the PSTN is Public Safety Answering Point (PSAP).

- CP Client => CP Server => CP MG => PSTN EO => PSTN Selective Router => PSTN ESB (PSAP).
- CP Client => CP Server => CP SBC => UC Session Controller => SC MG => PSTN EO => PSTN Selective Router => PSTN ESB (PSAP).
- CP Client => CP Server => CP MG => DSN EO => Local Military Base ESB (Military PSAP).
- CP Client => CP Server => CP SBC => UC Session Controller => SC MG => DSN EO => Local Military Base ESB (Military PSAP).

Historically, PSTN PSAPs in the United States make a distinction between Basic 911 Service and Enhanced 911 Service (E911). With Basic 911 Service, the calling party and the called ESB are served by the same local switching system (usually legacy), and that switching system is served by only one ESB. With E911, the calling party is served by a local switching system (legacy or VoIP), the called ESB (legacy or VoIP) is served by a special emergency switching system called an E911 Selective Router (also legacy or VoIP), and each local switching system is connected to at least one Selective Router. With E911, the local switching system can also be served by more than one Selective Router, and a Selective Router typically serves multiple ESBs. An individual ESB can also be served by multiple Selective Routers.

Both Basic 911 and E911 allow the ESB to "hold" a caller's 911 connection when that caller hangs up (i.e., keep the connection active), and to disconnect the caller's 911 connection once the ESB believes that it is no longer necessary to talk to the caller. Basic 911 and E911 also use caller identification methods such as Automatic Number Identification (ANI) and Calling Number Delivery (CND) to tell the ESB where the caller is calling from.

AUX-006970 [**Optional: CP**] The CP shall support Emergency Services Access ~~services~~ for CP end users. The CP shall allow the end user to dial an Emergency Services number as part a Voice call request (e.g., 911 in the United States and Canada, and 112 in European countries), in order to place an emergency call and reach an ESB/PSAP.

AUX-006980 [**Optional: CP**] Once the Emergency Services number is dialed, the CP shall route the call to a specified route for outgoing Emergency calls. The CP shall support the following Emergency call routes:

- CP Client => CP Server => CP MG => PSTN PRI => PSTN EO (which would typically route the call to a PSTN PSAP).
- CP Client => CP Server => CP SBC => AS-SIP Interface => UC Session Controller (which could route the call to either a PSTN PSAP or a Military PSAP, depending on the SC's configuration).
- CP Client => CP Server => CP MG => DSN PRI => DSN EO => (which could route the call to either a PSTN PSAP or a Military PSAP, depending on the EO's configuration).

This requirement applies for 911 calls on U.S. bases and 112 calls on European bases (when 112 is used as an Emergency Services Number on European bases). It also applies for 911 calls on bases outside the United States, when the 911 calls are routed to a Military PSAP on that base.

AUX-006990 [**Optional: CP**] Once the Emergency Services call is answered at the ESB, the CP shall prevent the CP calling party from ending the call (i.e., a disconnect request from that caller shall be rejected).

The CP shall allow the CP MG or the CP SBC to end the call in this case, provided that the CP MG or CP SBC receives a disconnect request from the destination PSAP indicating that the call can be disconnected. This supports the ESB/PSAP "Emergency Call Hold" feature described previously.

AUX-007000 [**Optional: CP**] The CP shall provide Calling Party Number (CPN) information with the Emergency call request (911 or 112 call) to signal to the destination PSAP where the emergency call is being originated from.

The CP shall include this CPN information in the ISDN PRI signaling when the call leaves the CP via the CP MG. The CP shall include this CPN information in the AS-SIP signaling when the call leaves the CP via the CP SBC.

AUX-007010 [**Optional: CP**] The CP shall allow the CP System Administrator to associate a calling user with a calling physical location on the base, and a CPN value that points to that calling physical location. The CP should use this configured CPN value to identify the calling location on outgoing Emergency call requests, through the CP MG and CP SBC.

AUX-007020 [**Optional: CP**] The CP shall allow the CP end user to place a 911 Emergency Services call without having to dial a PSTN access code (e.g., 9+9) or a DSN access code (e.g., 9+4). The CP is not required to support a 911 Emergency Services call using the PSTN Access Code (e.g., by dialing 9+9+911) or a DSN Access Code (e.g., by dialing 9+4+911).

AUX-007030 [**Optional: CP**] When the CP provides the Emergency Service feature using the 911 number, the feature's operation shall also be IAW Telcordia Technologies GR-529-CORE (Functional Specifications Document [FSDs] 15 01-0000, 15-03-0000, and 15-07-0000).

Since GR-529-CORE was written for legacy voice systems, the CP vendor may interpret how to apply the GR's 911 requirements to 911 Voice calls from CP end users. If the vendor's interpretation of GR-529-CORE conflicts with the previous requirements in this section for 911 calls, then those previous requirements should take precedence.

The Emergency Services feature does not currently apply to emergency video call requests from CP end users.

3.9.3.9 Basic Session Admission Control

AUX-007040 [**Optional: CP]** The CP shall implement call counts and call thresholds for VoIP sessions, and call counts and call thresholds for Video over IP sessions, in order to perform Session Admission Control (SAC).

SAC refers to the CP's enforcement of voice and video call thresholds for the following:

- Outgoing Voice calls from CP end users to UC network and DSN end users, via the CP Server and the CP SBC.
- Incoming Voice calls to CP end users from UC network and DSN end users, via the CP SBC and the CP Server.
- Outgoing Video calls from CP end users to UC network end users, via the CP Server and the CP SBC.
- Incoming Video calls to CP end users from UC network end users, via the CP SBC and the CP Server.

The voice and video call thresholds for SAC do not apply to the following types of calls:

- Outgoing Voice calls from CP end users to DSN and PSTN end users, via the CP Server and the CP MG.
- Incoming Voice calls to CP end users from DSN and PSTN end users, via the CP MG and the CP Server.
- Voice calls between CP end users served by the same CP Server.
- Video calls between CP end users served by the same CP Server.

AUX-007050 [**Optional: CP**] The CP shall support configuration of total voice call thresholds and total video call thresholds.

AUX-007060 [Optional: CP] The CP shall also support configuration of outbound voice call thresholds, inbound voice call thresholds, outbound video call thresholds, and inbound video call thresholds.

This support of different call thresholds for outbound calls (CP Server => CP SBC => UC Network) and inbound calls (UC Network => CP SBC => CP Server) is called directionalization.

AUX-007070 [**Optional: CP**] The CP shall apply SAC and enforce the configured voice and video call thresholds in the following cases:

- Reject outbound voice call requests from the CP to the UC Network that would exceed the configured voice call threshold (or the configured outbound voice call threshold, when directionalization is supported).
- Reject inbound voice call requests from the UC Network to the CP that would exceed the configured voice call threshold (or the configured inbound voice call threshold, when directionalization is supported).
- Reject outbound video call requests from the CP to the UC Network that would exceed the configured video call threshold (or the configured outbound video call threshold, when directionalization is supported).
- Reject inbound video call requests from the UC Network to the CP that would exceed the configured video call threshold (or the configured inbound video call threshold, when directionalization is supported).

AUX-007080 [**Optional: CP**] If commercial SIP is used between the CP Server and the CP SBC, then the CP shall treat new SIP INVITE requests (outbound or inbound) as new CP call requests, for both Voice and Video calls.

But the CP shall not treat SIP re-INVITE requests (outbound or inbound) as new CP call requests, for either Voice or Video calls, because the SIP re-INVITE requests are updates to previously accepted SIP INVITE requests.

3.9.4 IM/Chat/Presence Collaboration Product Requirements

3.9.4.1 Intra-System Capabilities

The requirements between clients hosted off a single collaboration system are provided in the following text.

3.9.4.1.1 Secure IM/Chat/Presence Sessions Over TLS

AUX-007090 [**Required: CP**] The CP shall use TLS to enable secure client-to-server connections between the host server and its clients.

3.9.4.1.2 Presence Subscription Management

AUX-007100 [**Required: CP**] The CP shall provide the ability for end users to subscribe to another user's presence (i.e., end user availability status) and to be notified when that state changes.

AUX-007110 [**Required: CP**] Before the subscribing end user is permitted to see a contact's presence information, the contact must authorize the subscription.

AUX-007120 [**Required: CP**] The CP shall support the ability for end users to cancel a subscription/unsubscribe to an end user's presence.

3.9.4.1.3 Exchange Presence

AUX-007130 [**Required: CP**] The CP shall enable end users to send presence information to the host server, and the host server shall in turn propagate that information to all the user's contacts who have an active subscription to that user's presence information.

AUX-007140 [**Required: CP**] The CP shall permit end users to update their presence (i.e., Availability Status), and the host server shall in turn broadcast the updated presence information to all the user's contacts who have an active subscription to that user's presence information.

AUX-007150 [**Required: CP**] With regard to the exchange of presence, the CP shall support the ability to block and unblock communications with selected users.

3.9.4.1.4 Roster (Contact List) Management

AUX-007160 [**Required: CP**] The CP shall store an end user's roster and shall permit end users to retrieve their roster upon login into the host server.

AUX-007170 [**Required: CP**] The CP shall enable end users to add, modify, or delete items in their roster. For example, adding or deleting a group to a roster.

3.9.4.1.5 One-to-One Chat

AUX-007180 [**Required: CP**] The CP shall enable a one-to-one chat (near real-time, text-based messaging) conversation between two parties.

AUX-007190 [**Required: CP**] The CP shall communicate chat state notifications (i.e., the ability to communicate when a chat partner is actively engaged in composing/typing a message).

AUX-007200 [**Required: CP**] With regard to one-to-one chat, the CP shall support the ability to block and unblock communications with selected end users.

3.9.4.1.6 Persistent Group Chat

AUX-007210 [**Required: CP**] The CP shall enable groups of end users to participate and maintain ongoing discussions within the context of a real-time, text-based conference.

AUX-007220 [**Required: CP**] The CP shall permit end users to create a chat room (i.e., a virtual space for a real-time, text-based conference). The end user who creates the room is designated as the owner of the room with moderator privileges.

AUX-007230 [**Required: CP**] The CP shall permit the owner/moderator to define a name for the room.

AUX-007240 [**Required: CP**] The CP shall permit an end user to "enter" a room by becoming an "occupant within the room" with the privilege to participate in the ongoing discussions.

AUX-007250 [**Required: CP**] The CP shall permit an end user to "exit" a room by ceasing to be an "occupant within the room."

AUX-007260 [**Required: CP**] The CP shall permit the room owner/moderator to ban a user from a room or to remove a participant from a room.

AUX-007270 [**Required: CP**] The CP shall permit an end user to create a members only room and to grant or revoke membership to other end users.

3.9.4.2 Inter-System Capabilities

The optional requirements between clients hosted off of different Collaboration Systems are provided in Table 3.9-1.

Table 3.9-1. Optional Inter-System Capability Requirements

REFERENCE SECTION	UC XMPP SECTION TITLE
Secure Server-to-Server over TLS [as defined in UC XMPP 2013 Specification]	
UC XMPP 2.5	XMPP Addressing
UC XMPP 2.6.1.1	Hostname Resolution
UC XMPP 2.6.2	Stream Negotiation
UC XMPP 2.6.3	Stream Features
UC XMPP 2.6.4	Stream Restarts
UC XMPP 2.6.5	Continuation and Completion of Stream Negotiation
UC XMPP 2.6.6	Directionality
UC XMPP 2.6.7	Closing a Stream
UC XMPP 2.6.8	Stream Attributes
UC XMPP 2.6.9	Namespaces
UC XMPP 2.7	STARTTLS Negotiation
UC XMPP 2.8	Authentication and SASL Negotiation
IM/Presence [as defined in UC XMPP 2013 Specification]	
UC XMPP 2.12.1	Subscription Requests and Approvals
UC XMPP 2.12.2	Cancelling a Subscription

REFERENCE SECTION	UC XMPP SECTION TITLE
UC XMPP 2.12.3	Unsubscribing
UC XMPP 2.13	Exchanging Presence Information
UC XMPP 2.13.1	Initial Presence
UC XMPP 2.13.3	Subsequent Presence Broadcasts
UC XMPP 2.13.4	Unavailable Presence
UC XMPP 2.13.5	Presence Syntax
UC XMPP 2.14.1	One-to-One Chat Sessions
UC XMPP 2.14.2	Message Stanza Syntax
Persistent Group Chat [as defined in XEP-0045, Multi-User Chat and UC XMPP 2013 Specification]	
XEP-0045 3	Requirements
XEP-0045 5	Roles, Affiliations, and Privileges (Capabilities which are defined as "Required" in XEP 0045)
XEP-0045 6	Entity Use Cases (Capabilities which are defined as "Required" in XEP 0045)
XEP-0045 7	Occupant Use Cases (Capabilities which are defined as "Required" in XEP 0045)
Persistent Group Chat [as defined in XEP-0045, Multi-User Chat and UC XMPP 2013 Specification]	
XEP-0045 8	Moderator Use Cases (Capabilities which are defined as "Required" in XEP 0045)
XEP-0045 9	Admin Use Cases (Capabilities which are defined as "Required" in XEP 0045)
XEP-0045 10	Owner Use Cases (Capabilities which are defined as "Required" in XEP 0045)
UC XMPP, Table 2.16-2	Elevated/Clarified Requirements
UC XMPP, 18	DiffServ Code Point (DSCP) Requirements

SECTION 4
INFORMATION ASSURANCE

4.1 INTRODUCTION

This section defines the interoperability focused Information Assurance (IA) requirements for Unified Capabilities (UC) products. These products include but are not limited to Softswitches (SSs), Session Controllers (SCs), Session Border Controllers (SBCs), and End Instruments (EIs). While Voice and Video over Internet Protocol (VVoIP) IA interoperability remains a key focus area, over time this section has been expanded to incorporate the general IA, interoperability-focused requirements for additional UC Approved Products List (APL) products. This section of the Unified Capabilities Requirements (UCR) also incorporates the general information assurance requirements for a number of UC APL "Security Devices," generally considered to be "Information Assurance Products" in accordance with Department of Defense (DoD) Directive (DoDD) 8500.1. These requirements include network-based Firewalls (FWs), Intrusion Prevention Systems (IPSs), Virtual Private Network (VPN) servers, and Network Access Controllers (NACs), for example. More information on Security Devices can be found in Section 13, Security Devices, which specifies the "security-device-unique" functional requirements for these products.

A number of requirements have been removed from this UCR section in order to minimize the number of requirements that overlap with the requirements already found in Defense Information Systems Agency (DISA) Facility Security Office (FSO) Security Technical Implementation Guides (STIGs) and Security Requirement Guides (SRGs). The STIGs and SRGs now serve as the primary baseline for purely IA-focused requirements, and this UCR section focuses on those requirements that impact interoperability from an IA standpoint. Since both the UCR and STIGs/SRGs are utilized during testing, the intent is to minimize redundancy in information assurance test procedures and reports.

4.1.1 Product Configuration Considerations

In many cases, a system is composed of multiple appliances. For example, typically an SC is composed of a Call Connection Agent (CCA), a media server, a configuration server, a voicemail server, and other servers. Because of the wide variation in vendor products, it is impossible to break out the requirements for each component of a system and the reader should apply the higher level requirements to that component unless specifically stated. For example, the SC requirements apply to a media server within the SC system, even though this relationship is not directly stated. On the other hand, Media Gateway (MG) and EI requirements are called out separately; therefore, the SC requirements would not apply to these devices.

During information assurance testing at approval DoD laboratories, UC APL products are tested against the UCR requirements in this section and information assurance requirements found in other sections of the UCR (e.g., 5, 13), as applicable, in addition to the STIGs and SRGs. For all

products not directly addressed within Section 4 or other UCR sections from an IA perspective, IA testing for the product will include testing against all applicable STIGs and SRGs.

The requirement key words (i.e., REQUIRED, CONDITIONAL) are defined elsewhere in this UCR. Failure to satisfy a requirement in this section will result in a Technical Deficiency Report (TDR), which differs from past versions of this section in which the requirements were adjudicated as UCR CAT I, II, or III findings in the IA Test Report.

Finally, the requirements that follow do not include all administrative requirements (nontechnical) associated with policy STIGs and SRGs. For instance, if someone is required to document something administratively (e.g., waiver, pilot request) as part of site accreditation, that requirement is not included.

4.2 REQUIREMENTS

4.2.1 The [Alarm] Tag: Generation of Alarms

When the [Alarm] tag appears after a requirement's applicability statement (e.g., Required and Conditional), this indicates that the product must support, at a minimum, the capability to perform the following functions in addition to complying with the specified requirement:

1. Generate an alarm to the Network Management System (NMS) based on the alarmable actions identified in the requirement and using the configured alarm transmission mechanism [e.g., Simple Network Management Protocol (SNMP), syslog, email].
2. Record an entry in the product's system and audit logs indicating that the event occurred.

This tag is intended to facilitate rapid identification of all those requirements that result in alarm conditions by automated requirement management tools.

4.2.2 Product Category Definitions

Table 4.2-1, Acronyms and Appliances Specifying Type of Component, shows the acronyms and appliances that represent a specific UC APL product.

Table 4.2-1. Acronyms and Appliances Specifying Type of Component

ACRONYM	APPLIANCES
AEI	Assured Services Session Initiation Protocol (AS-SIP) End Instrument (including Multipoint Conference Units [MCUs] and other devices that provide AEI-equivalent functionality on their respective interfaces)
EI	End Instrument (Including MCUs and other devices that provide EI-equivalent functionality on their respective interfaces)
FW	Data Firewall
IPS	Intrusion Detection/Prevention System

ACRONYM	APPLIANCES
LS	Local Area Network (LAN) Switch
MG	Media Gateway
NAC	Network Access Controller
R	Router
RSF	Real-Time Services (RTS) Stateful Firewall
SBC	Session Border Controller
SC	Session Controller
SD	Security Device (generic, overarching category which encompasses all devices addressed in Section 13~~8~~ including FW, IPS, VPN, NAC, WIDS)
SS	Softswitch
VPN	Virtual Private Network−concentrator and termination
WIDS	Wireless Intrusion Detection System

4.2.3 User Roles

IA-000000 [**Required: SS, SC**] The product shall be capable of having at least five types of user roles: a system security administrator (e.g., auditor), a system administrator, an application administrator, a privileged application user, and an application user.

IA-001000 [**Required: R, LS, SBC, RSF, MG**] The product shall be capable of having at least three types of user roles: a system security administrator (e.g., auditor), a system administrator, and an application administrator.

IA-002000 [**Required: EI, AEI**] The product shall be capable of supporting at least three types of user roles: a system administrator, a privileged application user, and an application user.

NOTE: The product demonstrates the ability to support a privileged application user by being able to dial precedence digits to signal the SC the precedence of the session.

IA-003000 [**Required: EI, AEI**] The product shall be capable of setting the default user precedence VVoIP session origination capability as ROUTINE.

IA-004000 [**Required: SS, SC, MG, SBC, RSF, R, LS, SD**] The product shall be capable of providing a mechanism for the appropriate administrator (not a user in the User role) to perform the following functions:

IA-004010 [**Required: SS, SC, MG, SBC, RSF, R, LS, SD**] Monitor the activities of a specific terminal, port, or network address of the system in real time.

IA-004020 [**Required:, SS, SC, MG, SBC, RSF, R, LS, SD**] Define the events that may trigger an alarm, the levels of alarms, the type of notification, and the routing of the alarm.

IA-004030 [**Required: SS, SC, MG, SBC, RSF, R, LS, SD**] Provide a capability to monitor the system resources and their availabilities.

IA-005000 [**Required: FW, IPS, VPN, NAC~~SD~~**] The product shall support at least four roles: Cryptographic Administrator (CAdmin), Audit Administrator (AAdmin), System Administrator, User.

NOTE: The CAdmin and AAdmin roles are defined in National Information Assurance Partnership (NIAP) publications.

IA-006000 [**Required: FW, IPS, VPN, NAC~~SD~~**] The ability to perform the following functions shall be restricted to the System Administrator role:

IA-006010 [**Required: FW, IPS, VPN, NAC~~SD~~**] Modify security functions.

IA-006020 [**Required: FW, IPS, VPN, NAC~~SD~~**] Enable or disable security alarm functions.

IA-006030 [**Required: FW, IPS, VPN, NAC~~SD~~**] Enable or disable the Internet Control Message Protocol (ICMP) and destination unreachable notification on external interfaces [in an Internet protocol (IP)-based network], or other appropriate network connectivity tool (for a non-IP-based network).

IA-006040 [**Required: FW, IPS, VPN, NAC~~SD~~**] Determine the administrator-specified period for any policy.

IA-006050 [**Required: FW, IPS, VPN, NAC~~SD~~**] Set the time/date used for timestamps.

IA-006060 [**Required: FW, IPS, VPN, NAC~~SD~~**] Query, modify, delete, and/or create the information flow policy rule set.

IA-006070 [**Required: FW, IPS, VPN, NAC~~SD~~**] Revoke security attributes associated with the users, information flow policy rule set, and services available to unauthenticated users within the security device.

IA-007000 [**Required: FW, IPS, VPN, NAC~~SD~~**] The ability to enable, disable, determine, and/or modify the functions of the security audit or the security audit Analysis shall be restricted to the AAdmin role.

IA-008000 [**Required: FW, IPS, VPN, NAC~~SD~~**] The ability to perform the following functions shall be restricted to the CAdmin role:

IA-008010 [**Required: FW, IPS, VPN, NAC~~SD~~**] Enable and/or disable the cryptographic functions.

IA-008020 [**Required: FW, IPS, VPN, NAC~~SD~~**] Modify the cryptographic security data.

4.2.4 Ancillary Equipment

IA-009000 [**Conditional:, SS, SC, MG, SBC, RSF, R, LS, EI, AEI, SD**] Products that use external Authentication, Authorization, and Accounting (AAA) services provided by the Diameter Base Protocol shall do so in accordance with (IAW) Request for Comment (RFC) 3588.

IA-009010 [**Conditional:, SS, SC, MG, SBC, RSF, R, LS, EI, AEI, SD**] Systems that act as Diameter agents shall be capable of being configured as proxy agents.

IA-009020 [**Conditional: SS, SC, MG, SBC, RSF, R, LS, EI, AEI, SD**] Systems that act as proxy agents shall maintain session state.

IA-009030 [**Conditional: SS, SC, MG, SBC, RSF, R, LS, EI, AEI, SD**] All Diameter implementations shall ignore answers received that do not match a known Hop-by-Hop Identifier field.

IA-009040 [**Conditional: SS, SC, MG, SBC, R, LS, EI, AEI, SD**] All Diameter implementations shall provide transport of its messages IAW the transport profile described in RFC 3539.

IA-009050 [**Conditional: SS, SC, MG, SBC, RSF, R, LS, EI, AEI, SD**] Products that use the Extensible Authentication Protocol (EAP) within Diameter shall do so IAW RFC 4072.

IA-010000 [**Required: R, LS – Conditional: SS, SC, MC, SBC, RSF, EI, AEI, SD**] Products shall support the capability to use the Remote Authentication Dial In User Service (RADIUS) IAW RFC 2865 to provide AAA services.

NOTE: For products to which the Conditional statement applies, the condition is implementation of RADIUS.

IA-010010 [**Required: R, LS – Conditional: SS, SC, MC, SBC, RSF, EI, AEI, SD**] Products that use the EAP within RADIUS shall do so IAW RFC 3579.

NOTE: For products to which the Contitional statement appies, the condition is implementation of RADIUS.

IA-010020 [**Required: R, LS – Conditional: SS, SC, MC, SBC, RSF, EI, AEI, SD**] If the products support RADIUS based accounting, then the system shall do so IAW RFC 2866.

IA-011000 [**Conditional: SS, SC, MG, SBC, RSF, R, LS, EI, AEI, SD**] Products that use external AAA services provided by the Terminal Access Controller Access Control System (TACACS+) shall do so IAW the TACACS+ Protocol Specification 1.78 (or later).

NOTE: The intent is to use the most current TACACS+ specification.

IA-012000 [**Conditional: EI, AEI**] that use external address assignment services provided by the Dynamic Host Configuration Protocol (DHCP) shall do so IAW RFC 2131.

NOTE: An external address assignment service is a service that extends beyond the boundary of the system.

IA-012010 [**Conditional: EI, AEI**] Products that act as DHCP clients upon receipt of a new IP address shall probe [e.g., with Address Resolution Protocol (ARP)] the network with the newly received address to ensure the address is not already in use.

NOTE: The actions to take if a duplicate address is detected are found in RFC 2131.

IA-012020 [**Conditional: EI, AEI**] Products that act as DHCP clients upon receipt of a new IP address shall broadcast an ARP reply to announce the client's new IP address and clear outdated ARP cache entries in hosts on the client's subnet.

IA-013000 [**Conditional: R, LS, EI, AEI, SD**] Products that use external AAA services provided by port based network access control mechanisms shall do so IAW Institute of Electrical and Electronics Engineers (IEEE) 802.1X-2010 in combination with Protected Extensible Authentication Protocol (PEAP) and Extensible Authentication Protocol (EAP)-Transport Layer Security (TLS) support, at a minimum, plus any other desired secure EAP types [e.g., EAP-Tunneled TLS (TTLS)].

IA-013010 [**Conditional: R, LS, EI, AEI, SD**] Products that use external EAP services provided by EAP shall do so IAW RFC 3748 and its RFC extensions.

IA-014000 [**Conditional: SS, SC, MG, SBC, RSF, R, LS, SD**] Products that use external syslog services shall support the capability to do so IAW RFC 3164.

IA-014010 [**Conditional: SS, SC, MG, SBC, RSF, R, LS, SD**] Products that support syslog over User Datagram Protocol (UDP) IAW RFC 3164 shall use UDP port 514 for the source port of the sender when using UDP for transport.

IA-014020 [**Conditional: SS, SC, MG, SBC, RSF, R, LS, SD**] If the product supports syslog, then the product shall support the capability to generate syslog messages that have all the parts of the syslog packet as described in Section 4.1 of RFC 3164.

IA-014030 [**Conditional: SS, SC, MG, SBC, RSF, R, LS, SD**] If the originally formed message has a TIMESTAMP in the HEADER part, then it shall support the capability to specify this field's value in the local time of the device within its time zone and support the ability to specify this field's value in Greenwich Mean Time (GMT).

IA-014040 [**Conditional: SS, SC, MG, SBC, RSF, R, LS, SD**] If the originally formed message has a HOSTNAME field, then it shall contain the hostname as it knows itself. If it does not have a hostname, then it shall contain its own IP address.

IA-014050 [**Conditional: SS, SC, MG, SBC, RSF, R, LS, SD**] If the originally formed message has a TAG value, then it shall be the name of the program or process that generated the message.

IA-014060 [**Conditional: SS, SC, MG, SBC, RSF, R, LS, FW, IPS, VPN, NAC**] If products use Transmission Control Protocol (TCP) for the delivery of syslog events, then the system shall support the capability to do so IAW the Read and Write (RAW) profile defined in RFC 3195.

IA-015000 [**Required: SBC**] The product shall either support an onboard VVoIP Intrusion Detection System (IDS)/IPS capability that can monitor all VVoIP signaling and media traffic in decrypted form, or support the capability to present all signaling and bearer traffic to an external VVoIP IDS/IPS in a secure manner.

IA-015010 [**Required: SBC**] The VVoIP IDS/IPS threat detection capabilities shall be IAW the VVoIP IDS/IPS functional requirements specified in Section 13, Security Devices. The product shall support the capability to generate and transmit an alarm to the NMS when these threats are identified.

IA-015020 [**Conditional: SBC**] If the product provides the capability to transmit decrypted VVoIP media and signaling to an external IDS/IPS platform, then this interface shall use publicly accessible specifications and standards.

NOTE: The intent of this requirement is to ensure that third party IDS/IPS vendors have the information necessary to create an interface that can accept and process the received VVoIP information.

IA-016000 [**Conditional: SS, SC, MG, SBC, RSF, R, LS, SD**] If the product implements NTP, then the ~~default version~~product shall support interoperability with ~~be~~ Network Time Protocol (NTP) version 3 (NTPv3) at a minimum even if higher versions of NTP are supported.

4.2.5 VVoIP Authentication

IA-017000 [**Required: SC**] The product shall be capable of authenticating the EI using TLS (or its equivalent) (Threshold) with Public Key Infrastructure (PKI) certificates issued from a DoD-approved PKI.

NOTE: This assumes the EI is served directly by the appliance.

IA-018000 [**Required: SC**] The product shall be capable of authenticating the AEI using TLS with PKI certificates issued from a DoD-approved PKI.

IA-019000 [**Required: EI**] The product shall be capable of authenticating the SC using TLS (or its equivalent) (Threshold) with PKI certificates issued from a DoD-approved PKI.

IA-020000 [**Required: AEI**] The product shall be capable of authenticating the SC using TLS with PKI certificates issued from a DoD-approved PKI.

IA-021000 [**Required: EI, AEI**] The product shall be capable of allowing users to place ROUTINE precedence calls without authenticating.

IA-022000 [**Required: EI, AEI**] The product shall be capable of allowing users to place emergency calls without authenticating.

IA-023000 [**Required: EI, AEI**] If the product supports authentication for precedence calls, then the product shall support a configuration setting which allows only authenticated users to access the product for services above the ROUTINE precedence level.

IA-023010 [**Conditional: SC, EI, AEI**] If the product uses SIP or AS-SIP, then the system shall, at a minimum, support the use of SIP digest authentication as specified in RFC 3261 when authenticating users. The product may support the ability to authenticate users via PKI certificates when authenticating user credentials to the SC via the EI or the AEI using proprietary mechanisms.

NOTE: The SC 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.

IA-023020 [**Conditional: SC, EI, AEI**] If the product implements AS-SIP and supports authentication for precedence calls, then the product shall use the procedures and algorithms specified in RFC 3261, Section 22.4, to execute SIP digest authentication for user authentication with a Personal Identification Number (PIN). The User-ID entered by the user shall be used for the value of the "username" field, and the PIN entered by the user shall be used as the value for "secret" in the digest calculation.

IA-023030 [**Conditional: EI, AEI**] If the product supports authentication for precedence calls via a PIN, then the device shall support the capability to provide audible and/or visible notification to the user, which, in a human understandable manner, prompts the user to enter his or her assigned User-ID and PIN when a precedence level above ROUTINE is requested.

IA-023040 [**Required: SC, EI, AEI**] The user authentication mechanism shall be software enabled or disabled.

NOTE: In certain deployments, the user does not have the time to input authentication credentials and the EI or AEI is located in a secure environment where credentials are not necessary due to the mission. By default this capability will be disabled to allow users to place calls without authenticating.

IA-023050 [**Conditional: EI, AEI, (Softphone)**] If the product is a softphone, then the product shall support the capability to provide user authentication by presenting the user credentials extracted from the Common Access Card (CAC) or other DoD PKI Project Management Office (PMO)-approved PKI token to the SC.

NOTE: The mechanism for AEIs and EIs to authenticate the User CAC or approved token credentials is permitted to occur via proprietary means. However, authentication of users via User ID and PIN authentication has been standardized for AEIs in this UCR.

IA-024000 [**Required: SS, SC, MG, SBC, AEI**] The product shall adhere to the requirements in RFC 5922, Section 7.2, "Comparing SIP Identities," when comparing the domains extracted from X.509v3 certificates with AS-SIP identities contained in signaling messages.

NOTE: This requirement applies to server certificates, not end-user device or CAC card certificates.

IA-025000 [**Conditional: SS, SC**] If the system supports AEIs that use the sip.instance media feature tag (RFC 5626), then the system shall ensure that the identity claimed in the AEI's X.509 certificate Subject Common Name presented during TLS session establishment maps to the AS-SIP Address of Record (AOR) and sip.instance values specified in AS-SIP signaling messages.

NOTE: This requirement is meant to ensure that the identity claimed by a registering AEI in AS-SIP is authorized based on its presented X.509 certificate.

4.2.6 VVoIP Authorization

IA-026000 [**Required: R, LS, SBC, RSF**] The product shall have the capability of controlling the flow of traffic across an interface to the network based on the source/destination IP address, source/destination port number, Differentiated Services Code Point (DSCP), and protocol identifier ("6 tuple").

IA-027000 [**Required: SBC, RSF**] The product shall have the capability of opening and closing "gates/pinholes" (i.e., packet filtering based on the "6 tuple") based on the information contained within the Session Description Protocol (SDP) body of the AS-SIP messages.

IA-028000 [**Required: SBC, RSF**] The product shall have the capability to close a "gate/pinhole" based on a configurable media inactivity timer and issue a BYE message to upstream and downstream AS-SIP signaling appliances (lost BYE scenario).

NOTE: The inactivity timer is based on the inactivity of the media stream.

IA-029000 [**Required: SBC, RSF**] The default media inactivity value for closing a session and issuing BYE messages shall be 15 minutes.

IA-030000 [**Required: R, SBC, RSF**] The product shall have the capability of permitting the configuration of filters that will permit or deny IP packets on the basis of the values of the packet's source address, destination address, protocol, source port, and destination port in the packets header. These filters shall have the capability of using any one value, all values, or any combination of values. Filters using source ports and destination ports shall have the capability to be configured to use ranges of values defined by the operators (1) equal to, (2) greater than, (3) less than, (4) greater than or equal to and (5) less than or equal to.

IA-031000 [**Required: R, LS**] The product shall be capable of supporting a minimum of five distinct VLANs for VVoIP.

IA-032000 [**Required: SBC**] The product shall be capable of using Network Address Translation (NAT) and Network Address Port Translation (NAPT) on all VVoIP enclave-to-Wide Area Network (WAN) connections.

IA-033000 [**Required: R, SBC, RSF**] The product shall have the capability to deploy using private address space IAW RFC 1918.

IA-034000 [**Required: SBC**] The SBC shall be an AS-SIP intermediary in all WAN signaling sessions.

IA-035000 [**Required: SBC**] To enable the application of NAT and NAPT, the SBC shall be able to inspect and modify the SDP body (i.e., the SDP "c=" and the "m=" lines) of the corresponding AS-SIP message.

IA-036000 [**Conditional: SBC**] If the system supports H.323 video sessions, then the SBC shall be capable of supporting H.323 NAT and NAPT.

IA-037000 [**Conditional: R, LS, EI, AEI**] If DHCP is used, then the product shall be capable of using 802.1X in combination with a secure EAP type (defined within this UCR and the STIGs/SRGs) residing on the authentication server and within the operating system or application software of the EI and AEI to authenticate to the LAN.

IA-038000 [**Required: RSF**] The product shall be capable of being configured to ensure that VVoIP and non-VVoIP traffic between their respective VLANs is filtered and controlled so that traffic is restricted to planned and approved traffic between authorized devices using approved ports, protocols, and services.

IA-039000 [**Required: SBC, RSF**] The product FWs deployed at the boundaries of the VVoIP enclave shall have the capability to use stateful packet inspection.

4.2.7 Public Key Infrastructure

IA-040000 [**Required: SS, SC, MG, SBC, RSF, R, AEI, NAC, LS, SD; Conditional: EI**] The product shall be capable of generating asymmetric keys whose length is at least 2048 for Rivest Shamir Adleman (RSA).

IA-041000 [**Required: SS, SC, MG, SBC, RSF, R, AEI, EI, LS, SD**] The product shall be capable of generating symmetric keys whose length is at least 128 bits.

NOTE: This generation must be done in accordance with the STIGs and SRGs, which require cryptographic operations to be in accordance with Federal Information Processing Standard (FIPS) 140-2.

IA-042000 [**Required: SS, SC, MG, SBC, RSF, R, AEI, LS, SD; Conditional: EI**] The product shall be capable of storing key pairs and their related certificates.

IA-043000 [**Required: SS, SC, MG, SBC, RSF, R, AEI, LS, SD; Conditional: EI**] The product shall operate with DoD-approved trust anchors (e.g., public keys and the associated certificates the relying party deems as reliable and trustworthy, typically root certification authorities [CAs]).

IA-043010 [**Required: SS, SC, MG, SBC, RSF, R, AEI, LS, SD; Conditional: EI**] Any system that performs PKI certificate validation operations must implement the basic steps outlined in Section 6.1.3 of the internet X.509 certificate specification Request for Comment (RFC) 5280.

IA-043020 [**Conditional: SS, SC, MG, SBC, RSF, R, AEI, LS, EI, SD**] The system must also provide the capability to check certificate revocation status as part of the certificate validation process as defined in RFC 5280.

IA-044000 [**Required: SS, SC, MG, SBC, RSF, R, AEI, LS, SD; Conditional: EI**] The product shall be capable of supporting end entity server and device certificates and populating all certificate fields IAW methods described in the "DoD PKI Functional Interface Specification."

IA-045000 [**Required: SS, SC, MG, SBC, RSF, R, AEI, NAC, LS, SD; Conditional: EI**] The product shall be capable of using the Lightweight Directory Access Protocol (LDAP) version 3 (LDAPv3), LDAP over TLS (LDAPS), Hypertext Transfer Protocol (HTTP), or HTTP Secure (HTTPS) as appropriate when communicating with DoD-approved PKIs.

IA-046000 [**Conditional: SS, SC, MG, SBC, RSF, R, AEI, EI, LS, SD**] If Certificate Revocation Lists (CRLs) are used, then the product shall be capable of using either the date and time specified in the next update field in the CRL or using a configurable parameter to define the period associated with updating the CRLs.

IA-047000 [**Conditional: SS, SC, MG, SBC, RSF, R, AEI, EI, LS, SD**] If CRLs are used, then the product shall be capable of obtaining the CRL from the CRL Distribution Point (CDP) extension of the certificate in question. The product shall be able to process HTTP pointers in the CDP field whereas the ability to process HTTPS and LDAP pointers is considered Objective and is not a hard requirement.

NOTE: This requirement does not prevent the product from supporting the ability to use manually configured, local CDPs which differ from the CDP provided in the certificate.

IA-048000 [**Conditional: SS, SC, SBC, RSF, R, AEI, EI, LS, SD**] If Online Certificate Status Protocol (OCSP) is used, then the product shall support the capability to use both the Delegated Trust Model (DTM), whereby the OCSP responder's signing certificates are signed by DoD approved PKI CAs, and the OCSP Trusted Responder model, where the OCSP responder uses a self-signed certificate to sign OCSP responses, IAW DoD PKI PMO guidance.

NOTE: The OCSP responder's DTM certificate is appended to every OCSP response sent from the DoD PKI OCSP responders. Products should expect these certificates to change regularly (approximately every 30 days or less).

NOTE: RFC 2560 describes both the Trust Responder and Delegated Trust (termed "Authorized Responder" within RFC 2560) models. Though DoD PKI-specific implementation details can be found only in DoD PKI PMO publications.

NOTE: In DTM, each CA issues a certificate to the OCSP responder specifically to be used for signing OCSP responses [denoted by the inclusion of the id-ad-ocspSigning object identifier (OID) in the extended key usage extension of the certificate]. The OCSP signing certificate issued by the CA that issued the certificate whose status is being determined is then used to sign the OCSP response.

NOTE: In the Explicit Trust Model (self signed), an OCSP client is explicitly configured to look for a specific certificate to have signed the OCSP response. In this model, OCSP clients typcially must have the OCSP responder's signing certificate installed in their local trust store.

IA-049000 [**Conditional: SS, SC, MG, SBC, RSF, R, AEI, EI, LS, SD**] If OCSP is used, then the OCSP responder shall be contacted based on the following information:

IA-049010 [**Conditional: SS, SC, MG, SBC, RSF, R, AEI, EI, LS, SD**] The OCSP responder preconfigured in the application or toolkit; and

IA-049020 [**Conditional: SS, SC, MG, SBC, RSF, R, AEI, EI, LS, SD**] The OCSP responder location identified in the OCSP field of the Authority Information Access (AIA) extension of the certificate in question.

IA-049030 [**Conditional: SS, SC, MG, SBC, RSF, R, AEI, EI, LS, SD**] If both of the above are available, then the product shall be configurable to provide preference for one over the other.

IA-049040 [**Conditional: SS, SC, MG, SBC, RSF, R, AEI, EI, LS, SD**] The product should (not shall) be configurable to provide preferences or a preconfigured OCSP responder based on the Issuer DN.

IA-050000 [**Conditional: EI**] If the EI is PKI enabled, then the EI shall support a mechanism for verifying the status of an SC certificate using a Certificate Trust List (CTL), CRLs, or an online status check (OCSP in the case of the DoD PKI).

NOTE: It is understood that the system administrator must ensure that the CTL is current to ensure that the status is accurate.

NOTE: When implemented the CRL and OCSP implementation must conform to the CRL and OCSP requirements specified previously and later in this section.

IA-051000 [**Conditional: SC**] If the EI is PKI enabled, then the SC shall verify the status of an EI certificate using the CTL, CRLs, or an online status check (OCSP in the case of the DoD PKI).

NOTE: It is understood that the system administrator must ensure that the CTL is current to ensure that the status is accurate.

NOTE: When implemented the CRL and OCSP implementation must conform to the CRL and OCSP requirements specified previously and later in this section.

IA-052000 [**Required: SS, SC, MG, SBC, RSF, R, AEI, LS, SD; Conditional: EI**] The product shall support all of the applicable requirements in the latest DoD Public Key Enabled (PKE) Application Requirements specification published by the DoD PKI PMO.

NOTE: At the time of this UCR's writing, the “DoD Class 3 Public Key Infrastructure Public Key-Enabled Application Requirements” defines the PKE requirements for DoD products.

IA-053000 [**Required: SS, SC, MG, SBC, RSF, R, AEI, LS, SD; Conditional: EI**] Systems that perform any PKI operations (e.g., certificate path processing, certificate validation, digital signature generation, and encryption) must support RSA keys up to 2048 bits with Secure Hash Algorithm (SHA)-1 and SHA-2 digital signatures as dictated by the National Institute of Standards and Technology (NIST) Special Publications (SP) 800-57, SP 800-78, and SP 800-131A and the DoD Certificate Policy.

IA-053010 [**Required: SS, SC, MG, SBC, RSF, R, AEI, LS, SD; Conditional: EI**] The product shall support the capability to verify certificates, CRLs, OCSP responses, or any other signed data produced by a DoD approved PKI using RSA in conjunction with the SHA-256 algorithm.

NOTE: During the migration to SHA-256, certificate chains may contain a mix of certificates signed using either SHA-1 or SHA-256 within the same chain.

IA-054000 [**Required: SS, SC, MG, SBC, RSF, R, LS, SD**] The product shall log when a session is rejected due to a revoked certificate.

IA-055000 [**Required: SS, SC, MG, SBC, RSF, R, AEI, LS, SD; Conditional: EI**] The product shall be capable of supporting the development of a certificate path and be able to process the path.

NOTE: The path development process produces a sequence of certificates that connect a given end-entity certificate to a trust anchor. The process terminates when either the path tracks from a trust anchor to an end entity or a problem occurs that prohibits validation of the path.

IA-055010 [**Required: SS, SC, MG, SBC, RSF, R, AEI, LS, SD; Conditional: EI**] The path process shall fail when a problem that prohibits the validation of a path occurs.

IA-056000 [**Required: SS, SC, MG, SBC, RSF, R, AEI, LS, SD; Conditional: EI**] The product shall be capable of ensuring that the intended use of the certificate is consistent with the DoD-approved PKI extensions.

IA-056010 [**Required: SS, SC, MG, SBC, RSF, R, AEI, LS, SD; Conditional: EI**] The product shall be capable of ensuring that the key usage extension in the end entity certificate is set properly.

IA-056020 [**Required: SS, SC, MG, SBC, RSF, R, AEI, LS, SD; Conditional: EI**] The product shall be capable of ensuring that the digital signature bit is set for authentication uses.

IA-056030 [**Required: SS, SC, MG, SBC, RSF, R, AEI, NAC, LS, SD; Conditional: EI**] The product shall be capable of ensuring that the non-repudiation bit is set for non-repudiation uses.

IA-057000 [**Conditional: SS, SC, MG, SBC, RSF, AEI, EI**] [**Alarm**] During VVoIP session establishment, if the product uses an online status check to validate a certificate and the product cannot contact the online status check responder (OSCR) (in the case of the DoD PKI, this will be an RFC 2560 OCSP responder) and backup OSCRs, the product will establish the VVoIP session (e.g., shall not terminate the session), but will log the event and send an alarm to the NMS.

NOTE: This requirement applies only to the establishment of VVoIP sessions. This requirement is not applicable to scenarios related to non-VVoIP-session related functions such as logging on to administrative interfaces. The intent of this requirement is to prevent phone or video calls from being denied due to connectivity issues with the OCSP responder.

IA-058000 [**Conditional: SS, SC, MG, SBC, RSF, AEI, EI**] [**Alarm**] During VVoIP session establishment, if the product uses CRLs to validate a certificate and the product cannot reach the

CDP or any backup CDPs, the product will continue the process (e.g. shall not terminate the session), but will log the event and send an alarm to the NMS.

NOTE: This requirement applies only to the establishment of VVoIP sessions (see the note on the preceding requirement).

NOTE: DoD PKI PMO Guidance: Contacting a CDP for a CRL download will result in a massive overhead delaying the establishment of the VoIP session for up to a minute or more depending on the CA. This should only be default for enclave-wide systems and only as a backup for end-user devices.

IA-059000 [**Required: SS, SC, MG, SBC, RSF, R, AEI, LS, SD; Conditional: EI**]
Periodically, the system shall examine all of the certificates and trust chains associated with ongoing, long-lived, sessions. The system shall terminate any ongoing sessions based on updated revocation/trust information if it is determined that the corresponding certificates have been revoked, are no longer trusted, or are expired.

NOTE: The system must not terminate VVoIP sessions simply because of a failure to retrieve the latest CRL or perform an online status check.

IA-059010 [**Conditional: SS, SC, MG, SBC, RSF, R, AEI, EI, LS, SD**] If the system supports manual loading of a CRL or CTLs configured by an administrator, then the system shall check all ongoing sessions as soon as updates to the internally stored CRL or trust lists occur.

IA-059020 [**Conditional: SS, SC, MG, SBC, RSF, R, AEI, EI, LS, SD**] If the system supports automated retrieval of a CRL from a CDP, then the system shall immediately check the certificates and trust chains associated with all ongoing sessions against the newly retrieved CRL.

IA-059030 [**Conditional: SS, SC, MG, SBC, RSF, R, AEI, EI, LS, SD**] If the system supports automated retrieval of a CRL from a CDP, then the system shall support the ability to configure the interval in which the CRL is retrieved periodically.

IA-059040 [**Conditional: SS, SC, MG, SBC, RSF, R, AEI, EI, LS, SD**] If the system supports queries against an online status check responder (an OCSP responder in the case of the DoD PKI), then the system shall periodically query the responder to determine if the certificates corresponding to any ongoing sessions have been revoked.

IA-059050 [**Conditional: SS, SC, MG, SBC, RSF, R, AEI, EI, LS, SD**] If the system supports queries against an online status check responder (an OCSP responder in the case of the DoD PKI), by default, for each session, then the device shall query the online status check responder every 24 hours for as long as the session remains active.

IA-059060 [**Conditional: SS, SC, MG, SBC, RSF, R, AEI, EI, LS, SD**] If the system supports queries against an online status check responder (an OCSP responder in the case

of the DoD PKI), then the system shall support the ability to configure the interval at which the system periodically queries the online status check responder.

IA-060000 [**Required: SS, SC, MG, SBC, RSF, R, AEI, LS, SD; Conditional: EI**] [**Alarm**] The system shall be capable of sending an alert when installed certificates corresponding to trust chains, OCSP responder certificates, or any other certificates installed on the device that cannot be renewed in an automated manner, are nearing expiration.

NOTE: Since EIs and AEIs are not expected to have direct access to the NMS, the SC, or SS is expected to generate this alert to the NMS on behalf of any subtended EIs or AEIs. However, EIs and AEIs should also alert their users via the EI or AEI user interface when certificates are nearing expiration.

NOTE: There is no expectation for vendors to develop a proprietary protocol for this purpose. It is sufficient for an SS, or SC to inspect the certificate of a served EI or AEI during registration time and periodically thereafter for the duration of the signaling session. Some products may also store the certificate associated with their subscribing EIs and AEIs so as to enable this check to be performed even when the EIs and AEIs are offline.

IA-060010 [**Required: SS, SC, MG, SBC, RSF, R, AEI, LS, SD; Conditional: EI**] [**Alarm**] By default, the system shall be capable of sending this alert 60 days before the expiration of the installed credentials, which cannot be renewed automatically. This alert should be repeated periodically on a weekly or biweekly basis by default.

IA-061000 [**Required: SS, SC, MG, SBC, RSF, AEI, EI, SD; Conditional: EI**] The product shall support the capability to verify that the identity claimed in an X.509v3 certificate Subject Common Name, used to establish an authenticated and secure channel, correctly maps to the identity claimed in signaling messages transmitted within the same secure channel.

NOTE: At this time the identity claimed in an X.509v3 certificate Subject Common Name may be a FQDN, IPv4, or IPv6 address.

NOTE: The Subject Common Name is expected to "map" to the identity claimed in signaling messages, but this mapping does not mean that the Subject Common Name and the identity in the signaling messages are identical or related. For example, the identity claimed in a signaling message may be 1234567890@uc.mil, and this might be compared to a CAC Subject Common Name of Doe.John.A. 2378324324 to verify that the certificate presented in the CAC maps to the claimed phone number for authorization purposes.

IA-061010 [**Required: SS, SC, MG, SBC, EI, AEI; Conditional: EI**] The product shall support the capability to examine the identity claimed by the X.509v3 Subject Common Name field and compare it to the identity claimed within signaling messages regardless of whether the claimed identity contains an FQDN, IPv4 address, or IPv6 address.

IA-061020 [**Required: SS, SC, MG, SBC, RSF, AEI, EI**] The product shall support the capability to statically map the FQDNs contained in X.509v3 certificate Subject Common Names to IP addresses via a configurable lookup table.

NOTE: Use of DNS to map X.509v3 Subject Common name fields to IP addresses may be optionally supported in addition to this requirement. However, using DNS in this manner is not required because all MILDEP sites will not be configured to populate certificates with only DNS associated X.509 Subject Common Name FQDNs.

4.2.8 Integrity

IA-062000 [**Required: SS, SC, SBC, RSF, AEI; Conditional: EI**] The product shall be capable of using TLS for providing integrity of AS-SIP messages.

NOTE: The condition for the EI is the support of AS-SIP.

IA-062010 [**Required: SS, SC, SBC, RSF, AEI; Conditional: EI**] The product shall be capable of using Hash-Based Message Authentication Code (HMAC)-SHA1-160 with 160 bit keys.

IA-063000 [**Conditional: SS, SC, EI, AEI**] If the product uses H.323, then the product shall be capable of using H.235.1 Baseline Security Profile guidance for mutually authenticated shared keys and HMAC-SHA1-96 with 160 bit keys.

IA-064000 [**Required: EI, AEI, MG, SS**] The product shall be capable of providing data integrity of the Secure Real-Time Transport Protocol (SRTP) bearer (transport) packets.

IA-064010 [**Required: EI, AEI, MG, SS**] The product shall be capable of using HMAC-SHA1-32 for the authentication tag with 160 bit key length as the default integrity mechanism for SRTP packets.

IA-064020 [**Required: EI, AEI, MG, SS**] The product shall be capable of using HMAC-SHA1-80 for the authentication tag with 160 bit key length as the default integrity mechanism for Secure Real-Time Transport Control Protocol (SRTCP).

NOTE: The ability to process received SRTCP messages is optional, but the capability to transmit SRTCP messages is required.

IA-065000 [**Conditional: SS, SC, MG, SD**] If the product uses IP Security (IPSec), then the product shall be capable of using HMAC-SHA (class value 2) (Reference Appendix A of RFC 2409 for the definition of 'Class Value 2') as the default Internet Key Exchange (IKE) integrity mechanism as defined in RFC 2409.

IA-066000 [**Required: SS, SC, MG, SBC, RSF, R, LS, SD**] The entire SNMPv3 message shall be checked for integrity and shall use the HMAC-SHA1-96 with 160-bit key length by default.

IA-067000 [**Conditional: SS, SC, MG, SBC, RSF, R, LS, SD**] If the product uses SSHv2, then the product shall use HMAC-SHA1-96 with 160 bit key length for data integrity.

IA-068000 [**Removed**~~**Conditional: SS, SC, MG, SBC, RSF, EI, AEI, SD**~~] ~~If the product uses TLS, then the product shall be capable of using TLS in combination with HMAC-SHA1-160 with 160 bit keys to provide integrity for the session packets.~~

4.2.9 Confidentiality

IA-069000 [**Required: EI, AEI, MG**] The product shall be capable of providing confidentiality for media streams using SRTP with either the AES_CM_128 encryption algorithm as the default.

IA-069010 [**Required: SS, SC, MG, EI, AEI**] The product shall be capable of distributing the Master Key and the Salt Key in the VVoIP signaling messages IAW RFC 4568.

IA-069020 [**Required: SS, SC, MG, EI, AEI**] The product shall be capable of distributing the Master Key and the Salt Key in concatenated form.

IA-069030 [**Required: EI, AEI, MG**] The product shall use a Master Key of 128 bits to support 128-bit Advanced Encryption Standard (AES) encryption.

NOTE: This implies that the Master Salt Key may be null.

IA-069040 [**Required: EI, AEI, MG**] The Master Key and a random Master Salt Key shall be supported for SRTP sessions.

IA-069050 [**Required: SS, SC, SBC, MG, AEI, EI**] When the system assigns the port numbers to a session, the system shall assign the SRTP port ranges within a configurable range between 2048 and 65535 with the default between: 16384 to 32764.

IA-070000 [**Conditional: SS, SC, MG, EI, AEI**] If H.323, Media Gateway Control Protocol (MGCP), or H.248 (MEGACO) is used, then the product shall be capable of using IPSec to provide confidentiality.

IA-070010 [**Conditional: SS, SC, MG**] If the product uses H.248 (MEGACO), then the product shall be capable of distributing the SRTP Master Key and Salt Key in the SDP "k =" crypto field when using H.248.15.

IA-070020 [**Conditional: SS, SC, MG, EI, AEI**] If H.323 is used, then the product shall be capable of distributing the SRTP Master Key and Salt Key in H.235 using the H235Key as described in H.235.0 and H.235.8.

IA-071000 [**Conditional: SS, SC, MG, SBC, RSF, R, LS, AEI, EI, SD**] If IPSec is used, then the product shall be capable of using IKE for IPSec key distribution:

IA-071010 [**Required: SS, SC, MG, SBC, RSF, R, LS, AEI, EI, SD**] The product shall be capable of using IKE version 1.

IA-071020 [**Removed**~~**Conditional: SS, SC, MG, SBC, RSF, R, LS, AEI, EI, SD**~~] ~~If IPSec is used, then the product shall be capable of using the digital signature authentication mode with X.509 certificates during Phase I of the Internet Security Association and Key Management Protocol (ISAKMP) negotiation for authentication.~~

IA-071030 [**Conditional: SS, SC, MG, SBC, RSF, R, LS, AEI, EI, SD**] If IPSec is used, then the product shall be capable of using the Quick Mode as the default Phase II Security Association mechanism for the IPSec service.

IA-071040 [**Conditional: SS, SC, MG, SBC, RSF, R, LS, AEI, EI, SD**] If IPSec is used, then the product shall be capable of using and interpreting certificate requests for Public-Key Cryptography Standard #7 (PKCS#7) wrapped certificates as a request for the whole path of certificates.

IA-071050 [**Conditional: SS, SC, MG, SBC, RSF, R, LS, AEI, EI, SD**] If IPSec is used, then the product shall be capable of using Main Mode associated with the Diffie-Hellman approach for key generation for the security association negotiation.

IA-071060 [**Conditional: SS, SC, MG, SBC, RSF, R, LS, AEI, EI, SD**] If IPSec is used, then the product shall be capable of using Diffe-Hellman Groups 1, 2, and 14, at a minimum.

IA-071070 [**Conditional: SS, SC, MG, FW, IPS, VPN, NAC**] If the product uses IPSec, then the system shall be capable of using AES_128_CBC as the default encryption algorithm. The system shall be capable of supporting 3DES-CBC (class value 5) for backwards compatibility with previous UCR revisions.

IA-071080 [**Removed**~~**Conditional: SS, SC, MG, SBC, RSF, R, LS, AEI, EI, SD**~~]
~~[**Former ID: 5.4.6.2.3 1.c.1.c.vi.A**] If IPSec is used, then the product shall only support the following erroneous messages associated with a certificate request:~~

~~(1) Invalid Key.~~

~~(2) Invalid ID.~~

~~(3) Invalid certificate encoding.~~

~~(4) Invalid certificate.~~

~~(5) Certificate type unsupported.~~

~~(6) Invalid CA.~~

~~(7) Invalid hash.~~

~~(8) Authentication failed.~~

~~(9) Invalid signature.~~

~~(10) Certificate unavailable.~~

IA-072000 [**Required: SS, SC, MG, SBC, RSF, AEI**] The product shall be capable of using TLS (dual path method) to provide confidentiality for the AS-SIP as described in RFC 3261.

NOTE: Upon receipt of an INVITE over a TLS-established session, an SC shall respond to the INVITE (and any subsequent requests received over that TLS path) using this TLS session. If the SC originates an INVITE or request, then it shall establish a separate and unique TLS session, and the SC shall expect to receive a response to its request over this new TLS session. Two TLS sessions are established for communications between the SC and the SBC, MFSS and SBC, SC and SC, SC to AEI via RSF, or SBC and SBC. Since the AEI is required to support the dual path method, it has to act as both a SIP client and server and must support both TLS client and server functionality. Due to the proprietary nature of line side IP solutions implemented by EIs, EI vendors may support TLS reuse or the dual path method described in this requirement for line side implementations. The details associated with the reuse method are described in http://tools.ietf.org/html/rfc5923.

IA-072010 [**Required: SS, SC, MG, SBC, RSF, AEI; Conditional: EI**] The underlying protocol for AS-SIP shall be the TCP.

IA-072020 [**Required: SS, SC, MG, SBC, RSF, AEI; Conditional: EI**] The product shall be capable of using as its default cipher suite TLS_RSA_WITH_AES_128_CBC_SHA.

IA-072030 [**Required: SS, SC, MG, SBC, RSF, AEI; Conditional: EI**] The product shall be capable of using a default of no compression for AS-SIP messages.

IA-072040 [**Required: SS, SC, MG, SBC, RSF, AEI; Conditional: EI**] The product shall be capable of exchanging AS-SIP TLS messages in a single exchange or multiple exchanges.

IA-072050 [**Required: SS, SC, MG, SBC, RSF, AEI; Conditional: EI**] The product shall be capable of distributing the SRTP Master Key and Salt Key in the AS-SIP message using the SDP crypto= field.

NOTE: EI condition is whether it supports AS-SIP.

IA-072060 [**Conditional: SS, SC, EI, SBC, RSF, AEI**] If AS-SIP is used, then the product shall transmit only packets that are secured with TLS and use port 5061.

NOTE: The products may use other signaling protocols for interfacing to e.g. MGs, EIs.

IA-072070 [**Required: SS, SC, EI, SBC, RSF, AEI**] The product shall reject all received AS-SIP packets associated with port 5061 that are not secured with TLS.

NOTE: This ensures that the product does not process UDP, Stream Control Transmission Protocol (SCTP), and TCP SIP packets that are not secured using a combination of TLS and TCP.

IA-072080 [**Required: SS, SC, EI, SBC, RSF, AEI**] The product shall only accept and process AS-SIP packets that arrive on port 5061.

NOTE: The product should discard AS-SIP packets that arrive on a different port.

IA-072090 [**Required: RSF**] The product shall support both the reuse and dual path TLS methods.

NOTE: This is required of an RSF since it has to support TLS sessions between the SC and AEI and Proprietary IP Voice EIs (PEIs). The AEI uses the dual path method and PEIs have the option of using the reuse method.

IA-073000 [**Conditional: SS, SC, MG, SBC, RSF, R, LS, AEI, EI, SD**] If the product uses TLS, then the product shall do so in a secure manner as defined by the following subtended requirements.

IA-073010 [**Conditional: SS, SC, MG, SBC, RSF, R, LS, EI, AEI, SD**] If the product uses TLS, then the system shall be capable of using TLS_RSA_WITH_AES_128_CBC_SHA as its default cipher suite.

IA-073020 [**Conditional: SS, SC, MG, SBC, RSF, R, LS, AEI, EI, SD**] If the product uses TLS, then the system shall be capable of using a default of no compression.

IA-073030 [**Conditional: SS, SC, MG, SBC, RSF, R, LS, AEI, EI, SD**] If the product uses TLS, then the system shall be capable of exchanging TLS messages in a single exchange or multiple exchanges.

IA-073040 [**Conditional: SS, SC, MG, SBC, RSF, R, LS, AEI, EI, SD**] If TLS session resumption is used, then a timer associated with TLS session resumption shall be configurable and the default shall be 1 hour.

NOTE: This requirement is not associated with NM-related sessions.

IA-073050 [**Conditional: SS, SC, MG, SBC, RSF, R, LS, AEI, EI, SD**] If TLS session resumption is used, then the maximum time allowed for a TLS session to resume (session resumption) without repeating the TLS authentication/confidentiality/authorization process (e.g., a full handshake) is 1 hour.

IA-073060 [**Required: SS, SC, MG, SBC, RSF, R, LS, AEI, EI, SD**] If the product supports SSL/TLS renegotiation, then the product shall support the capability to disable this feature or the product shall support RFC 5746.

NOTE: Supporting RFC 5746 includes providing a configurable option to terminate a TLS session if the peer does not support the "renegotiation_info" extension.

IA-074000 [**Conditional: SS, SC, MG, SBC, RSF, EI, AEI, R, LS, SD**] If the product uses Secure Shell (SSH), then the system shall do so in a secure manner as defined by the following subtended requirements.

NOTE: An EI's remote manual configurations shall not be enabled and all non-automatic processes shall be performed locally.

IA-074010 [**Conditional: SS, SC, MG, SBC, RSF, EI, AEI, R, LS, SD**] If the product uses SSH, then the system shall be capable of supporting the RSA 2,048-bit key algorithm and the Diffie-Hellman 2,048 bit key algorithm.

IA-074020 [**Conditional: SS, SC, MG, SBC, RSF, EI, AEI, R, LS, SD**] If the product uses SSH, then a client shall close the session if it receives a request to initiate an SSH session whose version is less than 2.0.

NOTE: Closing the session may be either a default behavior or a configurable option. If this is a configurable option, then the conditions of fielding should clearly specify that this option must be configured.

IA-074030 [**Conditional: SS, SC, MG, SBC, RSF, EI, AEI, R, LS, SD**] If the product uses SSH, then the SSH sessions shall rekey at a minimum every gigabyte of data received or every 60 minutes, whichever comes sooner.

IA-074040 [**Conditional: SS, SC, MG, SBC, RSF, EI, AEI, R, LS, SD**] If the product uses SSH, then the SSH sessions shall rekey at a minimum every gigabyte of data transmitted or every 60 minutes, whichever comes sooner.

IA-074050 [**Conditional: SS, SC, MG, SBC, RSF, EI, AEI, R, LS, SD**] If the product uses SSH, then the SSH sessions shall minimally support the AES 128-CBC algorithm as defined in RFC 4253.

IA-074070 [**Conditional: SS, SC, MG, SBC, RSF, EI, AEI, R, LS, SD**] If the product uses SSH, then the SSH sessions shall use TCP as the underlying protocol.

IA-074080 [**Removed**~~**Conditional: SS, SC, MG, SBC, RSF, EI, AEI, R, LS, SD**~~] ~~If the product uses SSH, then it shall be capable of processing packets with uncompressed payload lengths up to 32,768 bytes or shall be configurable to specify that value; also,~~

~~this length shall be the default value. This does not preclude the system from automatically sizing the Maximum Transmission Unit (MTU) if it is less than 32,768.~~

IA-074090 [**Removed**~~**Conditional: SS, SC, SBC, RSF, EI, AEI, R, LS, MG, SD**~~] ~~If the product uses SSH, then the SSH packets shall have a maximum packet size of 35,000 bytes or shall be configurable to that value; also, this length shall be the default value.~~

~~NOTE: The 35,000 bytes includes the packet_length, padding_length, payload, random padding, and MAC.~~

IA-074100 [**Conditional: SS, SC, MG, SBC, RSF, EI, AEI, R, LS, SD**] If the product uses SSH, then the product shall discard SSH packets that exceed the maximum packet size to avoid denial of service (DoS) attacks or buffer overflow attacks.

IA-074110 [**Conditional: SS, SC, MG, SBC, RSF, EI, AEI, R, LS, SD**] If the product uses SSH, then the SSH packets shall use random bytes if packet padding is required.

IA-074120 [**Conditional: SS, SC, MG, SBC, RSF, EI, AEI, R, LS, SD**] If the product uses SSH, then the system shall treat all SSH-encrypted packets sent in one direction as a single data stream. For example, the initialization vectors shall be passed from the end of one packet to the beginning of the next packet.

IA-074130 [**Conditional: SS, SC, MG, SBC, RSF, EI, AEI, R, LS, SD**] If the product uses SSH, then the system shall be capable of setting Diffie-Hellman-Group14-SHA1 as the preferred key exchange mechanism for SSH.

IA-075000 [**Conditional: SS, SC, MG, SBC, RSF, R, LS, SD**] If the product uses SSH with X.509v3 certificates and provides an SSH server function, then the SSH server shall support the capability to use an X.509v3 certificate provided by a DoD-approved PKI.

IA-075010 [**Conditional: SS, SC, MG, SBC, RSF, LS, R, SD**] If the product uses SSH with X.509v3 certificates and provides an SSH server function, then the SSH Server function shall support, at a minimum, the “x509v3-ssh-rsa” and "x509v3-rsa2048-sha256” key types as defined in RFC 6187

IA-075020 [**Conditional: SS, SC, MG, SBC, RSF, R, LS, SD**] If the product uses SSH with X.509v3 certificates and provides an SSH server fuction, then the SSH Server function shall support the capability to, in a configurable manner, specify the highest preferred key type advertised during the SSH_MSG_KEXINIT message exchange.

IA-075030 [**Conditional: SS, SC, MG, SBC, RSF, R, LS, SD**] If the product uses SSH with X.509v3 certificates and provides an SSH server function, then the SSH server function shall support the capability to deny SSH sessions when the session fails to negotiate a configured set of preferred key types.

IA-076000 [**Conditional: SS, SC, MG, SBC, RSF, R, LS, SD**] If the product uses SSH with X.509v3 certificates and provides an SSH server function, then the SSH client shall support the capability to use an X.509v3 certificate provided by a DoD-approved PKI.

IA-076010 [**Conditional: SS, SC, MG, SBC, RSF, R, LS, SD**] If the product provides an SSH client function and the SSH client has a CAC (or equivalent) reader, then the SSH client may use the X.509v3 certificate on the user's CAC to establish the encrypted session.

IA-076020 [**Conditional: SS, SC, MG, SBC, RSF, R, LS, SD**] If the product uses SSH and if the client has a CAC (or equivalent) reader and also has its own PKI certificate from a DoD-approved PKI, then the client may use either its certificate or the certificate on the user's CAC to establish the encrypted sessions.

IA-076030 [**Conditional: SS, SC, MG, SBC, RSF, R, LS, SD**] If the product uses SSH with X.509v3 certificates,and provides an SSH client function, then the SSH client shall support, at a minimum, the "x509v3-ssh-rsa" and "x509v3-rsa2048-sha256" key types as defined in RFC 6187.

IA-077000 [**Required: SS, SC, MG, SBC, RSF, R, LS, SD**] The product shall be capable of using SNMPv3 for all SNMP sessions.

NOTE: If the product is using Version 1 or Version 2 (instead of SNMPv3) with all of the appropriate patches to mitigate the known security vulnerabilities, then any findings associated with this requirement may be downgraded. In addition, if the product has developed a migration plan to implement Version 3, then any findings associated with this requirement may be further downgraded.

IA-077010 [**Required: SS, SC, MG, SBC, RSF, R, LS, SD**] The security level for SNMPv3 in the DoD VVoIP environment shall be authentication with privacy – snmpSecurityLevel=authPriv. The product shall set snmpSecurityLevel=authPriv as the default security level used during initial configuration.

IA-077020 [**Required: SS, SC, MG, RSF, R, LS, SBC, SD**] The SNMPv3 implementation shall be capable of allowing an appropriate administrator to manually configure the snmpEngineID from the operator console. A default unique snmpEngineID may be assigned to avoid unnecessary administrative overhead, but this must be changeable.

IA-077030 [**Required: SS, SC, MG, SBC, RSF, R, LS, SD**] The security model for SNMPv3 shall be the User-Based Security Model – snmpSecurityModel=3.

IA-077040 [**Conditional: SS, SC, MG, SBC, RSF, R, LS, SD**] If the product receives SNMPv3 response messages, then the product shall conduct a timeliness check on the SNMPv3 message.

IA-077050 [**Required: SS, SC, MG, SBC, RSF, R, LS, SD**] An SNMPv3 engine shall perform time synchronization using authenticated messages.

IA-077060 [**Required: SS, SC, MG, SBC, RSF, R, LS, SD**] The message processing model shall be SNMPv3 – snmpMessageProcessingModel=3.

IA-077070 [**Required: SS, SC, MG, SBC, RSF, R, LS, SD**] For backwards compatibility, the product shall support the capability to use Data Encryption Standard-Cipher Block Chaining (DES-CBC) (usmDESPrivProtocol) with a 16 octet (128 bit) input key, as specified in RFC 3414, as an encryption cipher for SNMPv3.

IA-077080 [**Required: SS, SC, MG, SBC, RSF, R, LS, SD**] The product shall support the capability to use the CFB-AES128 encryption cipher usmAesCfb128PrivProtocol for SNMPv3 as defined in RFC 3826 and specify this as the default encryption cipher for SNMPv3.

IA-077090 [**Conditional: SS, SC, MG, SBC, RSF, R, LS, SD**] If the product receives SNMPv3 response messages, then the SNMPv3 engine shall discard SNMP response messages that do not correspond to any current outstanding Request messages.

IA-077100 [**Conditional: SS, SC, MG, SBC, RSF, R, LS, SD**] If the product receives SNMPv3 responses, then the SNMPv3 Command Generator Application shall discard any Response Class Protocol Data Unit (PDU) for which there is no outstanding Confirmed Class PDU.

IA-077110 [**Required: SS, SC, MG, SBC, RSF, R, LS, SD**] When using msgID for correlating Response messages to outstanding Request messages, the SNMPv3 engine shall use different msgIDs in all such Request messages that it sends out during a 150 second Time Window.

IA-077120 [**Required: SS, SC, MG, SBC, RSF, R, LS, SD**] An SNMPv3 Command Generator or Notification Originator Application shall use different request-ids in all Request PDUs that it sends out during a Time Window.

IA-077130 [**Required: SS, SC, MG, SBC, RSF, R, LS, SD**] When sending state altering messages to a managed authoritative SNMPv3 engine, a Command Generator Application should delay sending successive messages to that managed SNMPv3 engine until a positive acknowledgement is received from the previous message or until the message expires.

IA-077140 [**Required: SS, SC, MG, SBC, RSF, R, LS, SD**] The product using SNMPv3 shall implement the key-localization mechanism.

IA-078000 [**Conditional: SS, SC, MG, SBC, RSF, R, LS, AEI, EI, SD**] If the product uses web browsers or web servers, then the product web browsers and web servers shall be capable of supporting TLS 1.0 or higher for confidentiality.

IA-079000 [**Required: SS, SC, MG, SBC, RSF, R, LS, SD**] The product shall be capable of using SSHv2 or TLS 1.0 or higher for remote configuration of appliances.

NOTE: The EIs and AEIs remote manual configurations shall not be enabled and all non-automatic processes shall be performed locally.

IA-080000 [**Conditional: SS, SC, MG**] If the product uses different signaling protocols (i.e., H.323 and AS-SIP), then the system shall be capable of translating or transferring the bearer keys between different signaling protocols.

IA-081000 [**Conditional: SS, SC, MG, EI, AEI**] If the product is the originating party and receives a 181 message indicating that the call is being forwarded, then, upon completion of the session establishment between the originating party and the forwarded-to party, the originating party must initiate a rekeying.

NOTE: The rekeying is designed to prevent the "forwarding party" from having the key to the bearer session associated with the originating party and the forwarded-to party. If the forwarding party had the key to the bearer session, then the forwarding party would be able to eavesdrop on the forwarded session. SCs, and SS may act as a B2BUA for an EI or an AEI and so would originate the AS-SIP session on behalf of the EI or AEI.

IA-082000 [**Conditional: EI, AEI**] If the EI or AEI acts as a bridge or a MCU, then it shall establish a unique key for each EI or AEI connection.

IA-083000 [**Conditional: SBC**] If the product transmits decrypted VVoIP signaling and/or bearer traffic to an external IDS/IPS, then confidentiality for the decrypted signaling and media traffic shall be ensured using cryptographic protection, where the strength of the cryptographic protocol/algorithms used is greater than or equal to the TLS and SRTP cryptographic profiles defined in this document.

4.2.10 Non-Repudiation

IA-084000 [**Required: SS, SC, MG, SBC, RSF, R, LS, SD**] The security log shall be capable of using a circular (or equivalent) recording mechanism (i.e., oldest record overwritten by newest).

IA-085000 [**Required: SS, SC, MG, SBC, RSF, R, LS, SD**] Only the System Security Administrator and System Administrator roles shall have the ability to retrieve, print, copy, and upload the security log(s)

IA-086000 [**Required: SS, SC, MG, SBC, RSF, R, LS, SD**] The product/system shall be able to generate a human understandable presentation of any audit data stored in the audit trail.

IA-087000 [**Required: SS, SC, MG, SBC, RSF, R, LS, SD**] The product shall provide a mechanism to locally store audit log/event data when communication with the management station is unavailable.

NOTE: In the case of protocols that use unreliable delivery, such as syslog over UDP, use of mechanisms at lower Open System Interconnect (OSI) layers (e.g. ICMP, OSI Layer 1 and 2 mechanisms) must be used to detect such connectivity issues.

SECTION 5
IPV6

5.1 INTRODUCTION

This section describes the IPv6 requirements for Sensitive but Unclassified (SBU) Unified Capabilities (UC) subsets provided by all products and technologies used to send and receive or to support voice, video, or data across Department of Defense (DoD) networks that provide UC services.

5.2 IPV6

The system requirements specified in Section 2, Session Control Products, are the minimum set of requirements necessary for the system to be Internet protocol (IP) version 6 (IPv6) capable for Video and Voice over IP (VVoIP). An implementer may choose to specify additional IPv6 requirements based on its non-VVoIP or unique VVoIP requirements. Also, a vendor may choose to implement additional IPv6 functions based on its commercial market. This section focuses on the "deltas" between an IPv6 implementation and an IPv4 implementation, and does not address consistencies or inconsistencies between IPv4 and IPv6.

When the [Alarm] tag appears after a requirement's applicability statement, the guidance from Section 4.2.1, The [Alarm] Tag: Generation of Alarms, is to be followed.

The requirements defined in Section 2, Session Control Products, are associated with the external interfaces of the UC products or network appliances. For defining each requirement, the terms "UC products" and "Network Appliance (NA)" are shortened to "system." As shown in Figure 2.1-1, High-Level DISN Assured Services Network Model, the external interfaces for an NA are generally considered to be interfaces that connect to and interact with the Assured Services Local Area Network (ASLAN) or the non-ASLAN. The primary interfaces associated with the IPv6 requirements are the signaling: UC Session Initiation Protocol (SIP) and bearer: Secure Real-Time Transport Protocol (SRTP) interfaces.

Whenever a reference to a specific Request for Comments (RFC) appears in a UC Requirements (UCR) requirement, the specific language of the UCR document and its subtended requirements should be understood within the context of the RFC.

Finally, the acronyms used for designating the various UC Products are shown in Table 5.2-1, IPv6 Requirements for UC Products.

Table 5.2-1. IPv6 Requirements for UC Products

UC PRODUCT	IPV6 REQUIREMENTS
SBU IP-Based UC Product	
Softswitch (SS)	Must be IPv6-capable. Use guidance in Table 5.2-4 for NA/SS.
Session Controller (SC) including Master SC (MSC), Subtended SC (SSC), and Deployable SC (DSC)	The SC/Call Connection Agent (CCA) application in conjunction with the VVoIP EI and Media Gateway (MG) must be IPv6-capable. Use guidance in Table 5.2-4 for NA/SS.
Router (R)	Must be IPv6-capable. Use guidance in Table 5.2-5 for Routers.
Customer Edge (CE) Router (CE-R)	Must be IPv6-capable. Use guidance in Table 5.2-5 for Routers.
Assured Services (AS) Session Initiation Protocol (SIP) (AS-SIP) End Instrument (AEI)	The EI in conjunction with the Call Connection Agent (CCA) application must be IPv6-capable. Use guidance in Table 5.2-3 for EI.
Secure End Instrument (SEI)	Same as AEI, above.
Extensible Messaging and Presence Protocol (XMPP) Server/Client	Must be IPv6-capable. Use guidance in Table 5.2-4 for NA/SS.
AS-SIP Time Division Multiplexing (TDM) gateway (AS-SIP TDM GW)	If the AS-SIP TDM GW has an IP interface, then the AS-SIP TDM GW must be IPv6-capable. Use guidance in Table 5.2-4 for NA/SS.
AS-SIP IP Gateway (AS-SIP IP GW)	Must be IPv6-capable. Use guidance in Table 5.2-4 for NA/SS.
Collaboration Product (Server Component)	Must be IPv6-capable. Use guidance in Table 5.2-4 for NA/SS.
Collaboration Product (Client Component)	Must be IPv6-capable. Use guidance in Table 5.2-3 for EI.
LAN Product	
LAN Switch (LS)	Must be IPv6-capable. Use guidance in Table 5.2-6.
LAN Access Switch	Must be IPv6-capable. Use guidance in Table 5.2-6 Part 1 for LAN Access Switch and Section 7.2.1.5, Protocols.
LAN Distribution Switch	Must be IPv6-capable. Use guidance in Table 5.2-6 Part 2 for LAN Distribution Switches and Section 7.2.1.5, Protocols.
LAN Core Switch	Must be IPv6-capable. Use guidance in Table 5.2-6 Part 3 for LAN Core Switches and Section 7.2.1.5, Protocols.
Wireless LAN Product	

UC PRODUCT	IPV6 REQUIREMENTS
Wireless LAN Access Switch (WLAS)	Must be IPv6-capable. Use guidance in Table 5.2-6 Part 1 for LAN Access Switch.
Wireless LAN Access Bridge (WAB)	Must be IPv6-capable. Use guidance in Table 5.2-4 for NA/SS.
Wireless End Instrument (WEI)	Must be IPv6-capable. Same as AEI, above.
Peripheral Products	
Customer Premises Equipment (CPE)	If the CPE has an IP interface, then the CPE must be IPv6-capable. Use guidance in Table 5.2-4 for NA/SS.
Integrated Access Switch (IAS)	Must be IPv6-capable. Use guidance in Table 5.2-4 for NA/SS.
AS-SIP IP Gateway (GW)	Must be IPv6-capable. Use guidance in Table 5.2-4 for NA/SS.
AS-SIP TDM Gateway (GW)	Must be IPv6-capable. Use guidance in Table 5.2-4 for NA/SS.
Signaling Multipoint Control Unit (SMCU)	If the SMCU has an IP interface, then the SMCU must be IPv6-capable. Use guidance in Table 5.2-4 for NA/SS.
DoD Secure Communications Device (DSCD)	Same as SEI, above.
UC Conference System (UCCS)	Must be IPv6-capable. Use guidance in Table 5.2-4 for NA/SS.
UC External Adjunct Devices	UC External Adjunct Devices that are not covered under CPE [such as a Lightweight Directory Access Protocol (LDAP) server, local directory services server] are to be covered under DoD IPv6 Profile for Net App or Simple Server. Use guidance in Table 5.2-4 for NA/SS.
Network monitoring for IPv6 data/voice networks	Must be IPv6-capable. Use guidance in Table 5.2-4 for NA/SS.
Instant Messaging, Chat, and Presence/Awareness Features	Must be IPv6-capable. Use guidance in Table 5.2-4 for NA/SS.
Real-Time Services (RTS) Routing Database	Must be IPv6-capable. Use guidance in Table 5.2-4 for NA/SS.
UC Tool Suite	Must be IPv6-capable. Use guidance in Table 5.2-4 for NA/SS.
E911 Management System	Must be IPv6-capable. Use guidance in Table 5.2-4 for NA/SS.
Network Infrastructure Products	
Multiservice Provisioning Platform (MSPP)	If the MSPP has an IP interface, then the MSPP must be IPv6-capable. Use guidance in Table 5.2-4 for NA/SS.
Optical Digital Cross-Connect (ODXC)	If the ODXC has an IP interface, then the ODXC must be IPv6-capable. Use guidance in Table 5.2-4 for NA/SS.
Provider Router/Provider Edge Router (P/PE Router)	Must be IPv6-capable. Use guidance in Table 5.2-5 for Router.
DISN Optical Transport Switch (OTS)	If the OTS has an IP interface, then the OTS must be IPv6-capable. Use guidance in Table 5.2-4 for NA/SS.

UC PRODUCT	IPV6 REQUIREMENTS
Transport Switch Function (TSF)	If the TSF has an IP interface, then the TSF must be IPv6-capable. Use guidance in Table 5.2-4 for NA/SS.
Aggregate Grooming Function (AGF)	If the AGF has an IP interface, then the AGF must be IPv6-capable. Use guidance in Table 5.2-4 for NA/SS.
Access Aggregation (AAG) Function	If the AAG has an IP interface, then the AAG must be IPv6-capable. Use guidance in Table 5.2-4 for NA/SS.
Timing and Synchronization (T&S)	If the T&S has an IP interface, then the T&S must be IPv6-capable. Use guidance in Table 5.2-4 for NA/SS.
Tactical UC Product	
Deployable Network Element (D-NE)	Must be IPv6-capable. Use guidance in Table 5.2-4 for NA/SS.
Deployable LAN (DLAN) Products and infrastructure	Must be IPv6-capable. Use guidance from LAN Products, above.
Deployed Tactical Radio (DTR)	Must be IPv6-capable. Use guidance in Table 5.2-4 for NA/SS.
Deployable Cellular Voice Exchange (DCVX)	Must be IPv6-capable. Use guidance in Table 5.2-4 for NA/SS.
Multifunction Mobile Devices	
Multifunction Mobile Device	Must be IPv6-capable. Use guidance in Table 5.2-3 for EI.
Multifunction Mobile Device Backend Support System (MBSS)	Must be IPv6-capable. Use guidance in Table 5.2-3 for EI.
Security Devices (SDs)	
High Assurance IP Encryptor (HAIPE)	Must be IPv6-capable. Use guidance in Table 5.2-7.
Link Encryptor Family (LEF)	Must be IPv6-capable. Use guidance in Table 5.2-7.
Session Border Controller (SBC)	Must be IPv6-capable. Use guidance in Table 5.2-7 and in UCR 2013, Section 13, Security Devices.
Firewall (FW)	Must be IPv6-capable. Use guidance in Table 5.2-7 and in UCR 2013, Section 13, Security Devices.
Intrusion Protection System (IPS) and Intrusion Detection System (IDS)	Must be IPv6-capable and must be capable of inspecting IPv4 and IPv6 packets simultaneously, and those packets contained within tunnels that are not encrypted (e.g., GRE, IPSec AH, IP in IP) or shall support the capability to alarm if tunneled packets are detected that could not be inspected further. Use guidance in Table 5.2-7 and in UCR 2013, Section 13, Security Devices.
Virtual Private Network (VPN) Concentrator	Must be IPv6-capable. Use guidance in Table 5.2-7 and in UCR 2013, Section 13, Security Devices.
Network Access Control (NAC)	Must be IPv6-capable. Use guidance in Table 5.2-7 and in UCR 2013, Section 13, Security Devices.
Integrated Security Solution (ISS)	Must be IPv6-capable. Use guidance in Table 5.2-7 and in UCR 2013, Section 13, Security Devices.
Information Assurance Tools (IATs)	Must be IPv6-capable. Use guidance in UCR 2013, Section 13, Security Devices.

UC PRODUCT	IPV6 REQUIREMENTS
RTS Stateful Firewall (RSF)	Must be IPv6-capable. Use guidance in Table 5.2-7 and in UCR 2013, Section 13, Security Devices.
Storage Devices	
Data Storage Controller (DSC)	Must be IPv6 capable. Use guidance in Table 5.2-4 for NA/SS.
Network Elements	
Assured Services Network Element (AS-NE)	Must be IPv6 capable. Use guidance in Table 5.2-4 for NA/SS.
Defense Switched Network (DSN) Fixed Network Element (F-NE)	Must be IPv6-capable. Use guidance in Table 5.2-4 for NA/SS.
Classified Products	
Classified Session Controller (SC)	Same as SC, above.
Classified Core Switch	Same as LAN Core Switch, above.
Classified Distribution Switch	Same as LAN Distribution Switch, above.
Classified Access Switch	Same as LAN Access Switch, above.
Classified Session Border Controller (SBC)	Same as SBC, above.
Classified CE-R	Same as CE-R, above.
Secure UC Conference System (UCCS)	Same as UCCS, above.
Secure Multi Signaling Multipoint Control Unit (SMCU)	Same as SMCU, above.
Network Management	
Element Management System (EMS)	Conditional, dependent on the vendor's decision to use IPv6 for NM.
VVoIP EMS	Conditional, dependent on the vendor's decision to use IPv6 for NM.

5.2.1 Product

IP6-000010 [**Required: EI, NA/SS, R, SD**] The product shall support dual IPv4 and IPv6 stacks as described in RFC 4213. [**Conditional: LS**] If the Local Area Network (LAN) Switch (LS) also supports a routing function, then the product shall also support dual IPv4 and IPv6 stacks as described in RFC 4213.

NOTE: The tunnel requirements are associated only with appliances that provide IP routing functions (e.g., routers). The primary intent of these requirements is to (1) require dual stacks on all UC appliances and (2) allow dual stacks and tunneling on routers.

IP6-000020 [**Required: EI, NA/SS, LS, SD**] Dual-stack end points or Call Connection Agents (CCAs) shall be configured to choose IPv4 over IPv6.

IP6-000030 [**Required: EI, NA/SS, R, LS, SD**] All nodes and interfaces that are "IPv6-capable" must be carefully configured and verified that the IPv6 stack is disabled until it is deliberately enabled as part of a deliberate transition strategy. This includes the stateless autoconfiguration of link-local addresses. Nodes with multiple network interfaces may need to be separately configured per interface.

IP6-000040 [**Conditional: R, LS**] If the LS supports a routing function, then the product shall support the manual tunnel requirements as described in RFC 4213.

IP6-000050 [**Required: EI, NA/SS, R, LS, SD**] The system shall provide the same (or equivalent) functionality in IPv6 as in IPv4 consistent with the requirements in the UCR for its Approved Products List (APL) category.

NOTE: This requirement applies only to products that are required to perform IPv6 functionality and the feature parity is limited to the functionality tested in accordance with the distributed test laboratory approved test procedures for the category of the product.

IP6-000060 [**Required: EI, NA/SS, R, SD**] The product shall support the IPv6 format as described in RFC 2460 and updated by RFC 5095. [**Conditional: LS**] If the LS also supports a routing function, then the product shall support RFC 2460 and be updated by RFC 5095.

IP6-000070 [**Required: EI, NA/SS, R, LS, SD**] The product shall support the transmission of IPv6 packets over Ethernet networks using the frame format defined in RFC 2464.

NOTE: This requirement does not mandate that the remaining sections of RFC 2464 have to be implemented.

5.2.1.1 Maximum Transmission Unit

IP6-000080 [**Required: EI (Softphone Only), R, LS, SD**] The product shall support Path Maximum Transmission Unit (MTU) Discovery as described in RFC 1981.

IP6-000090 [**Required: EI, NA/SS, R, LS, SD**] The product shall support a minimum MTU of 1280 bytes as described in RFC 2460 and updated by RFC 5095.

NOTE: Guidance on MTU requirements and settings can be found in Section 6.11.4.2, Layer 2 – Data Link Layer.

IP6-000100 [**Conditional: EI, NA/SS, SD**] If Path MTU Discovery is used and a "Packet Too Big" message is received requesting a next-hop MTU that is less than the IPv6 minimum link MTU, then the product shall ignore the request for the smaller MTU and shall include a fragment header in the packet.

NOTE: Unlike IPv4, fragmentation in IPv6 is performed only by source nodes, not by routers along a packet's delivery path.

5.2.1.2 Flow Label

IP6-000110 [**Required: EI, NA/SS, R, LS, SD**] The product shall not use the Flow Label field as described in RFC 2460.

IP6-000120 [**Required: EI, NA/SS, R, LS, SD**] The product shall be capable of setting the Flow Label field to zero when originating a packet.

IP6-000130 [**Required: R, LS**] The product shall not modify the Flow Label field when forwarding packets.

IP6-000140 [**Required: EI, NA/SS, R, LS, SD**] The product shall be capable of ignoring the Flow Label field when receiving packets.

5.2.1.3 Address

IP6-000150 [**Required: EI, NA/SS, R, LS, SD**] The product shall support the IPv6 Addressing Architecture as described in RFC 4291.

NOTE 1: According to "DoD IPv6 Standard Profiles For IPv6-capable Products-Supplemental Guidance" version 6.0, the use of "IPv4-mapped" addresses "on-the-wire" is discouraged due to security risks raised by inherent ambiguities.

NOTE 2: As noted in National Institute of Standards and Technology (NIST) Special Publication (SP) 500-267 25, "A Profile for IPv6 in the U.S. Government – Version 1.0":

The use of the old Site-Local address type (RFC3879) is deprecated. The Unique Local IPv6 Unicast Addresses (ULA) (RFC 4193) mechanism has been designed to fulfill a similar requirement. While Private Addresses are widely used in IPv4 networks, generalized ULA use and support in IPv6 are not as mature nor is their architectural desirability as well understood.

For these reasons, the UC products are not required to support ULA at this time.

NOTE 3: An end site is defined as an end-user (subscriber) edge network domain that requires multiple subnets/64. Therefore, vendors will not be required to support anything greater than /64, such as /116 or /126 subnet.

IP6-000160 [**Required: EI, NA/SS, R, LS, SD**] The product shall support the IPv6 Scoped Address Architecture as described in RFC 4007.

IP6-000170 [**Conditional: EI, NA/SS, R, LS, SD**] If a scoped address (RFC 4007) is used, then the product shall use a scope index value of zero when the default zone is intended.

5.2.1.4 Dynamic Host Configuration Protocol

IP6-000180 [**Required: EI**] [**Conditional: NA/SS, R**] If Dynamic Host Configuration Protocol (DHCP) is supported within an IPv6 environment, then it shall be implemented in accordance with the DHCP for IPv6 (DHCPv6) as described in RFC 3315.

IP6-000190 [**Conditional: LS**] If the LS supports DHCP and a routing function, then the product shall support RFC 3315.

IP6-000200 [**Conditional: EI, NA/SS**] If the product is a DHCPv6 client, then the product shall discard any messages that contain options that are not allowed to appear in the received message type (e.g., an Identity Association option in an Information-Request message).

IP6-000210 [**Required: EI**] The product shall support DHCPv6 as described in RFC 3315.

NOTE: The following subtended requirements are predicated upon an implementation of DHCPv6 for the EI. It is not expected that other UC appliances will use DHCPv6.

IP6-000220 [**Required: EI**] [**Conditional: NA/SS**] If the product is a DHCPv6 client and the first retransmission timeout has elapsed since the client sent the Solicit message and the client has received an Advertise message(s), but the Advertise message(s) does not have a preference value of 255, then the client shall continue with a client-initiated message exchange by sending a Request message.

IP6-000230 [**Required: EI**] [**Conditional: NA/SS**] If the product is a DHCPv6 client and the DHCPv6 solicitation message exchange fails, then it shall restart the reconfiguration process after receiving user input, system restart, attachment to a new link, a system configurable timer, or a user defined external event occurs.

NOTE: The intent is to ensure that the DHCP client continues to restart the configuration process periodically until it succeeds.

IP6-000240 [**Required: EI**] [**Conditional: NA/SS**] If the product is a DHCPv6 client and it sends an Information-Request message, then it shall include a Client Identifier option to allow it to be authenticated to the DHCPv6 server.

IP6-000250 [**Required: EI**] [**Conditional: NA/SS**] If the product is a DHCPv6 client, then it shall perform duplicate address detection upon receipt of an address from the DHCPv6 server before transmitting packets using that address for itself.

IP6-000260 [**Required: EI**] [**Conditional: NA/SS**] [Alarm] If the product is a DHCPv6 client, then it shall log all reconfigure events.

NOTE: Some systems may not be able to log all this information (e.g., the system may not have access to this information).

IP6-000270 [**Conditional: EI, NA/SS, R, LS**] [Alarm] If the product supports DHCPv6 and uses authentication, then it shall discard unauthenticated DHCPv6 messages from UC products and log the event.

NOTE: Some systems may not be able to log all this information (e.g., the system may not have access to this information).

5.2.1.5 Neighbor Discovery

IP6-000280 [**Required: EI, NA/SS, R, SD**] The product shall support Neighbor Discovery for IPv6 as described in RFC 4861.

IP6-000290 [**Conditional: LS**] If the LS also supports a routing function, then the product shall support RFC 4861.

IP6-000300 [**Required: NA/SS, R, LS, SD**] The product shall not set the override flag bit in the Neighbor Advertisement message for solicited advertisements for any cast addresses or solicited proxy advertisements.

IP6-000310 [**Required: EI, NA/SS, R, LS, SD**] When a valid "Neighbor Advertisement" message is received by the product and the product neighbor cache does not contain the target's entry, the advertisement shall be silently discarded.

IP6-000320 [**Required: EI, NA/SS, R, LS, SD**] When a valid "Neighbor Advertisement" message is received by the product and the product neighbor cache entry is in the INCOMPLETE state when the advertisement is received and the link layer has addresses and no target link-layer option is included, the product shall silently discard the received advertisement.

IP6-000330 [**Required: EI, NA/SS, R, LS, SD**] When address resolution fails on a neighboring address, the entry shall be deleted from the product's neighbor cache.

5.2.1.5.1 Redirect Messages

IP6-000340 [**Required: EI, NA/SS, SD**] The product shall support the ability to configure the product to ignore Redirect messages.

IP6-000350 [**Required: EI, NA/SS, SD**] The product shall only accept Redirect messages from the same router as is currently being used for that destination.

NOTE: The intent of this requirement is that if a node is sending its packets destined for location A to router X, that it can only accept a Redirect message from router X for packets destined for location A to be sent to router Z.

IP6-000360 [**Conditional: EI, NA/SS**] If "Redirect" messages are allowed, then the product shall update its destination cache in accordance with the validated Redirect message.

IP6-000370 [**Conditional: EI, NA/SS**] If the valid "Redirect" message is allowed and no entry exists in the destination cache, then the product shall create an entry.

IP6-000380 [**Conditional: EI, NA/SS**] If redirects are supported, then the device shall support the ability to disable this functionality.

NOTE: The default setting is "disabled" so that the redirect functions must explicitly be "enabled."

5.2.1.5.2 Router Advertisements

IP6-000390 [**Required: R**] [**Conditional: LS**] [Alarm] If the product supports routing functions, then the product shall inspect valid router advertisements sent by other routers and verify that the routers are advertising consistent information on a link and shall log any inconsistent router advertisements.

NOTE: Some products may not be able to log all this information (e.g., the product may not have access to this information).

IP6-000400 [**Required: EI, NA/SS, SD**] The product shall prefer routers that are reachable over routers whose reachability is suspect or unknown.

IP6-000410 [**Required: R**] [**Conditional: LS**] If the product supports routing functions, then the product shall be capable of supporting the MTU value in the router advertisement message for all links in accordance with RFC 4861.

5.2.1.6 Stateless Address Autoconfiguration and Manual Address Assignment

IP6-000420 [**Conditional: EI, NA/SS, R, LS, SD**] If the product supports stateless IP address autoconfiguration including those provided for the commercial market, then the product shall

support IPv6 Stateless Address Autoconfiguration (SLAAC) for interfaces supporting UC functions in accordance with RFC 4862.

NOTE 1: RFC 4862 has replaced the now-obsolete RFC 2462. The scope of RFC 2462, Section 5.5, is Creation of Global and Site-Local Addresses. The scope of RFC 4862, Section 5.5, is Creation of Global Addresses.

NOTE 2: "DoD IPv6 Standard Profiles for IPv6-capable Products-Supplemental Guidance" defines Host as a PC or other end-user computer or workstation running a general-purpose operating system.

NOTE 3: The UC EI platform (on which the softphone is located) may be certified to the DoD IPv6 Profile and required to support autonomous configuration, either SLAAC or DHCPv6 client.

IP6-000430 [**Conditional: EI, NA/ SS, R, LS, SD**] If the product supports IPv6 SLAAC, then the product shall have a configurable parameter that allows the function to be enabled and disabled. Specifically, the product shall have a configurable parameter that allows the "managed address configuration" flag and the "other stateful configuration" flag to always be set and not perform stateless autoconfiguration.

IP6-000440 [**Conditional: EI (except softphones), NA/ SS, R, LS, SD**] If the product supports IPv6 SLAAC, then the product shall have the configurable parameter set not to perform stateless autoconfiguration.

NOTE: The objective of this requirement is to prevent a product from using stateless auto configuration. Stateless address autoconfiguration is focused solely on softphones since they reside on PCs.

IP6-000450 [**Required: EI, NA/SS, R, LS, SD**] While nodes are not required to autoconfigure their addresses using SLAAC, all IPv6 Nodes shall support link-local address configuration and Duplicate Address Detection (DAD) as specified in RFC 4862. In accordance with RFC 4862, DAD shall be implemented and shall be on by default. Exceptions to the use of DAD are noted in the following text.

IP6-000460 [**Required: EI, NA/SS, R, LS, SD**] A node MUST allow for autoconfiguration-related variable to be configured by system management for each multicast-capable interface to include DupAddrDetectTransmits where a value of zero indicates that DAD is not performed on tentative addresses as specified in RFC 4862.

NOTE: Network Infrastructure Security Technical Implementation Guide (STIG) states the following:

The use of Duplicate Address Detection opens up the possibility of denial of service attacks. Any node can respond to Neighbor Solicitations for a tentative address,

causing the other node to reject the address as a duplicate. This attack is similar to other attacks involving the spoofing of Neighbor Discovery messages.

Further, RFC 4862 states the following:

> By default, all addresses should be tested for uniqueness prior to their assignment to an interface for safety. The test should individually be performed on all addresses obtained manually, via stateless address autoconfiguration, or via DHCPv6. To accommodate sites that believe the overhead of performing Duplicate Address Detection outweighs its benefits, the use of Duplicate Address Detection can be disabled through the administrative setting of a per-interface configuration flag.

The products may include an administrative setting to disable DAD.

IP6-000470 [**Required: EI, NA/SS, R, LS, SD**] The product shall support manual assignment of IPv6 addresses.

IP6-000480 [**Required: EI (Softphones only)**] The product shall support stateful autoconfiguration (i.e., ManagedFlag=TRUE) as described in RFC 4862.

NOTE: This requirement is associated with the earlier Requirement 10.2 for the EI to support DHCPv6.

IP6-000490 [**Required: R**] [**Conditional: LS**] If the product provides routing functions, then the product shall default to using the "managed address configuration" flag and the "other stateful flag" set to TRUE in their router advertisements when stateful autoconfiguration is implemented.

IP6-000500 [**Conditional: EI**] If the product supports a subtended appliance behind it, then the product shall ensure that the IP address assignment process of the subtended appliance is transparent to the UC components of the product and does not cause the product to attempt to change its IP address.

NOTE: An example is a PC that is connected to the LAN through the hub or switch interface on a phone. The address assignment process of the PC should be transparent to the EI and should not cause the phone to attempt to change its IP address.

IP6-000510 [**Conditional: EI (Softphones only)**] If the product supports SLAAC and security constraints prohibit the use of hardware identifiers as part of interface addresses generated using SLAAC, then Internet Protocol Security (IPSec)-capable products shall support privacy extensions for stateless address autoconfiguration as defined in RFC 4941.

Table 5.2-2, UCR Policy for Manual, Stateful, and Stateless IPv6 Address Configuration, summarizes the policy for configuring Manual, DHCP, and SLAAC for IPv6 address for the various UC Products.

Table 5.2-2. UCR Policy for Manual, Stateful, and Stateless IPv6 Address Configuration

UC PRODUCT	MANUAL IPV6 CONFIGURATION	IPV6 STATEFUL CONFIGURATION VIA DHCPV6	IPV6 SLAAC
Softphones	Yes, Requirement 12.3	Yes, Requirement 10	Yes, Requirement 12.4
EI (except softphones)	Yes, Requirement 12.3	Yes, Requirement 10	No, Requirement 12.1.1
NA/SS	Yes, Requirement 12.3	No for SC, SS, MG, Requirement 10, Note 1. Yes for all others if RFC 3315 is supported, Requirement 10	No, Requirement 12.1.1
R	Yes, Requirement 12.3	Conditionally Yes if RFC 3315 is supported, Requirement 10	No, Requirement 12.1.1
LS	Yes, Requirement 12.3	Conditionally Yes if RFC 3315 and routing functions are supported, Requirement 10	No, Requirement 12.1.1
SD	Yes, Requirement 12.3	No, Requirement 10	No, Requirement 12.1.1
Where "No" could be (1) not installed, (2) removed from Operating System, or (3) disabled by parameter.			

5.2.1.7 Internet Control Message Protocol

IP6-000520 [**Required: EI, NA/SS, R, LS, SD**] The product shall support the Internet Control Message Protocol (ICMP) for IPv6 as described in RFC 4443.

IP6-000530 [**Required: R, LS**] The product shall have a configurable rate-limiting parameter for rate limiting the ICMP error messages it originates.

IP6-000540 [**Required: NA/SS, R, LS, SD**] The product shall support the capability to enable or disable the ability of the product to generate a Destination Unreachable message in response to a packet that cannot be delivered to its destination for reasons other than congestion.

NOTE: In lieu of the RFC 4443 paragraph 3.1 requirement to prohibit routers from forwarding a code 3 (address unreachable) message on point-to-point link back onto the arrival link, vendors may alternatively use a prefix length of 127 on Inter-Router Links to address ping-pong issues on non-Ethernet interfaces (the ping-pong issue is not present on Ethernet interfaces).

IP6-000550 [**Required: EI, NA/SS, R, LS, SD**] The product shall support the enabling or disabling of the ability to send an Echo Reply message in response to an Echo Request message sent to an IPv6 multicast or anycast address.

NOTE: The number of responses may be traffic conditioned to limit the effect of a denial of service attack.

IP6-000560 [**Required: EI, NA/SS, R, LS, SD**] The product shall validate ICMPv6 messages, using the information contained in the payload, before acting on them.

NOTE: The actual validation checks are specific to the upper layers and are out of the scope of this UCR. Protecting the upper layer with IPSec mitigates these attacks.

5.2.1.8 Routing Functions

IP6-000570 [**Required: R**] [**Conditional: LS**] If the product supports routing functions, then the product shall support the Open Shortest Path First (OSPF) for IPv6 as described in RFC 5340.

IP6-000580 [**Required: R**] [**Conditional: LS**] If the product supports routing functions, then the product shall support securing OSPF with IPSec as described for other IPSec instances in Section 4, Information Assurance.

IP6-000590 [**Required: R**] [**Conditional: LS**] If the product supports routing functions, then the product shall support router-to-router integrity using the IP Authentication Header with HMAC-SHA1-96 within Encapsulating Security Payload (ESP) and Authentication Header (AH) as described in RFC 2404.

NOTE: NIST Special Publication 500-267, "A Profile for IPv6 in the U.S. Government," forwards the following guidance:

Although HMAC-SHA-1 (RFC 2404) is still considered secure, the Internet Engineering Task Force (IETF) is encouraging the standardization of HMAC-SHA-256 to ensure an orderly transition to a more secure Message Authentication Code (MAC).

IP6-000600 [**Required: R**] [**Conditional: LS**] If the product supports interior routing functions of OSPFv3, then the product shall support RFC 4552.

NOTE: RFC 4552 relies on manual key exchange (pre-configuration) and may not be appropriate in a dynamic Tactical environment. Router acquisitions for Tactical deployment are exempt from this requirement.

IP6-000610 [**Conditional: R, LS**] If the product supports the Intermediate System to Intermediate System (IS-IS) routing protocol used in DoD backbone networks, then the product shall support the IS-IS for IPv6 as described in RFC 5308.

NOTE: IS-IS is the primary routing protocol in the Defense Information Systems Network (DISN) backbone for handling the infrastructure (non-customer) routes. The Provider (P), Classified CE-R (C-PE), Unclassified CE-R (U-PE), and Aggregation Router (AR) devices all have instances of the routing protocol. The IS-IS is also used on the RED side across the Generic Routing Encapsulation (GRE) tunnels.

IP6-000620 [**Conditional: R, LS**] If the product supports IS-IS routing architecture (for IPv6-only or dual-stack operation), then the product shall support RFC 5304 and RFC 5310 and shall support RFC 6119 for IPv6 traffic engineering.

IP6-000630 [**Conditional: R, LS**] If the product acts as a CE Router (CE-R), then the product shall support the use of Border Gateway Protocol (BGP) as described in RFC 1772 and RFC 4271.

a. If the product acts as a CE-R, then the product shall support the use of BGP4 multiprotocol extensions for IPv6 inter-domain routing as described in RFC 2545.

NOTE: The requirement to support BGP4 is in Section 6, Network Infrastructure End-to-End Performance.

IP6-000640 [**Conditional: R, LS**] If the product acts as a CE-R, then the product shall support multiprotocol extensions for BGP4 in RFC 4760.

NOTE: The requirement to support BGP4 is in Section 6, Network Infrastructure End-to-End Performance.

IP6-000650 [**Conditional: R**] If the product acts as a CE-R, then the product shall support the GRE as described in RFC 2784.

IP6-000660 [**Conditional: R**] If the product acts as a CE-R, then the product shall support the Generic Packet Tunneling in IPv6 Specification as described in RFC 2473.

NOTE 1: Tunneling is provided for data applications and is not needed as part of the VVoIP architecture.

NOTE 2: Section 13, Security Devices, requires that Firewall (FW) and Intrusion Protection System (IPS) shall conform to all of the MUST requirements found in RFC 2473.

IP6-000670 [**Required: EI (Softphone Only), R**] [**Conditional: LS**] If the product supports routing functions, then the product shall support the Multicast Listener Discovery (MLD) process as described in RFC 2710 and extended in RFC 3810.

NOTE: The current VVoIP design does not use multicast, but routers supporting VVoIP also support data applications that may use multicast. A softphone will have non-routing functions that require MLDv2.

a. If the product supports MLD process as described in RFC 2710 and extended in RFC 3810, then the product shall support RFC 2711.

IP6-000680 [**Required: EI, NA/SS, SD**] The product shall support MLD as described in RFC 2710.

NOTE: This requirement was added to ensure that Neighbor Discovery multicast requirements are met. Routers are not included in this requirement since they have to meet RFC 2710 in the preceding requirement.

5.2.1.9 IP Security

IP6-000690 [**Required: EI (Softphone Only), R**] [**Conditional: EI, NA/SS, LS, SD**] If the product uses IPSec, then the product shall be compatible with the Security Architecture for the IPSec described in RFC 4301.

NOTE 1: RFC 4301 mandates support for several features for which support is available in Internet Key Exchange (IKE) version 2 (IKEv2) but not in IKEv1, e.g., negotiation of a Security Association (SA) representing ranges of local and remote ports or negotiation of multiple SAs with the same selectors.

However, at this time the UCR does not require the use of IKEv2. Therefore, implementation at this time of RFC 4301 will include only those features which are compatible with the use of IKEv1.

NOTE 2: The interfaces required to use IPSec are defined in Section 4, Information Assurance.

b. If RFC 4301 is supported, then the product shall support binding of a SA with a particular context.

c. If RFC 4301 is supported, then the product shall be capable of disabling the BYPASS IPSec processing choice.

NOTE: The intent of this requirement is to ensure that no packets are transmitted unless they are protected by IPSec.

IP6-000700 [**Required: EI (Softphone Only), R**] [**Conditional: EI, NA/SS, LS, SD**] If RFC 4301 is supported, then the product shall not support the mixing of IPv4 and IPv6 in a SA.

IP6-000710 [**Required: EI (Softphone Only), R**] [**Conditional: EI, NA/SS, LS, SD**] If RFC 4301 is supported, then the product's security association database (SAD) cache shall have a method to uniquely identify a SAD entry.

NOTE: The concern is that a single SAD entry will be associated with multiple security associations. RFC 4301, Section 4.4.2, Security Association Database (SAD), describes a scenario where this could occur.

IP6-000720 [**Required: EI (Softphone Only), R**] [**Conditional: EI, NA/SS, LS, SD**] If RFC 4301 is supported, then the product shall implement IPSec to operate with both integrity and confidentiality.

IP6-000730 [**Required: EI (Softphone Only), R**] [**Conditional: EI, NA/SS, LS, SD**] If RFC 4301 is supported, then the product shall be capable of enabling and disabling the ability of the product to send an ICMP message informing the sender that an outbound packet was discarded.

IP6-000740 [**Required: EI (Softphone Only), R**] [**Conditional: EI, NA/SS, LS, SD**] If an ICMP outbound packet message is allowed, then the product shall be capable of rate limiting the transmission of ICMP responses.

IP6-000750 [**Required: EI (Softphone Only), R**] [**Conditional: EI, NA/SS, LS, SD**] If RFC 4301 is supported, then the system's Security Policy Database (SPD) shall have a nominal, final entry that discards anything unmatched.

IP6-000760 [**Required: EI (Softphone Only), R**] [**Conditional: EI, NA/SS, LS, SD**] [Alarm] If RFC 4301 is supported, and the product receives a packet that does not match any SPD cache entries, and the product determines it should be discarded, then the product shall log the event and include the date/time, Security Parameter Index (SPI) if available, IPSec protocol if available, source and destination of the packet, and any other selector values of the packet.

NOTE: Some products may not be able to log all this information (e.g., the product may not have access to this information).

IP6-000770 [**Required: EI (Softphone Only), R**] [**Conditional: EI, NA/SS, LS, SD**] [Alarm] If RFC 4301 is supported, then the product should include a management control to allow an administrator to enable or disable the ability of the product to send an IKE notification of an INVALID_SELECTORS.

NOTE: Some products may not be able to log all this information (e.g., the product may not have access to this information).

IP6-000780 [**Required: EI (Softphone Only), R**] [**Conditional: EI, NA/SS, LS, SD**] If RFC 4301 is supported, then the product shall support the ESP Protocol in accordance with RFC 4303.

IP6-000790 [**Required: EI (Softphone Only), R**] [**Conditional: EI, NA/SS, LS, SD**] If RFC 4303 is supported, then the product shall be capable of enabling anti-replay.

IP6-000800 [**Required: EI (Softphone Only), R**] [**Conditional: EI, NA/SS, LS, SD**] If RFC 4303 is supported, then the product shall check, as its first check, after a packet has been matched to its SA whether the packet contains a sequence number that does not duplicate the sequence number of any other packet received during the life of the security association.

IP6-000810 [**Required: EI (Softphone Only), R**] [**Conditional: EI, NA/SS, LS, SD**] If RFC 4301 is supported, then the product shall support IKEv1 as defined in RFC 2409.

NOTE: The IKEv1 requirements are found in Section 4, Information Assurance.

IP6-000820 [**Conditional: EI, NA/SS, R, LS, SD**] To prevent a Denial of Services (DoS) attack on the initiator of an IKE_SA, the initiator shall accept multiple responses to its first message, treat each as potentially legitimate, respond to it, and then discard all the invalid half-open connections when it receives a valid cryptographically protected response to any one of its requests. Once a cryptographically valid response is received, all subsequent responses shall be ignored whether or not they are cryptographically valid.

IP6-000830 [**Required: EI (Softphone Only), R**] [**Conditional: EI, NA/SS, LS, SD**] If RFC 4301 is supported, then the product shall support extensions to the Internet IP Security Domain of Interpretation for the Internet Security Association and Key Management Protocol (ISAKMP) as defined in RFC 2407.

IP6-000840 [**Required: EI (Softphone Only), R**] [**Conditional: EI, NA/SS, LS, SD**] If RFC 4301 is supported, then the product shall support the ISAKMP as defined in RFC 2408.

IP6-000850 [**Required: EI (Softphone Only), R**] [**Conditional: EI, NA/SS, LS, SD**] If the product supports the IPSec Authentication Header Mode, then the product shall support the IP Authentication Header (AH) as defined in RFC 4302.

IP6-000860 [**Required: EI (Softphone Only), R**] [**Conditional: EI, NA/SS, LS, SD**] If RFC 4301 is supported, then the product shall support manual keying of IPSec.

IP6-000870 [**Required: EI (Softphone Only), R**] [**Conditional: EI, NA/SS, LS, SD**] If RFC 4301 is supported, then the product shall support the ESP and AH cryptographic algorithm implementation requirements as defined RFC 4835

IP6-000880 [**Required: EI (Softphone Only), R**] [**Conditional: EI, NA/SS, LS, SD**] If RFC 4301 is supported, then the product shall support the IKEv1 security algorithms as defined in RFC 4109.

5.2.1.10 Network Management

IP6-000890 [**Conditional: R, LS**] If IPv6-compatible nodes are managed via Simple Network Management Protocol (SNMP) using IPv6, then the product shall comply with the Management Information Base (MIB) for IPv6 textual conventions and general group as defined in RFC 4293.

NOTE: The requirements to support SNMPv3 are found in Section 4, Information Assurance.

IP6-000900 [**Conditional: R, LS**] If the product performs routing functions and if IPv6-capable nodes are managed via SNMP management using IPv6, then the product shall support the SNMPv3 management framework as described in RFC 3411.

IP6-000910 [**Conditional: R, LS**] If the product performs routing functions and if IPv6-capable nodes are managed via SNMP management using IPv6, then the product shall support SNMPv3 message processing and dispatching as described in RFC 3412.

IP6-000920 [**Conditional: R, LS**] If the product performs routing functions and if IPv6-capable nodes are managed via SNMP management using IPv6, then the product shall support the SNMPv3 applications as described in RFC 3413.

IP6-000930 [**Conditional: R, LS**] If IPv6-compatible nodes are managed via SNMP using IPv6, then the product shall support the IP MIBs as defined in RFC 4293.

IP6-000940 [Conditional: R, LS] If IPv6-compatible nodes are managed via SNMP using IPv6, then the product shall support the Transmission Control Protocol (TCP) MIBs as defined in RFC 4022.

IP6-000950 [Conditional: R, LS] If IPv6-compatible nodes are managed via SNMP using IPv6, then the product shall support the User Datagram Protocol (UDP) MIBs as defined in RFC 4113.

IP6-000960 [Conditional: R, LS] If IPv6-compatible nodes are managed via SNMP using IPv6, and the product performs routing functions and tunneling functions, then the product shall support IP tunnel MIBs as described in RFC 4087.

IP6-000970 [Conditional: R, LS] If the product performs routing functions and is managed by SNMP using IPv6, then the product shall support the IP Forwarding MIB as defined in RFC 4292.

IP6-000980 [Conditional: R, LS] If the product supports routing functions, and the IPSec policy database is configured through SNMPv3 using IPv6, then the product shall support RFC 4807.

IP6-000990 [Required: EI (Softphone only)] [Conditional: EI, NA/SS, R, LS, SD] If the product uses Uniform Resource Identifiers (URIs) in combination with IPv6, then the product shall use the URI syntax described in RFC 3986.

IP6-001000 [**Conditional: EI, NA/SS**] If the product uses the Domain Name Service (DNS) resolver for IPv6 based queries, then the product shall conform to RFC 3596 for DNS queries.

5.2.1.11 Traffic Engineering

IP6-001010 [**Required: NA/SS, R, LS, SD**] For traffic engineering purposes, the bandwidth required per voice subscriber is calculated to be 110.0 kbps (each direction) for each IPv6 call. This is based on G.711 (20 ms codec) with IP overhead (100 kbps) resulting in a 250-byte bearer packet plus 10 kbps for signaling, Ethernet Interframe Gap, and the Secure Real-Time Transport Control Protocol (SRTCP) overhead. Based on overhead bits included in the bandwidth calculations, vendor implementations may use different calculations and hence arrive at slightly different numbers.

IP6-001020 [**Required: R, LS**] Despite the differences in IPv6 and IPv4 packet sizes, for planning purposes, the number of VoIP subscribers per link size for IPv6 should be assumed to be approximately the same as for IPv4 and is defined in Table 7.6-2, LAN VoIP Subscribers for IPv4 and IPv6, in Section 7, Network Edge Infrastructure.

IP6-001030 [**Required: R, LS**] Despite the differences in IPv6 and IPv4 packet sizes, for planning purposes, the number of video subscribers per link size for IPv6 should be assumed to be approximately the same as for IPv4 and is defined in Section 7, Network Edge Infrastructure.

5.2.1.12 IP Version Negotiation

IP6-001040 [**Required: NA/SS, SD**] The product shall forward packets using the same IP version as the version in the received packet.

NOTE: If the packet was received as an IPv6 packet, then the appliance will forward it as an IPv6 packet. If the packet was received as an IPv4 packet, then the appliance will forward the packet as an IPv4 packet. This requirement is primarily associated with the signaling packets to ensure that translation does not occur.

IP6-001050 [**Required: EI, NA/SS**] When the product is establishing media streams from dual-stacked appliances for AS-SIP signaled sessions, the product shall use the Alternative Network Address Type (ANAT) semantics for the Session Description Protocol (SDP) in accordance with RFC 4091. Also, the following conditional requirements would apply.

NOTE 1: Guidance on clarification on the use of ANAT for related media is located in the AS-SIP 2013, Section 5.2.5, Clarification on the Use of ANAT for Related Media Streams.

NOTE 2: Guidance on SIP syntax and encoding rules for IPv6 Augmented Backus-Naur Form (ABNF) per RFC 5954 is located in AS-SIP 2013, Section 4.1.3, Basic Requirements for AS-SIP Signaling Appliances and AS-SIP EI.

IP6-001050.a [**Required: EI, NA/SS**] The product shall prefer any IPv4 address to any IPv6 address when using ANAT semantics.

NOTE: This requirement will result in all AS-SIP sessions being established using IPv4.

IP6-001050.b [**Required: EI, NA/SS**] The product shall place the option tag "SDP-ANAT" in a Required header field when using ANAT semantics in accordance with RFC 4092.

IP6-001050.c [**Required: EI**] The products shall include the IPv4 and IPv6 addresses within the SDP of the SIP INVITE message when the INVITE contains the SDP.

5.2.1.13 Services Session Initiation Protocol IPv6 Unique Requirements

IP6-001060 [**Conditional: EI, NA/SS, SD**] If the product is using AS-SIP, and the <addrtype> is IPv6, and the <connection-address> is a unicast address, then the product shall support generation and processing of unicast IPv6 addresses having the following formats:

- x:x:x:x:x:x:x:x (where x is the hexadecimal values of the eight 16-bit pieces of the address). Example: 1080:0:0:0:8:800:200C:417A.
- x:x:x:x:x:x:d.d.d.d (where x is the hexadecimal values of the six high-order 16-bit pieces of the address, and d is the decimal values of the four low-order 8-bit pieces of the address (standard IPv4 representation). For example, 1080:0:0:0:8:800:116.23.135.22.

IP6-001070 [**Conditional: EI, NA/SS, SD**] If the product is using AS-SIP, then the product shall support the generation and processing of IPv6 unicast addresses using compressed zeros consistent with one of the following formats:

- x:x:x:x:x:x:x:x format: 1080:0:0:0:8:800:200C:417A.
- x:x:x:x:x:x:d.d.d.d format: 1080:0:0:0:8:800:116.23.135.22.
- compressed zeros: 1080::8:800:200C:417A.

IP6-001080 [**Conditional: EI, NA/SS, SD**] If the product is using AS-SIP, and the <addrtype> is IPv6, and the <connection-address> is a multicast group address (i.e., the two most significant hexadecimal digits are FF), then the product shall support the generation and processing of multicast IPv6 addresses having the same formats as the unicast IPv6 addresses.

IP6-001090 [**Conditional: EI, NA/SS, SD**] If the product is using AS-SIP, and the <addrtype> is IPv6, then the product shall support the use of RFC 4566 for IPv6 in SDP as described in AS-SIP 2013, Section 4, SIP Requirements for AS-SIP Signaling Appliances and AS-SIP EIs.

IP6-001100 [**Conditional: EI, NA/SS, SD**] If the product is using AS-SIP, and the <addrtype> is IPv6, and the <connection-address> is an IPv6 multicast group address, then the multicast connection address shall not have a Time To Live (TTL) value appended to the address as IPv6 multicast does not use TTL scoping.

IP6-001110 [**Conditional: EI, NA/SS, SD**] If the product is using AS-SIP, then the product shall support the processing of IPv6 multicast group addresses having the <number of address> field and may support generating the <number of address> field. This field has the identical format and operation as the IPv4 multicast group addresses.

IP6-001120 [**Required: SD**] The product shall be able to provide topology hiding [e.g., Network Address Translation (NAT)] for IPv6 packets as described in Section 4, Information Assurance.

NOTE: Deployments requiring the network topology hiding that IPv4 NAT provided as a side-effect should consider RFC 4864 – Local Network Protection (LNP) for IPv6.

IP6-001130 [**Required: EI (Softphone Only)**] The product shall support default address selection for IPv6 as defined in RFC 3484 (except for Section 2.1).

NOTE: It is assumed that an IPv6 appliance will have as a minimum an IPv6 link local and an IPv4 address, and will have at least two addresses.

5.2.1.14 Miscellaneous

IP6-001140 [**Conditional: R, SD**] If the product supports Remote Authentication Dial-in User Service (RADIUS) authentication, then the product shall support RADIUS as defined in RFC 3162. [**Conditional: LS**] If the LS supports a routing function and supports RADIUS authentication, then the product shall support RADIUS as defined in RFC 3162.

NOTE 1: RFC 3162 defines only the additional attributes of RADIUS that are unique to IPv6 implementations. For the base RADIUS requirements, other RFCs are required, such as RFC 2865.

NOTE 2: Because RFC 3162 cites the Network Access Server (NAS) functions would be on the Access Point (router), this function should be a feature of the router.

IP6-001150 [**Required: EI, NA/SS, R, LS, SD**] The products shall support Differentiated Services as described in RFC 2474 for a voice and video stream in accordance with Section 2, Session Control Products, and Section 6, Network Infrastructure End-to-End Performance, plain text DSCP plan.

IP6-001160 [**Conditional: NA/SS**] If the product acts as an IPv6 tunnel broker, then the product shall support the function as defined in RFC 3053.

IP6-001170 [**Conditional: R**] If the product supports roaming (as defined within RFC 4282), then the product shall support this function as described by RFC 4282.

IP6-001180 [**Conditional: R**] If the product supports the Point-to-Point Protocol (PPP), then the product shall support PPP as described in RFC 5072.

IP6-001190 [**Required: LS**] [**Conditional: R**] To support ASLAN assured services, all LAN switches that provide layer 3 functionality to the access layer shall support Virtual Router Redundancy protocol (VRRP) for IPv6 as detailed in RFC 5798.

NOTE: This applies to products only in the ASLAN.

IP6-001200 [**Conditional: R, LS**] If the product supports ECN, then the product shall support RFC 3168 for the incorporation of ECN to TCP and IP, including ECN's use of two bits in the IP header.

NOTE: This applies to the Core, Distribution, and Access products as identified in Section 7.2.1.5, Protocols. The use of RFC 3168 is Conditional for these products.

5.2.2 Mapping of RFCs to UC Profile Categories

Tables 5.2-3 through 5.2-7 map RFCs and requirements applicability to the various UC profile categories.

Table 5.2-3. UC End Instruments (EIs)

RFC NUMBER	RFC TITLE	REQUIRED – R * CONDITIONAL – C
1981	Path MTU Discovery for IP Version 6	R-8
2407	The Internet IP Security Domain of Interpretation for ISAKMP	R-8; C
2408	Internet Security Association and Key Management Protocol (ISAKMP)	R-8; C
2409	The Internet Key Exchange (IKE)	R-8; C
2460	Internet Protocol, Version 6 (IPv6) Specification	R-2
2464	Transmission of IPv6 Packets over Ethernet Networks	R-3
2474	Definition of the Differentiated Services Field (DS Field) in the IPv4 and IPv6 Headers	R-4
2710	Multicast Listener Discovery (MLD) for IPv6	R-8
2711	IPv6 Router Alert Option	R-8
3315	Dynamic Host Configuration Protocol for IPv6 (DHCPv6)	R
3484	Default Address Selection for Internet Protocol Version 6 (IPv6)	R-8
3596	DNS Extensions to Support IPv6	C
3810	Multicast Listener Discovery Version 2 (MLDv2) for IPv6	R-8
3986	Uniform Resource Identifier (URI): Generic Syntax	R-8; C
4007	IPv6 Scoped Address Architecture	R
4091	The Alternative Network Address Types (ANAT) Semantics for the Session Description Protocol (SDP) Grouping Framework	R
4092	Usage of the Session Description Protocol (SDP) Alternative Network Address Types (ANAT) Semantics in the Session Initiation Protocol (SIP)	R
4109	Algorithms for Internet Key Exchange Version 1 (IKEv1)	R-8; C
4213	Basic Transition Mechanisms for IPv6 Hosts and Routers	R-1
4291	IP Version 6 Addressing Architecture	R
4301	Security Architecture for the Internet Protocol	R-8; C
4302	IP Authentication Header	R-8; C
4303	IP Encapsulating Security Payload (ESP)	R-8; C
4443	Internet Control Message Protocol (ICMPv6) for the Internet Protocol Version 6 (IPv6) Specification	R
4566	SDP: Session Description Protocol	C
4835	Cryptographic Algorithm Implementation Requirements for Encapsulating Security Payload (ESP) and Authentication Header (AH)	R-8, C

RFC NUMBER	RFC TITLE	REQUIRED – R * CONDITIONAL – C
4861	Neighbor Discovery for IP Version 6 (IPv6)	R
4862	IPv6 Stateless Address Autoconfiguration	R-8; C
4941	Privacy Extensions for Stateless Address Autoconfiguration in IPv6	C-8
5095	Deprecation of Type 0 Routing Headers in IPv6	R

Notes:
C/R-1: Meets only the dual-stack requirements of this RFC.
C/R-2: Meets only the IPv6 formatting requirements of this RFC.
R-3: Meets only the framing format aspects of RFC.
R-4: Requirement covered in Section 6, Network Infrastructure End-to-End Performance.
C-5: Condition is that product acts as a router.
C-6: Applies only to MGs.
C-7: Requirements apply only if the product acts as a CE-R.
C/R-8: EI (softphones only).
* This column can have (1) softphones only, e.g., R-8, (2) EI, e.g., R-3; or (3) Softphones only and EI, e.g., R-8; C.

Table 5.2-4. UC Network Appliances and Simple Servers (NA/SS)

RFC NUMBER	RFC TITLE	REQUIRED – R CONDITIONAL – C
2407	The Internet IP Security Domain of Interpretation for ISAKMP	C
2408	Internet Security Association and Key Management Protocol (ISAKMP)	C
2409	The Internet Key Exchange (IKE)	C
2460	Internet Protocol, Version 6 (IPv6) Specification	R-2
2464	Transmission of IPv6 Packets over Ethernet Networks	R-3
2474	Definition of the Differentiated Services Field (DS Field) in the IPv4 and IPv6 Headers	R-4
2710	Multicast Listener Discovery (MLD) for IPv6	R-8
3053	IPv6 Tunnel Broker	C
3315	Dynamic Host Configuration Protocol for IPv6 (DHCPv6)	C
3596	DNS Extensions to Support IPv6	C
3986	Uniform Resource Identifier (URI): Generic Syntax	C
4007	IPv6 Scoped Address Architecture	R
4091	The Alternative Network Address Types (ANAT) Semantics for the Session Description Protocol (SDP) Grouping Framework	R
4092	Usage of the Session Description Protocol (SDP) Alternative Network Address Types (ANAT) Semantics in the Session Initiation Protocol (SIP)	R
4109	Algorithms for Internet Key Exchange Version 1 (IKEv1)	C
4213	Basic Transition Mechanisms for IPv6 Hosts and Routers	R-1
4291	IP Version 6 Addressing Architecture	R
4301	Security Architecture for the Internet Protocol	C

RFC NUMBER	RFC TITLE	REQUIRED – R CONDITIONAL – C
4302	IP Authentication Header	C
4303	IP Encapsulating Security Payload (ESP)	C
4443	Internet Control Message Protocol (ICMPv6) for the Internet Protocol Version 6 (IPv6) Specification	R
4566	SDP: Session Description Protocol	C
4835	Cryptographic Algorithm Implementation Requirements for Encapsulating Security Payload (ESP) and Authentication Header (AH)	C
4861	Neighbor Discovery for IP Version 6 (IPv6)	R
4862	IPv6 Stateless Address Autoconfiguration	C
5095	Deprecation of Type 0 Routing Headers in IPv6	R
Notes: C/R-1: Meets only the dual-stack requirements of this RFC. C/R-2: Meets only the IPv6 formatting requirements of this RFC. R-3: Meets only the framing format aspects of RFC. R-4: Requirement covered in Section 6, Network Infrastructure End-to-End Performance. C-5: Condition is that product acts as a router. C-6: Applies only to MGs. C-7: Requirements apply only if the product acts as a CE-R. C/R-8: EI (softphones only).		

Table 5.2-5. UC Router (R)

RFC NUMBER	RFC TITLE	REQUIRED – R CONDITIONAL – C
1772	Application of the Border Gateway Protocol in the Internet	C-7
1981	Path MTU Discovery for IPv6	R
2404	The Use of HMAC-SHA-1-96 within ESP and AH	R
2407	The Internet IP Security Domain of Interpretation for ISAKMP	R
2408	Internet Security Association and Key Management Protocol (ISAKMP)	R
2409	The Internet Key Exchange (IKE)	R
2460	Internet Protocol, Version 6 (v6) Specification	R-2
2464	Transmission of IPv6 Packets over Ethernet Networks	R-3
2473	Generic Packet Tunneling in IPv6 Specification	C-7
2474	Definition of the Differentiated Services Field (DS Field) in the IPv4 and IPv6 Headers	R-4
2545	Use of BGP-4 Multiprotocol Extensions for IPv6 Inter-Domain Routing	C-7
2710	Multicast Listener Discovery (MLD) for IPv6	R
2711	IPv6 Router Alert Option	R
2784	Generic Router Encapsulation	C-7

RFC NUMBER	RFC TITLE	REQUIRED – R CONDITIONAL – C
3162	RADIUS and IPv6	C
3168	The Addition of Explicit Congestion Notification (ECN) to IP	C
3315	Dynamic Host Configuration Protocol for IPv6 (DHCPv6)	C
3411	An Architecture for Describing Simple Network Management Protocol (SNMP) Management Frameworks	C
3412	Message Processing and Dispatching for the Simple Network Management Protocol (SNMP)	C
3413	Simple Network Management Protocol (SNMP) Applications	C
3810	Multicast Listener Discovery Version 2 (MLDv2) for IPv6	R
3986	Uniform Resource Identifier (URI): Generic Syntax	C
4007	IPv6 Scoped Address Architecture	R
4022	Management Information Base for the Transmission Control Protocol (TCP)	C
4087	IP Tunnel MIB	C
4109	Algorithms for Internet Key Exchange Version 1 (IKEv1)	R
4113	Management Information Base for the User Datagram Protocol (UDP)	C
4213	Basic Transition Mechanisms for IPv6 Hosts and Routers	R-1
4271	A Border Gateway Protocol 4 (BGP-4)	C-7
4282	The Network Access Identifier	C
4291	IP Version 6 Addressing Architecture	R
4292	IP Forwarding MIB	C
4293	Management Information Base for the Internet Protocol (IP)	C
4301	Security Architecture for the Internet Protocol	R
4302	IP Authentication Header	R
4303	IP Encapsulating Security Payload (ESP)	R
4443	Internet Control Message Protocol (ICMPv6) for the Internet Protocol Version 6 (IPv6) Specification	R
4552	Authentication Confidentiality for OSPFv3	R
4760	Multiprotocol Extensions for BGP-4	C-7, C
4807	IPSec Security Policy Database Configuration MIB	C
4835	Cryptographic Algorithm Implementation Requirements for Encapsulating Security Payload (ESP) and Authentication Header (AH)	R
4861	Neighbor Discovery for IP Version 6 (IPv6)	R
4862	IPv6 Stateless Address Autoconfiguration	C
5072	IP Version 6 over PPP	C
5095	Deprecation of Type 0 Routing Headers in IPv6	R

RFC NUMBER	RFC TITLE	REQUIRED – R CONDITIONAL – C
5304	IS-IS Cryptographic Authentication	C
5308	Routing IPv6 with IS-IS	C
5310	IS-IS Generic Cryptographic Authentication	C
5340	OSPF for IPv6	R
5798	Virtual Router Redundancy Protocol (VRRP) Version 3 for IPv4 and IPv6	C

Notes:
C/R-1: Meets only the dual-stack requirements of this RFC.
C/R-2: Meets only the IPv6 formatting requirements of this RFC.
R-3: Meets only the framing format aspects of RFC.
R-4: Requirement covered in Section 6, Network Infrastructure End-to-End Performance.
C-5: Condition is that product acts as a router.
C-6: Applies only to MGs.
C-7: Requirements apply only if the product acts as a CE-R.
C/R-8: EI (softphones only)

Table 5.2-6. LAN Switch (LS)

RFC NUMBER	RFC TITLE	REQUIRED – R CONDITIONAL – C
Part 1 LAN Access Switch		
1981	Path MTU Discovery for IPv6	R
2407	The Internet IP Security Domain of Interpretation for ISAKMP	C
2408	Internet Security Association and Key Management Protocol (ISAKMP)	C
2409	The Internet Key Exchange (IKE)	C
2460	Internet Protocol, Version 6 (v6) Specification	C-2
2464	Transmission of IPv6 Packets over Ethernet Networks	R-3
2474	Definition of the Differentiated Services Field (DS Field) in the IPv4 and IPv6 Headers	R-4
3168	The Addition of Explicit Congestion Notification (ECN) to IP	C
3411	An Architecture for Describing Simple Network Management Protocol (SNMP) Management Frameworks	C
3412	Message Processing and Dispatching for the Simple Network Management Protocol (SNMP)	C
3413	Simple Network Management Protocol (SNMP) Applications	C
3986	Uniform Resource Identifier (URI): Generic Syntax	C
4007	IPv6 Scoped Address Architecture	R
4022	Management Information Base for the Transmission Control Protocol (TCP)	C
4087	IP Tunnel MIB	C
4109	Algorithms for Internet Key Exchange Version 1 (IKEv1)	C

RFC NUMBER	RFC TITLE	REQUIRED – R CONDITIONAL – C
4113	Management Information Base for the User Datagram Protocol (UDP)	C
4291	IP Version 6 Addressing Architecture	R
4292	IP Forwarding MIB	C
4293	Management Information Base for the Internet Protocol (IP)	C
4301	Security Architecture for the Internet Protocol	C
4302	IP Authentication Header	C
4303	IP Encapsulating Security Payload (ESP)	C
4443	Internet Control Message Protocol (ICMPv6) for the Internet Protocol Version 6 (IPv6) Specification	R
4807	IPSec Security Policy Database Configuration MIB	C
4835	Cryptographic Algorithm Implementation Requirements for Encapsulating Security Payload (ESP) and Authentication Header (AH)	C
4862	IPv6 Stateless Address Autoconfiguration	C
5095	Deprecation of Type 0 Routing Headers in IPv6	C
Part 2 LAN Distributed L3 Switch Requirements from Part 1 above, plus the below		
1981	Path MTU Discovery for IPv6	C-5
2404	The Use of HMAC-SHA-1-96 within ESP and AH	C-5
2710	Multicast Listener Discovery (MLD) for IPv6	C-5
2711	IPv6 Router Alert Option	C-5
3162	RADIUS and IPv6	C-5
3315	Dynamic Host Configuration Protocol for IPv6 (DHCPv6)	C-5, C-9
3810	Multicast Listener Discovery Version 2 (MLDv2) for IPv6	C-5
4213	Basic Transition Mechanisms for IPv6 Hosts and Routers	C-1, C-5
4552	Authentication Confidentiality for OSPFv3 (Routing protocol authentication only)	C-5
4861	Neighbor Discovery for IP Version 6 (IPv6)	C-5
5304	IS-IS Cryptographic Authentication	C-5
5308	Routing IPv6 with IS-IS	C-5
5310	IS-IS Generic Cryptographic Authentication	C-5
5340	OSPF for IPv6	C-5
5798	Virtual Router Redundancy Protocol (VRRP) Version 3 for IPv4 and IPv6	R
Part 3 LAN Core L3 Switch Requirements from Part 2 above, plus the below		
1772	Application of the Border Gateway Protocol in the Internet	C-7
2473	Generic Packet Tunneling in IPv6 Specification	C-7

RFC NUMBER	RFC TITLE	REQUIRED – R CONDITIONAL – C
2545	Use of BGP-4 Multiprotocol Extensions for IPv6 Inter-Domain Routing	C-7
4271	A Border Gateway Protocol 4 (BGP-4)	C-7
4760	Multiprotocol Extensions for BGP-4	C-7

Notes:
C/R-1: Meets only the dual-stack requirements of this RFC.
C/R-2: Meets only the IPv6 formatting requirements of this RFC.
R-3: Meets only the framing format aspects of RFC.
R-4: Requirement covered in Section 6, Network Infrastructure End-to-End Performance.
C-5: Condition is that product acts as a router.
C-6: Applies only to MGs.
C-7: Requirements apply only if the product acts as a CE-R.
C/R-8: EI (softphones only).
C-9: Condition is that product supports DHCP.

Table 5.2-7. UC Information Assurance Security Devices (SD)

RFC NUMBER	RFC TITLE	REQUIRED – R CONDITIONAL – C
1981	Path MTU Discovery for IPv6	R
2407	The Internet IP Security Domain of Interpretation for ISAKMP	C
2408	Internet Security Association and Key Management Protocol (ISAKMP)	C
2409	The Internet Key Exchange (IKE)	C
2460	Internet Protocol, Version 6 (v6) Specification	R-2
2464	Transmission of IPv6 Packets over Ethernet Networks	R-3
2474	Definition of the Differentiated Services Field (DS Field) in the IPv4 and IPv6 Headers	R-4
2710	Multicast Listener Discovery Version 2 (MLDv2) for IPv6	R
3162	RADIUS and IPv6	C
3986	Uniform Resource Identifier (URI): Generic Syntax	C
4007	IPv6 Scoped Address Architecture	R
4109	Algorithms for Internet Key Exchange Version 1 (IKEv1)	C
4213	Basic Transition Mechanisms for IPv6 Hosts and Routers	R-1
4291	IP Version 6 Addressing Architecture	R
4301	Security Architecture for the Internet Protocol	C
4302	IP Authentication Header	C
4303	IP Encapsulating Security Payload (ESP)	C
4443	Internet Control Message Protocol (ICMPv6) for the Internet Protocol Version 6 (IPv6) Specification	R
4566	SDP: Session Description Protocol	C

RFC NUMBER	RFC TITLE	REQUIRED – R CONDITIONAL – C
4835	Cryptographic Algorithm Implementation Requirements for Encapsulating Security Payload (ESP) and Authentication Header (AH)	C
4861	Neighbor Discovery for IP version 6 (IPv6)	R
4862	IPv6 Stateless Address Autoconfiguration	C
5095	Deprecation of Type 0 Routing Headers in IPv6	R

Notes:
C/R-1: Meets only the dual-stack requirements of this RFC.
C/R-2: Meets only the IPv6 formatting requirements of this RFC.
R-3: Meets only the framing format aspects of RFC.
R-4: Requirement covered in Section 6, Network Infrastructure End-to-End Performance.
C-5: Condition is that product acts as a router.
C-6: Applies only to MGs.
C-7: Requirements apply only if the product acts as a CE-R.
C/R-8: EI (softphones only).

SECTION 6
NETWORK INFRASTRUCTURE END-TO-END PERFORMANCE

6.1 INTRODUCTION

This section focuses on the Wide Area Network (WAN) performance characteristics for Layer 3 routers and switches used in the End-to-End (E2E) Unified Capabilities (UC) network infrastructure. It defines the Differentiated Services Code Point (DSCP) Plan, Per-Hop Behavior (PHB) policy and priority as applied to packets based on the granular service class when traversing a Defense Information Systems Network (DISN) network hop, and traffic conditioning treatment requirements that are to be given to network queues. These requirements are additional to those defined in other sections of this document as follows:

1. Assured Services Local Area Network (ASLAN) Infrastructure requirements [i.e., Local Area Network (LAN) Core, Distribution, and Access switches; Customer Edge (CE) Routers (CE-Rs)] as defined in Section 7, Network Edge Infrastructure.
2. Network Infrastructure product requirements (i.e., DISN Router, Switch, and Access Elements) as defined in Section 10, Network Infrastructure Products.
3. E2E network design guidelines as described in Department of Defense (DoD) UC Framework 2013, Section 6.

A summary of network performance requirements as described in the UC Framework document is included in Section 6.1.1, Network Infrastructure Design Synopsis, as a reference.

6.1.1 Network Infrastructure Design Synopsis

The E2E network infrastructure consists of three network segments: the CE, Network Edge, and Core. These are illustrated in Figure 6.1-1 and described in detail in DoD UC Framework 2013, Section 6.

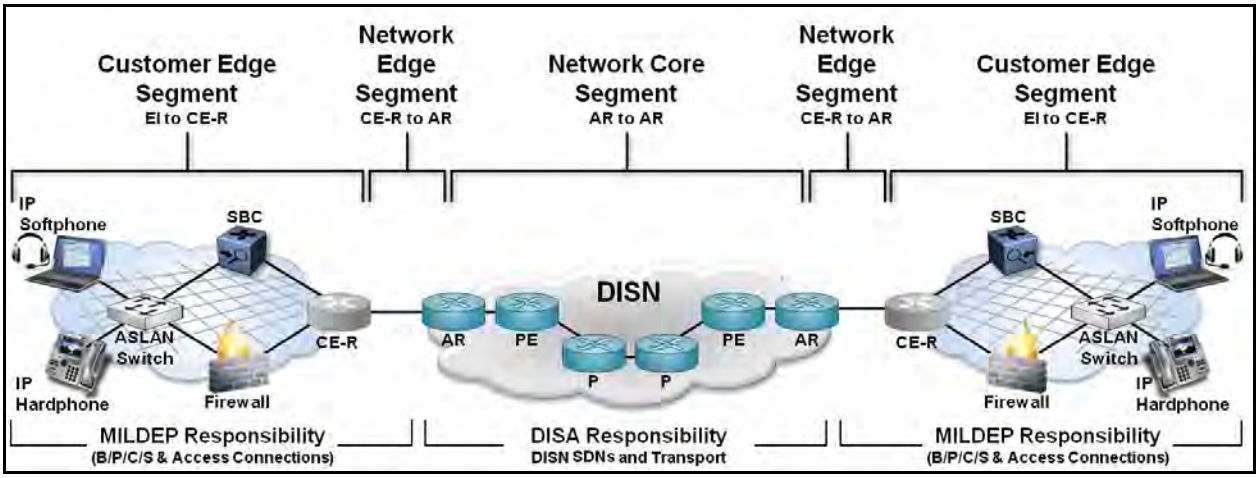


Figure 6.1-1. UC E2E Network Segments and Measurement Reference Points

6.2 GENERAL NETWORK

The primary performance driver for voice products in the DISN is the E2E voice quality.

WAN-000010 [**Required**] Voice quality shall be calculated E2E from handset to handset using the E-Model as described in the Telecommunications Industry Association (TIA)/ Telecommunication Standardization Bureau (TSB)-116 A, which is based on recommendation G.107.

6.3 PER-HOP BEHAVIOR AND SERVICE-LEVEL OBJECTIVE (SLO)

The Differentiated Services (DS) Architecture uses the terms Per-Hop Behavior (PHB) and Service Level Objective (SLO) to describe a service convention that specifies the forwarding service a customer should receive. The SLO includes service and traffic conditioning parameters and rules that constitute the overall design. The SLO is divided into Service-Level Specification (SLS), Traffic Conditioning Specification (TCS), and Traffic Conditioning Agreement (TCA). These rules are defined in Request for Comments (RFC) 3260, which updates RFCs 2474, 2475, and 2597.

6.3.1 Service-Level Specification (Previously Summary of Granular Service Class Performance Objectives)

The SLS is a set of parameters whose values together define the minimum acceptable service to be offered to a pre-determined network segment based on pre-defined Granular Service Classes.

Table 6.3-1, Service-Level Specification, summarizes the SLS for each granular UC service class as defined in DoD UC Framework 2013, Section 6. This table defines one-way performance requirements.

Table 6.3-1. Service-Level Specification

GRANULAR SERVICE CLASS	E2E LATENCY (MS)	AR-AR LATENCY (MS)	EI-CER LATENCY (MS)	E2E PACKET LOSS (%)	AR-AR PACKET LOSS (%)	EI-CER PACKET LOSS (%)	E2E JITTER (MS)	AR-AR JITTER (MS)	EI-CER JITTER (MS)
Short Messaging	1000	900	50	0.5	0.4	0.05			
Assured Voice	220	150	35	1	0.8	0.05	20	14	3
Assured Multimedia Conferencing	220	150	35	1	0.8	0.05	20	14	3
Broadcast Video	1000	900	50	0.1	0.08	0.01			
Multimedia Streaming (includes Non-Assured Video)	250	180	35	1	0.8	0.05	20	14	3

GRANULAR SERVICE CLASS	E2E LATENCY (MS)	AR-AR LATENCY (MS)	EI-CER LATENCY (MS)	E2E PACKET LOSS (%)	AR-AR PACKET LOSS (%)	EI-CER PACKET LOSS (%)	E2E JITTER (MS)	AR-AR JITTER (MS)	EI-CER JITTER (MS)
Non-Assured Voice	250	180	35	1	0.8	0.05	20	14	3
Low Latency Data: Instant Messaging (IM)/Chat, Presence	300	200	50	1	0.8	0.05			
High Throughput Data: Real-Time Data Backup, Web Hosting	300	200	50	1	0.8	0.05			
NOTE: Not All Aggregate Service Classes Have Performance Objectives (Best Effort, Signaling, Network Control, and Low Priority)									

WAN-000020 [**Required**] Products that provide UC services shall support the SLS based on the Granular Service Class as defined in Table 6.3-1, Service-Level Specification.

6.3.2 Traffic Conditioning Specification

The TCS is a set of parameters whose values together specify the DSCP classifier rules and traffic profiles for Aggregate and Granular Service Classes within DoD.

WAN-000030 [**Required**] Products that provide UC services shall support the TCS, which defines the DSCP Plan used in the DoD and is shown in Table 6.3-2, Traffic Conditioning Specification.

Table 6.3-2. Traffic Conditioning Specification

AGGREGATED SERVICE CLASS	GRANULAR SERVICE CLASS	PRIORITY/ PRECEDENCE	DSCP BASE10	DSCP BINARY	DSCP BASE8
Network Control	Network Signaling (OSPF, BGP, etc.)	N/A	48	110 000	60
Inelastic Real-Time	User Signaling (AS-SIP, H.323, etc.)	N/A	40	101 000	50
	Short Message	FO	32	100 000	40
	Assured Voice (Includes SRTCP)	FO	41	101 001	51
		F	43	101 011	53
		I	45	101 101	55
		P	47	101 111	57
		R	49	110 001	61
	Non-Assured Voice*	N/A	46	101 110	56
	Assured Multimedia	FO	33	100 001	41

AGGREGATED SERVICE CLASS	GRANULAR SERVICE CLASS	PRIORITY/ PRECEDENCE	DSCP BASE10	DSCP BINARY	DSCP BASE8
	Conferencing (voice, video, and data) (code points 28, 30, 34, 36, and 38 are for Non-Assured Multimedia Conferencing)	F	35	100 011	43
		I	37	100 101	45
		P	39	100 111	47
		R	51 [28, 30, 34,36,38]**	110 011	63
	Broadcast Video	N/A	24	011 000	30
Preferred Elastic	Multimedia Streaming	FO	25	011 001	31
		F	27	011 011	33
		I	29	011 101	35
		P	31	011 111	37
		R	26	011 010	32
	Low-Latency Data: (IM, Chat, Presence)	FO	17	010 001	21
		F	19	010 011	23
		I	21	010 101	25
		P	23	010 111	27
		R	18 [20,22]**	010 010	22
	High Throughput Data (Real-Time Data Backup, Web Hosting)	FO	9	001 001	11
		F	11	001 011	13
		I	13	001 101	15
		P	15	001 111	17
		R	10 [12,14]**	001 010	12
	OA&M	N/A	16	010 000	20
Elastic	Best Effort	N/A	0	000 000	00
	Low Priority Data	N/A	8	001 000	10

LEGEND:

AS-SIP: Assured Services Session Initiation Protocol	N/A: Not Applicable
BGP: Border Gateway Protocol	OA&M: Operations, Administration, and Maintenance
DSCP: Differentiated Services Code Point	OSPF: Open Shortest Path First
F: FLASH	P: PRIORITY
FO: FLASH OVERRIDE	R: ROUTINE
IM: Instant Messaging	SRTCP: Secure Real-Time Transport Control Protocol
I: INTERMEDIATE	

* For a definition, see UC Framework 2013, Appendix C, Definitions, Abbreviations and Acronyms, and References.

AGGREGATED SERVICE CLASS	GRANULAR SERVICE CLASS	PRIORITY/ PRECEDENCE	DSCP BASE10	DSCP BINARY	DSCP BASE8
** Code points in brackets are reserved for nonconformance marking.					

WAN-000040 [**Required**] DS assignments shall be software configurable for the full range of six-bit values (0–63 Base10) for backwards compatibility with Internet protocol (IP) precedence environments that may be configured to use the Type of Service (TOS) field in the IP header but that do not support DSCP.

WAN-000050 [**Conditional**] If Layer 3 devices supporting UC services are configured with interfaces T1 and below or on routers that do not support the six-queue model, then Layer 3 devices shall support configuration of the four-queue PHBs, as defined in Table 6.3-3, Four-Queue PHB Approach. Otherwise, the system routers supporting UC services shall support configuration of the six-queue PHBs as defined in Table 6.3-4, Six-Queue PHB Approach.

Table 6.3-3. Four-Queue PHB Approach

QUEUE	GRANULAR SERVICE CLASS	PRIORITY/ PRECEDENCE	DSCP BASE10	PHB
3	Network Signaling (See Note)	N/A	48	EF
	User Signaling	N/A	40	
	Short Message	FO	32	
	Assured Voice	FO	41	
		F	43	
		I	45	
		P	47	
		R	49	
2	Assured Multimedia Conferencing (Assured Video Conferencing)	FO	33	AF41
		F	35	
		I	37	
		P	39	
		R	51	
1	Broadcast Video	N/A	24	AF31
	Non-Assured Voice*	N/A	46	
	Multimedia Streaming (Video Streaming)	FO	25	
		F	27	
		I	29	
		P	31	
		R	26	
	Non-Assured Multimedia	FO	28	

QUEUE	GRANULAR SERVICE CLASS	PRIORITY/ PRECEDENCE	DSCP BASE10	PHB
	Conferencing (Non-Assured Video Conferencing)	F	30	
		I	34	
		P	36	
		R	38	
	Low-Latency Data (IM, Chat, Presence)	FO	17	
		F	19	
		I	21	
		P	23	
		R	18 [20,22]**	
	High Throughput Data (Real-Time Data Backup, Web Hosting)	FO	9	AF32
		F	11	
		I	13	
		P	15	
		R	10 [12,14]**	
	OA&M	N/A	16	
0	Best Effort	N/A	0	Default
	Low Priority	N/A	8	

NOTE: Many routers have a separate non-configurable queue for network control traffic. If a router does not have the network control queue, the network control traffic would be processed in the EF queue.

LEGEND:

AF: Assured Forwarding	I: IMMEDIATE	OSPF: Open Shortest Path First
DSCP: Differentiated Services Code Point	IM: Instant Messaging	P: PRIORITY
EF: Expedited Forwarding	IS-IS: Intermediate System-to-Intermediate System Protocol	PHB: Per Hop Behavior
F: FLASH	N/A: Not Applicable	R: ROUTINE
FO: FLASH OVERRIDE	OA&M: Operations, Administration, and Maintenance	

* For a definition, see UC Framework 2013, Appendix C, Definitions, Abbreviations and Acronyms, and References.

** Code points in brackets are reserved for nonconformance marking.

Table 6.3-4. Six-Queue PHB Approach

QUEUE	GRANULAR SERVICE CLASS	PRIORITY/ PRECEDENCE	DSCP BASE10	CER PHB
5	Network Signaling (See note)	N/A	48	EF
4	User Signaling	N/A	40	

QUEUE	GRANULAR SERVICE CLASS	PRIORITY/ PRECEDENCE	DSCP BASE10	CER PHB
	Short Message	FO	32	
	Assured Voice	FO	41	
		F	43	
		I	45	
		P	47	
		R	49	
	Assured Multimedia Conferencing (Assured Video Conferencing)	FO	33	
		F	35	
		I	37	
		P	39	
		R	51	
3	Broadcast Video	N/A	24	
	Non-Assured Voice*	N/A	46	
	Non-Assured Multimedia Conferencing (Non-Assured Video Conferencing)	FO	28	
		F	30	
		I	34	
		P	36	
		R	38	
2	Multimedia Streaming (Video Streaming)	FO	25	AF
		F	27	
		I	29	
		P	31	
		R	26	
	Low-Latency Data (IM, Chat, Presence)	FO	17	
		F	19	
		I	21	
		P	23	
		R	18 [20,22]**	
	High Throughput Data (Real-Time Data Backup, Web Hosting)	FO	9	
		F	11	
		I	13	
		P	15	
		R	10 [12,14]**	
	OA&M	N/A	16	
1	Best Effort (Default)	N/A	All Remaining	BE

QUEUE	GRANULAR SERVICE CLASS	PRIORITY/ PRECEDENCE	DSCP BASE10	CER PHB
0	Low Priority	N/A	8	
NOTE:	Many routers have a separate non-configurable queue for network control traffic. If a router does not have the network control queue, the network control traffic would be processed in the EF queue.			

LEGEND:

AF: Assured Forwarding	FO: FLASH OVERRIDE	R: ROUTINE
CER: Customer Edge Router	I: IMMEDIATE	N/A: Not Applicable
DSCP: Differentiated Services Code Point	IM: Instant Messaging	OA&M: Operations, Administration, and Maintenance
EF: Expedited Forwarding	P: PRIORITY	
F: FLASH	PHB: Per Hop Behavior	

* For a definition, see UC Framework 2013, Appendix C, Definitions, Abbreviations and Acronyms, and References.

** Code points in brackets are reserved for nonconformance marking.

WAN-000060 [**Required**] The same queuing model (six or four) shall be configured at both ends of the communication path to prevent asymmetrical performance.

NOTE: The Communication path for this requirement is defined from the egress interface of the local CE-R to the ingress interface of the remote CE-R.

WAN-000070 [**Required**] Bandwidth allocation and negotiation needs to occur between the Aggregation Router (AR) and the CE-R to prevent asymmetrical performance.

NOTE: The purpose of this requirement is to prevent back throttling, delay, jitter, or drop packets on EF queues because of asymmetrical queue configuration between the CE-R and the AR.

WAN-000080 [**Required**] The CE-R bandwidth budget must be less than or equal to the AR bandwidth budget per queue.

NOTE 1: For example, if a Session Controller (SC) session budget is 10 voice sessions, then the CE-R bandwidth budget for the EF queue must be greater than 1,100 kbps (10 x 110 kbps). If the CE-R bandwidth budget was, for example, 1400 kbps to account for expected growth, surge, or other unplanned EF traffic, then the AR bandwidth must be greater than 1400 kbps or greater than the CE-R bandwidth budget. The SC session budget must be less than the equivalent CE-R bandwidth budget, in the scenario previously described, less than 1400 kbps.

NOTE 2: PHB requirements are outlined in RFC 3246 and RFC 3260.

6.3.3 Traffic Conditioning Agreement (Previously Traffic Conditioning Requirements)

The TCA is the convention for how classifier rules and profiles defined by the TCS are metered, provisioned, marked, discarded and shaped based on the type of Aggregate or Granular service class.

WAN-000090 [**Required**] All CE-R and/or AR egress interfaces in the direction of the DISN shall mark packets in accordance with the TCS as defined in Section 6.3.2, Traffic Conditioning Specification (Previously Differentiated Services Code Point Plan).

WAN-000100 [**Required**] All CE-R and/or AR egress interfaces in the direction of the DISN shall support configuration of network queues in accordance with the TCS as defined in Table 6.3-2, Traffic Conditioning Specification, on an Aggregate Service class perspective on the input interface.

NOTE: When other queues are not saturated, the Best Effort traffic may surge beyond its traffic-engineered limit.

WAN-000110 [**Required**] All CE-R and/or AR egress interfaces in the direction of the DISN shall support configuration of network queues in accordance with the TCS as defined in Table 6.3-2, Traffic Conditioning Specification, on an Aggregate Service class perspective on the output interface.

NOTE: When other queues are not saturated, the Best Effort traffic may surge beyond its traffic-engineered limit.

WAN-000120 [**Required**] All CE-R and/or AR egress interfaces in the direction of the DISN shall have the capability to perform traffic conditioning as per the definition in DoD UC Framework 2013, Appendix C, Definitions, Abbreviations and Acronyms, and References.

NOTE 1: It is beyond the scope of this document to mandate specific bandwidth throttling, rate limiting or discarding mechanisms to manage congestion. It is up to the discretion of the Network Administrator to make the appropriate determination for the individual network.

NOTE 2: General Traffic Conditioning guidelines and considerations can be found in UC Framework 2013, Section 6.12, UC Network Infrastructure Survivability.

WAN-000130 [**Required**] The product shall calculate or be configurable to support bandwidth metering and provisioning.

NOTE: Queue size should account for the Layer 3 header (i.e., IP header) but not the Layer 2 headers (i.e., Point-to-Point Protocol [PPP]; MAC, etc.) within a margin of error of 10 percent, analogous as to how packet size is calculated for transmission IAW RFC 3246, Section 2.2.

WAN-000140 [**Required**] The system Layer 3 devices shall be able to traffic condition using IP addresses, protocol port numbers, and DSCPs as discriminators, at a minimum.

NOTE: The definition of traffic engineering is found in DoD UC Framework 2013, Appendix C, Definitions, Abbreviations and Acronyms, and References.

6.4 VVOIP NETWORK INFRASTRUCTURE NETWORK MANAGEMENT

The Voice and Video over Internet Protocol (VVoIP) Network Infrastructure Network Management (NM) requirements have been relocated to Section 2.19, Management of Network Appliances.

SECTION 7
NETWORK EDGE INFRASTRUCTURE

7.1 INTRODUCTION

This section defines the following:

- Technical requirements for the products used in configuring the network edge infrastructure.
- Technical requirements for Customer Edge (CE) Routers (CERs).
- Design requirements for Assured Services (AS) Local Area Networks (LANs) (ASLANs).

The network edge infrastructure consists of LAN products, local Digital Subscriber Line (DSL) and Passive Optical Network (PON) transport products, and the CER. The design requirements, based on commercial standards, were developed to support assured services for mission-critical users.

7.1.1 LAN Infrastructure Requirements by End User and Mission Environments

In order to provide cost-effective LAN solutions that meet mission requirements for all users served by a LAN, two types of LANs are defined: ASLANs and non-ASLANs. The LANs will be designed to meet traffic engineering and redundancy requirements, as required by applicable mission needs.

Table 7.1-1 summarizes selected LAN requirements in terms of LAN types and end user mission category.

Table 7.1-1. Summary of LAN Requirements by End User Mission Category

REQUIREMENT ITEM	SUBSCRIBER MISSION CATEGORY			
	F/FO	I/P	R	NON-MISSION CRITICAL
ASLAN High	R	P	P	P
ASLAN Medium	NP	P	P	P
Non-ASLAN	NP	NP	N	P
Redundancy (including diversity)	R	R	NR	NR
Battery Backup	8 hours	2 hours	NR	NR
Single Point of Failure User > 96 Allowed	No	No	Yes	Yes
Availability	99.999	99.997	99.9	99.8
LEGEND				
ASLAN: Assured Services LAN	LAN: Local Area Network		p: Probability of Blocking	
F/FO: FLASH/FLASH OVERRIDE	MLPP: Multilevel Precedence and Preemption			

REQUIREMENT ITEM	SUBSCRIBER MISSION CATEGORY			
	F/FO	I/P	R	NON-MISSION CRITICAL
I/P: IMMEDIATE/PRIORITY	NP: Not Permitted		P: Permitted	
GOS: Grade of Service	NR: Not Required		R: Required	

7.1.2 LAN Types and Nomenclature

The ASLANs and non-ASLANs may be designed to use any combination of the layers and functional capabilities, shown in Figure 7.1-1, LAN Layers. Multiple layers may be combined in a single switch or router (i.e., router acts as Distribution and Access Layers).

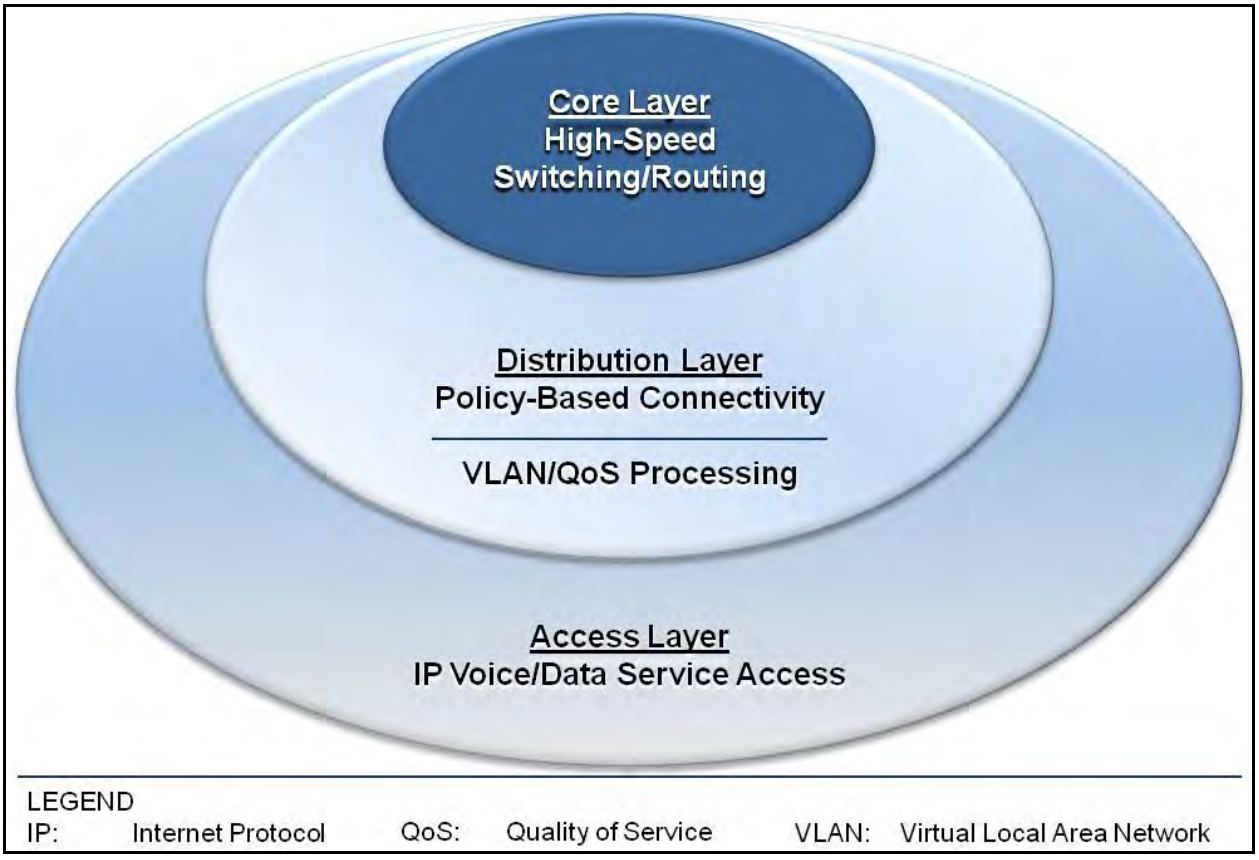


Figure 7.1-1. LAN Layers

The three LAN Layers are as follows:

1. Access Layer. The point at which local end users are allowed into the network. This layer may use access lists or filters to optimize further the needs of a particular set of users.
2. Distribution Layer. The demarcation point between the Access and Core Layers. Helps to define and differentiate the Core. Provides boundary definition and is the place at which packet manipulation can take place.

3. Core Layer. A high-speed switching backbone designed to switch packets as quickly as possible.

Figure 7.1-2, Representative B/P/C/S Design and Terminology, illustrates a typical Base/Post/Camp/Station (B/P/C/S) LAN design. The LAN design and requirements refer to LAN products in terms of the Core, Distribution, and Access Layer products. These products are often known by other names such as Main Communication Node (MCN), Area Distribution Node (ADN), and End User Building (EUB) switch.

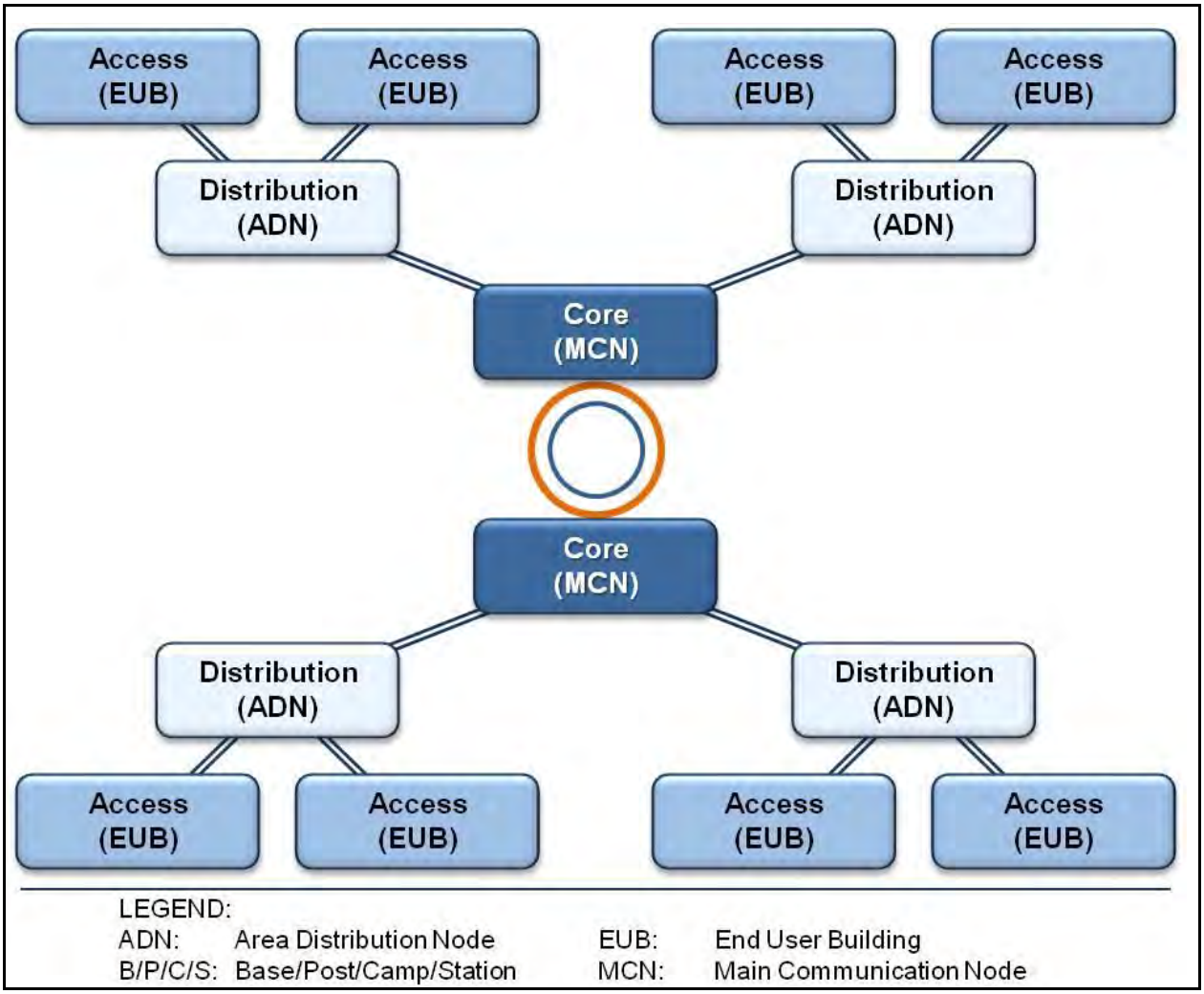


Figure 7.1-2. Representative B/P/C/S Design and Terminology

The LAN infrastructure may use DSL and PON products to extend voice, video, and data services at the access layer of the LAN hierarchy.

7.2 LAN SWITCH AND ROUTER PRODUCT

7.2.1 General LAN Switch and Router Product

EDG-000010 [**Required: Core, Distribution, and Access Products**] The Core, Distribution, and Access products shall be capable of meeting the following parameters:

a. Non-blocking. All Core, Distribution, and Access products shall be non-blocking for their ports based on the following traffic engineering. Non-blocking is defined as the capability to send and receive a mixture of 64 to 1518 byte packets at full duplex rates from ingress ports to egress ports through the component's backplane without losing any packets. In a non-blocking switch, all ports can run at full wire speed without any loss of packets or cells. Blocking factor is defined as the ratio of all traffic to non-blocked traffic (i.e., a blocking factor of 8 to 1 means that 12.5 percent of the traffic must be non-blocking). Each Core, Distribution, and Access product has up to three levels of performance: Minimum, Medium, and Maximum. For certification purposes, products need only meet minimum performance levels.

NOTE: These definitions/requirements are not applicable for wireless products; wireless products are half-duplex in accordance with (IAW) radio limitations.

(1) Access Products. Access products (including PON that is used as an access device) shall not have a blocking factor that exceeds 8 to 1 (minimum). This blocking factor includes all hardware and software components. Medium performance level Access products shall not have a blocking factor that exceeds 2 to 1. This blocking factor includes all hardware and software components. Maximum performance level Access products shall be non-blocking. This blocking factor includes all hardware and software components.

(2) Distribution and Core Products. These products shall not have a blocking factor that exceeds 2 to 1 (minimum). This blocking factor includes all hardware and software components. Medium performance level products shall not have a blocking factor that exceeds 1.5 to 1. This blocking factor includes all hardware and software components. Maximum performance level products shall be non-blocking. This blocking factor includes all hardware and software components.

b. Latency. All Core, Distribution, and Access products shall have the capability to transport prioritized packets (media and signaling) as follows. The latency shall be achievable over any 5-minute period measured from ingress ports to egress ports under congested conditions. Congested condition is defined as 100 percent bandwidth utilization. Prioritized packets are defined as packets having a service class above best effort. Latency numbers do not include serialization delay. Serialization delay may be added to below specified numbers.

(1) Voice Packets. No more than 2 milliseconds (ms) latency.

(2) Voice and video signaling packets. No more than 2 milliseconds (ms) latency.

(3) Video Packets. No more than 10 ms latency. Video packets are defined as including video, voice associated with video session, and video signaling. Video packets include both video teleconferencing and streaming video.

(4) Preferred Data Packets. N/A. Preferred data is defined in the UC Framework as preferred elastic traffic (see UC Framework 2013, Section 6, Network Infrastructure End-to-End Performance).

(5) Best Effort Data. N/A.

c. Jitter. All Core, Distribution, and Access products shall have the capability to transport prioritized packets (media and signaling) as follows. The jitter shall be achievable over any 5-minute period measured from ingress ports to egress ports under congested conditions. Congested condition is defined as 100 percent bandwidth utilization.

(1) Voice Packets. No more than 1 ms jitter.

(2) Video Packets. No more than 10 ms jitter.

(3) Preferred Data Packets. N/A.

(4) Best Effort Data. N/A.

d. Packet Loss. All Core, Distribution and Access products shall have the capability to transport prioritized packets (media and signaling) as follows. The packet loss shall be achievable over any 5-minute period measured from ingress ports to egress ports under congested conditions. Congested condition is defined as 100 percent bandwidth utilization.

(1) Voice Packets. Allowed packet loss is dependent upon the queuing implemented (i.e., amount of properly traffic shaped bandwidth). Packet loss measured within the configured queuing parameters shall be measured to be no more than 0.015 percent for Access, Distribution, and Core products.

(2) Video Packets. Allowed packet loss is dependent on the queuing implemented (i.e., amount of properly traffic shaped bandwidth). Packet loss measured within the configured queuing parameters shall be measured to be no more than 0.05 percent for Access, Distribution, and Core products.

(3) Preferred Data packets. Allowed packet loss is dependent on the queuing implemented (i.e., amount of properly traffic shaped bandwidth). Packet loss measured within the configured queuing parameters shall be measured to be no more than 0.05 percent for Access, Distribution, and Core products.

(4) Best Effort data packets. Best effort data has no packet loss requirements. Amount of loss is determined by traffic engineering and offered load.

7.2.1.1 Port Interface Rates

EDG-000020 [**Required: Core and Distribution Products**] Minimally, Core and Distribution products shall support the following interface rates [other rates and Institute of Electronics and Electrical Engineers (IEEE) standards may be provided as optional interfaces]. Rates specified are the theoretical maximum data bit rate specified for Ethernet; link capacity and effective throughput is influenced by many factors. For calculation purposes, link capacities are to be calculated IAW definitions contained in Request for Comments (RFC) 2330 and RFC 5136. Network Management (NM) interfaces are defined in Section 2.19.

The product must minimally support the following interfaces ~~for interconnection between the core to WAN, distribution-core, and distribution-access~~:

(1) 100 megabits per second (Mbps) in accordance with (IAW) IEEE 802.3u (for interconnection between the distribution-core and distribution access).

(2) 1000 Mbps IAW IEEE 802.3z (For interconnection between the core to WAN, distribution-core, and distribution-access).

EDG-000030 [**Required: Access Products**] Minimally, Access products shall provide one of the following user-side interface rates (other rates and IEEE standards may be provided as optional interfaces):

a. 10 Mbps IAW IEEE 802.3i.

b. 10 Mbps IAW IEEE 802.3j.

c. 100 Mbps IAW IEEE 802.3u.

d. 1000 Mbps IAW IEEE 802.3z.

e. 1000 Mbps IAW IEEE 802.3ab.

EDG-000040 [**Required: Access Products**] Minimally, Access products shall provide one of the following trunk-side interface rates (other rates and IEEE standards may be provided as optional interfaces):

a. 100 Mbps IAW IEEE 802.3u.

b. 1000 Mbps IAW IEEE 802.3z.

EDG-000050 [**Optional: Core, Distribution, and Access Products**] The Core, Distribution, and Access products may provide a fibre channel interface IAW American National Standards Institute (ANSI) International Committee for Information Technology Standards (INCITS) T11.2 and T11.3 (previously known as X3T9.3). If provided, the interface must meet the following:

a. RFC 4338, Transmission of IPv6, IPv4, and Address Resolution Protocol (ARP) Packets over Fibre Channel.

b. RFC 4044, Fibre Channel Management.

EDG-000060 [**Optional: Core, Distribution, and Access Products**] The Core, Distribution, and Access products may provide one or more of the following wireless LAN interface rates:

a. 54 Mbps IAW IEEE 802.11a.

b. 11 Mbps IAW IEEE 802.11b.

c. 54 Mbps IAW IEEE 802.11g.

d. 300–600 Mbps IAW IEEE 802.11n.

e. IEEE 802.16-2012: Broadband wireless communications standards for MANs.

f. Other approved IEEE wireless interfaces may be implemented as optional interfaces.

EDG-000070 [**Conditional**] If any of the above wireless interfaces are provided, then the interfaces must support the requirements of Section 7.3, Wireless LAN.

7.2.1.2 Port Parameter

EDG-000080 [**Required: Core, Distribution, and Access Products**] The Core, Distribution, and Access products shall provide the following parameters on a per port basis as specified:

a. Auto-negotiation IAW IEEE 802.3. All interfaces shall support auto-negotiation even when the IEEE802.3 standard has it as optional. This applies to 10/100/1000-T Ethernet standards (i.e., IEEE Ethernate Standard 802.3, 1993; or IEEE, Fast Ethernet Standard 802.3u, 1995; and IEEE, Gigabit Ethernet Standard 802.3ab, 1999).

b. Force mode IAW IEEE 802.3.

c. Flow control IAW IEEE 802.3x (Optional: Core).

d. Filtering IAW appropriate RFC 1812 sections (sections applying to filtering).

e. Link Aggregation IAW IEEE 802.1AX (applies to output/egress trunk-side ports only) (Optional Access).

f. Spanning Tree Protocol IAW IEEE 802.1D (Optional: Core).

g. Multiple Spanning Tree IAW IEEE 802.1s (Optional: Core).

h. Rapid Reconfiguration of Spanning Tree IAW IEEE 802.1w (Optional: Core).

i. Port-Based Access Control IAW IEEE 802.1x (Optional: Core, Distribution, and Access).

j. Link Layer Discovery Protocol (LLDP) IAW IEEE 802.1AB (Optional Core, Distribution, and Access).

k. Link Layer Discovery – Media Endpoint Discovery IAW ANSI/ Telecommunications Industry Association (TIA)-1057 (Optional Core, Distribution, and Access).

l. Power over Ethernet (PoE) IAW either 802.3af-2003 or 802.3at-2009. (Required only for VVoIP solutions; for data applications or non-Assured Services (AS) solutions, PoE is optionally required.)

7.2.1.3 Class of Service Markings

EDG-000090 [**Required: Core, Distribution, and Access Products**] The Core, Distribution, and Access products shall support Differentiated Services Code Points (DSCPs) IAW RFC 2474 for both Internet Protocol (IP) IPv4 and IPv6 Packets, as follows:

a. The Core and Distribution products shall be capable of accepting any packet tagged with a DSCP value (0-63) on an ingress port and assign that packet to a Quality of Service (QoS) behavior listed in Section 7.2.1.6, Quality of Service Features.

b. The Core and Distribution products shall be capable of accepting any packet tagged with a DSCP value (0-63) on an ingress port and reassign that packet to any new DSCP value (0-63). Current DSCP values are provided in Section 6.2.2, Differentiated Service Code Point. (Optional: Access products)

c. The Core and Distribution products must be able to support the prioritization of aggregate service classes with queuing according to Section 7.2.1.6, Quality of Service Features.

d. Access products (including Passive Optical Network) shall be capable of supporting the prioritization of aggregate service classes with queuing according to Section 7.2.1.6, Quality of Service Features. Queuing may be supported in either of the two following class of service (CoS) methods:

   (1) Layer 3 CoS. Layer 3 Cos involves support for DSCP IAW RFC 2474 for IPv4 and IPv6. Within this CoS method, the access product shall support queueing by either: a) queuing directly based on the DSCP within the IP header (IPv4 and IPv6). The original DSCP value must also be preserved and passed unaltered through the product; or, b) The product shall inspect the IP header (IPv4 and IPv6). Based on the DSCP value contained within the IP header, the product may map the DSCP value (0-63) to the Ethernet priority field (decimal values 0-7). Queuing may be based on the mapping of the DSCP to a layer 2 priority field value. Any received DSCP value (0-63) must be able to be mapped to any priority value (0-7). The original DSCP value must be preserved and passed unaltered through the product.

   (2) Layer 2 Cos. Layer 2 CoS shall use the Virtual LAN identification (VLAN ID), see Section 7.2.1.4, defined in IEEE 802.1Q to perform queuing assignment. Access devices shall be capable of assigning any VLAN ID (either directly or through the 3 Ethernet priority bits (decimal values 0 through 7) to any of the 4 queues.

NOTE: Layer 3 CoS DSCP support shall follow the 18-month rule in that it will be come effective 18-moths after the approval of UCR 2013. At that time, Layer 2 CoS shall no longer be required but may be provided as an optional feature.

EDG-000100 [**Optional: Core, Distribution, and Access Products**] The Core, Distribution, and Access products may support the 3-bit user priority field of the IEEE 802.1Q 2-byte Tag Control Information (TCI) field (see Figure 7.2-1, IEEE 802.1Q Tagged Frame for Ethernet, and

Figure 7.2-2, TCI Field Description). Default values are provided in Table 7.2-1, 802.1Q Default Values. If provided, the following Class of Service (CoS) requirements apply:

a. The Core, Distribution, and Access products shall be capable of accepting any frame tagged with a user priority value (0–7) on an ingress port and assign that frame to a QoS behavior listed in Section 7.2.1.6, Quality of Service Features.

b. The Core and Distribution products shall be capable of accepting any frame tagged with a user priority value (0-7) on an ingress port and reassign that frame to any new user priority value (0-7) (Optional: Distribution and Access).

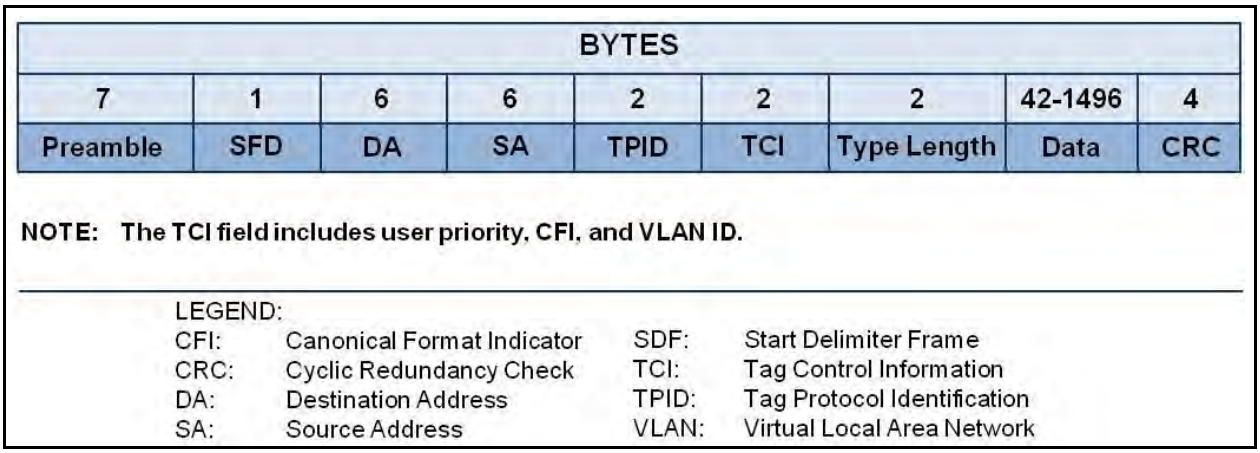


Figure 7.2-1. IEEE 802.1Q Tagged Frame for Ethernet

Table 7.2-1. 802.1Q Default Values

AGGREGATE SERVICE CLASS	GRANULAR SERVICE CLASS	DEFAULT 802.1Q COS TAG	
		BASE 2	BASE 10
Control	Network Control	111	7
Inelastic/ Real-Time	User Signaling1	110	6
	Circuit Emulation1	110	6
	Short messages1	110	6
	Voice2	101	5
	Video/VTC	100	4
	Streaming	011	3
Preferred Elastic	Interactive Transactions OA&M – SNMP	010	2
	File Transfers OA&M – Trap/SysLog	001	1
Elastic	Default	000	0

AGGREGATE SERVICE CLASS	GRANULAR SERVICE CLASS	DEFAULT 802.1Q COS TAG	
		BASE 2	BASE 10
NOTES: 1. All user signaling (voice and video) may be grouped into this granular service class. User signaling, circuit emulation, and short messages may use the same TCI tag. 2. Voice traffic must be differentiated with a different TCI tag from user signaling, circuit emulation, and short messages.			
LEGEND			
802.1Q: IEEE VLAN/User Priority Specification		SysLog: System Log	
CoS: Class of Service		TCI: Tag Control Information	
OA&M: Operations, Administration, and Maintenance		VLAN: Virtual Local Area Network	
SNMP: Simple Network Management Protocol		VTC: Video Teleconferencing	

7.2.1.4 Virtual LAN Capabilities

EDG-000110 [**Required: Core, Distribution, and Access Products**] The Core, Distribution, and Access products shall be capable of the following:

a. Accepting Virtual Local Area Network (VLAN) tagged frames according to IEEE 802.1Q (see Figure 7.2-1, IEEE 802.1Q Tagged Frame for Ethernet, and Figure 7.2-2, TCI Field Description).

BITS		
3	1	12
User Priority	CFI	VID

NOTES:
1. **User Priority. Defines eight (23) user priority levels. Access devices must be capable of recognizing the user priorities (0–7) and assign them to the QoS mechanisms listed below.**
2. **CFI. Always set to zero for Ethernet switches. CFI is used for compatibility reasons between Ethernet type network and Token Ring type network. If a frame received at an Ethernet port has a CFI set to 1, then that frame should not be forwarded as it is to an untagged port.**
3. **VID. Has 12 bits and allows the identification of 4096 (212) VLANs. Of the 4096 possible VIDs, a VID of 0 is used to identify priority frames and value 4095 (FFF) is reserved, so the maximum possible VLAN configurations are 4094.**

LEGEND:
CFI: Canonical Format Indicator
QoS: Quality of Service
VID: VLAN Identification
VLAN: Virtual Local Area Network

Figure 7.2-2. TCI Field Description

b. Configuring VLAN IDs (VIDs). VIDs on an ingress port shall be configurable to any of the 4094 values (except 0 and 4095).

c. Supporting VLANs types IAW IEEE 802.1Q.

The VLANs offer the following features:

- Broadcast Control. Just as switches isolate collision domains for attached hosts and forward only appropriate traffic out a particular port, VLANs refine this concept further and provide complete isolation between VLANs. A VLAN is a bridging domain, and all broadcast and multicast traffic is contained within it.
- Security. The VLANs provide security in two ways:
  - High-security users can be grouped into a VLAN, possibly on the same physical segment, and no users outside of that VLAN can communicate with them.
  - The VLANs are logical groups that behave like physically separate entities; inter-VLAN communication is achieved through a router. When inter-VLAN communication occurs through a router, all the security and filtering functionality that routers traditionally provide can be used because routers are able to look at Layer 3 information.

VLANs are defined as follows:

- Port-Based. Port-based VLANs are VLANs that are dependent on the physical port a product is connected to. All traffic that traverses the port is marked with the VLAN configured for that port. Each physical port on the switch can support only one VLAN. With port-based VLANs, no Layer 3 address recognition takes place. All traffic within the VLAN is switched, and traffic between VLANs is routed (by an external router or by a router within the switch). This type of VLAN is also known as a segment-based VLAN (see Figure 7.2-3, Port-Based VLANs).

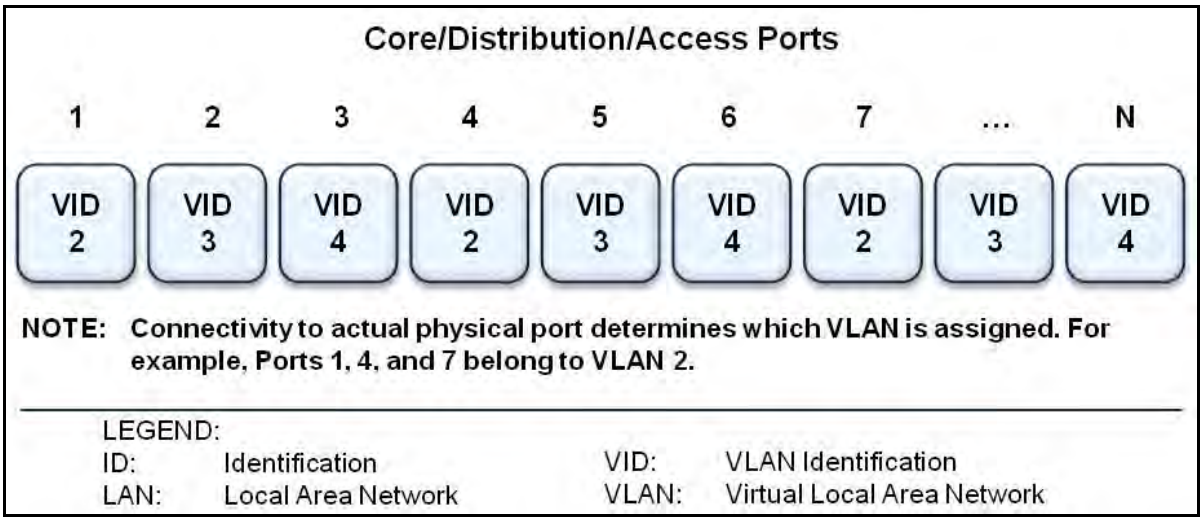


Figure 7.2-3. Port-Based VLANs

- IEEE 802.1Q. VLANs can be assigned by end products IAW the IEEE 802.1Q VLAN ID tag.

EDG-000120 [**Required: Core, Distribution, and Access Products**] The Unified Capabilities (UC) products must be capable of accepting VLAN tagged frames and assigning them to the VLAN identified in the 802.1Q VID field (see Figure 7.2-4, IEEE 802.1Q-Based VLANs).

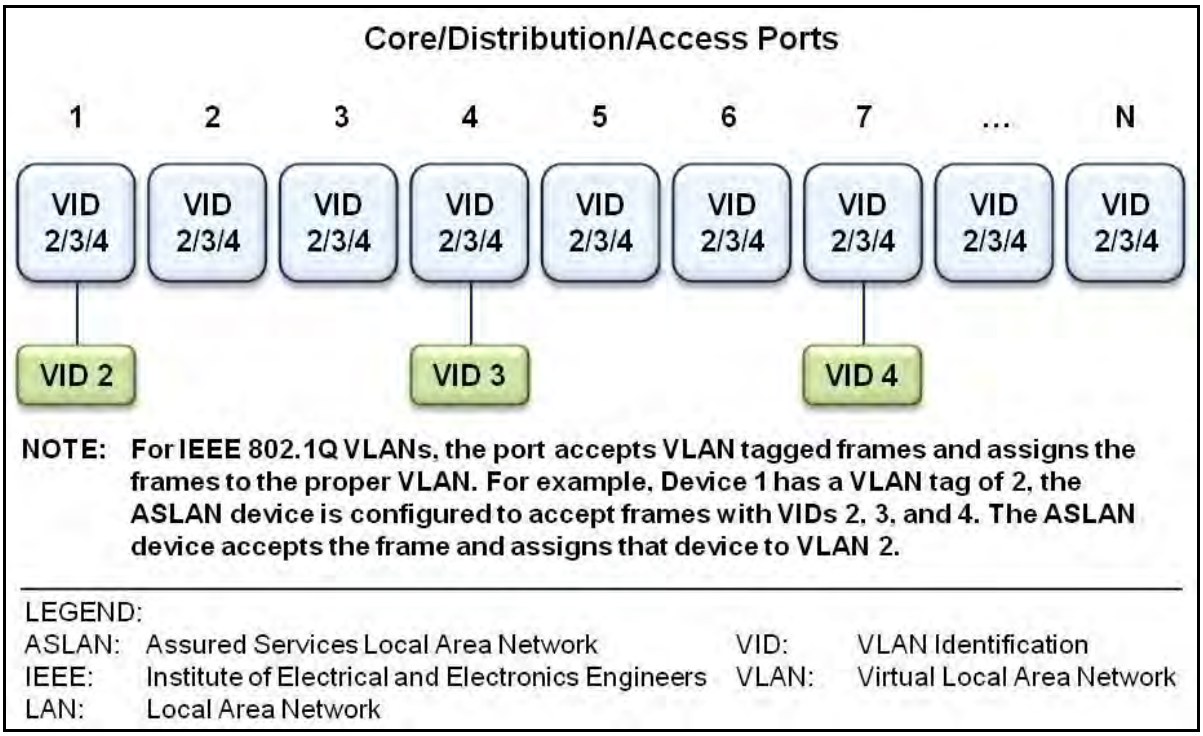


Figure 7.2-4. IEEE 802.1Q-Based VLANs

- User-Defined Value. This type of VLAN is typically the most flexible, allowing VLANs to be defined based on the value of any field in a packet or frame. For example, VLANs could be defined on a protocol basis or could be dependent on a particular address (Layer 2 or Layer 3). The simplest form of this type of VLAN is to group users according to their Media Access Control (MAC) addresses (see Figure 7.2-5, User-Defined VLANs). The LAN shall be designed so that Real-Time Services (RTS) and data reside in separate VLANs. Whether a product is performing converged services or a single service will decide how VLANs are designed.

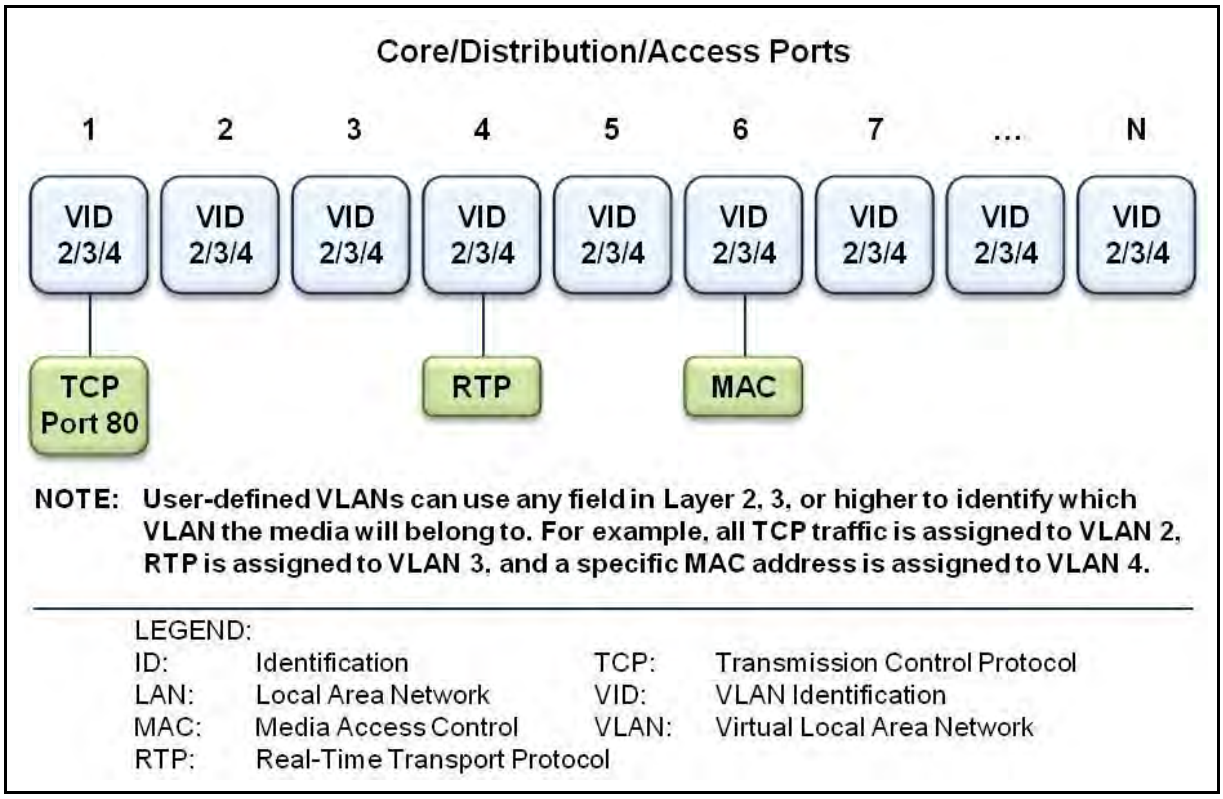


Figure 7.2-5. User-Defined VLANs

The required VLAN types are port-based and IEEE 802.1Q tagged frames. For VoIP, video, and data end products, any end system that supports convergence (i.e., more than one media) requires that the end-system pre-assign the VLAN using IEEE 802.1Q tags before the frames entering the ASLAN. For end-systems that support just one media (i.e., voice or video or data), the LAN can assign the VLAN based on port-based VLAN assignment.

Real-time services and data must be placed in separate VLANs for security purpose. The LAN may be designed with more than one VLAN per media type. Signaling for voice and video can be placed in the same VLAN as the respective media, or placed in an entirely different signaling VLAN.

7.2.1.5 Protocols

EDG-000130 [**Required: Core, Distribution, and Access Products**] The Core, Distribution, and Access products shall meet protocol requirements for IPv4 and IPv6. RFC requirements are listed in Table 7.2-2, ASLAN Infrastructure RFC Requirements. Additional IPv6 requirements by product profile are listed in Section 5, IPv6. These RFCs are not meant to conflict with Department of Defense (DoD) Information Assurance (IA) policy (e.g., Security Technical Implementation Guidelines [STIGs]). Whenever a conflict occurs, DoD IA policy takes precedence. If there are conflicts with Section 5, RFCs applicable to IPv6 in Section 5 take precedence.

Table 7.2-2. ASLAN Infrastructure RFC Requirements

TITLE	RFC	C	D	A	WIRELESS
Open System Interconnect (OSI) Intermediate System to Intermediate System (IS-IS) for routing in Transmission Control Protocol (TCP)/IP and dual environments	RFC 1195	C	C	C	NA
Internet Control Message Protocol (ICMP) Router Discovery messages	RFC 1256	R	R	R	R
Network Time Protocol (NTP) (v3)	RFC 1305	R	R	R	R
Point-to-Point Protocol (PPP) Internet Protocol Control Protocol (IPCP)	RFC 1332	C	C	C	C
Management Information Base (MIB) (Definitions of Managed Objects)	RFC 1471	C	C	C	C
Definitions of Managed Objects for the Security Protocols	RFC 1472	C	C	C	C
(Definitions of Managed Objects for the IP Network Control Protocol)	RFC 1473	C	C	C	C
CIDR MIB (Classless Inter-Domain Routing)	RFC 1519	R	R	C	C
PPP Extensions	RFC 1570	C	C	C	C
MIB (Definitions for 4th version of BGP-4)	RFC 1657	R	C	C	C
Border Gateway Protocol (BGP 4)	RFC 1772	R	C	C	C
Requirements for IP version 4 Routers	RFC 1812	R	R	R	R
PPP Link Quality	RFC 1989	C	C	C	C
PPP Multi-Link	RFC 1990	C	C	C	C
PPP Handshake	RFC 1994	C	C	C	C
BGP Communities	RFC 1997	R	C	C	C
MIBs (IP mobility)	RFC 2006	C	C	C	C
International Organization for Standardization (ISO) Transport	RFC 2126	C	C	C	C
Dynamic Host Configuration Protocol (DHCP)	RFC 2131	C	C	C	C
DHCP Options and BOOTP Vendor Extensions	RFC 2132	C	C	C	C
Resource Reservation Protocol (RSVP) – Version1 Functional Specificaton	RFC 2205	C	C	C	C
RSVP extensions	RFC 2207	C	C	C	C
RSVP with IntServ	RFC 2210	C	C	C	C
General Characterization Parameters for Integrated Service Network Elements	RFC 2215	C	C	C	C
Open Shortest Path First version 2 (OSPFv2)	RFC 2328	R	R	C	C
NBMA Next Hop Resolution Protocol (NHRP)	RFC 2332	C	C	C	C
BGP Protection	RFC 2385	R	C	C	C
BGP Route Flap Damping	RFC 2439	R	C	C	C
Definition of the DS Field in the IPv4 and IPv6 Headers	RFC 2474	R	R	R	R

TITLE	RFC	C	D	A	WIRELESS
IP Header Compression	RFC 2507	C	C	C	C
Compressing IP/UDP/RTP	RFC 2508	C	C	C	C
TCP Congestion Control	RFC 2581	R	R	R	R
AF Per-Hop Behavior (PHB) Group	RFC 2597	R	R	R	R
Entity MIB (Version 2)	RFC 2737	R	R	R	R
OSPF for IPv6	RFC 2740	R	R	C	C
MIB (Network Services)	RFC 2788	C	C	C	C
BGP-4 Route Reflection	RFC 2796	R	C	C	C
MIB (Interfaces Group)	RFC 2863	R	R	R	R
Route Refresh Capability for BGP-4	RFC 2918	R	C	C	C
Policy Core Information	RFC 3060	C	C	C	C
PHB ID Codes	RFC 3140	C	C	C	C
ECN	RFC 3168	C	C	C	C
IP Payload Compression	RFC 3173	C	C	C	C
Expedited PHB	RFC 3246	R	R	R	R
Remote Network Monitoring Management Information Base for High Capacity Network	RFC 3273	C	C	C	C
Mobility for IPv4	RFC 3344	C	C	C	C
IGMPv3	RFC 3376	R	R	C	C
Capabilities Advertisement With BGP-4	RFC 3392	R	C	C	C
Architecture for SNMP Management Frameworks	RFC 3411	R	R	R	R
Message Processing and Dispatching for the Simple Network Management Protocol (SNMP)	RFC 3412	R	R	R	R
SNMP Applications	RFC 3413	R	R	R	R
User-based Security Model (USM) for Version 3 of the Simple Network Management Protocol (SNMPv3)	RFC 3414	R	R	R	R
View-based Access Control Model	RFC 3415	R	R	R	R
V2 of SNMP Protocol Operations	RFC 3416	R	R	R	R
Transport Mappings for the Simple Network Management Protocol (SNMP)	RFC 3417	R	R	R	R
IP Header Compression over PPP	RFC 3544	C	C	C	C
OSPFv2 Graceful Restart	RFC 3623	R^2	R^2	C	C
BGP-4	RFC 4271	R	C	C	C
BGP-4 Extended Communities Attribute	RFC 4360	R	C	C	C
Robust Header Compression	RFC 4362	C	C	C	R

TITLE	RFC	C	D	A	WIRELESS
Remote Monitoring Management Information Base Version 2	RFC 4502	R	R	R	R
Authentication/Confidentiality for OSPFv3	RFC 4552	R	R	C	NA
PIM-SM	RFC 4601	R	R	C	NA
Graceful Restart for BGP	RFC 4724	R[2]	R[2]	C	C
MIB (OSPF V2)	RFC 4750	R	R	C	NA
OSPFv3 Graceful Restart	RFC 5187	R[2]	R[2]	C	C
RFC 5556 "Transparent Interconnection of Lots of Links (TRILL): Problem and Applicability Statement"	RFC 5556	C	C	C	C
NOTE 1: If there are any conflicts between the RFC and the implementation of DoD PKI requirements, then DoD PKI requirements take higher priority. NOTE 2: The 18-month rule applies.					

7.2.1.6 Quality of Service Features

EDG-000140 [**Required: Core, Distribution, and Access Products**] The Core, Distribution, and Access products shall be capable of the following QoS features:

a. Providing a minimum of four queues (see Figure 7.2-6, Four-Queue Design).

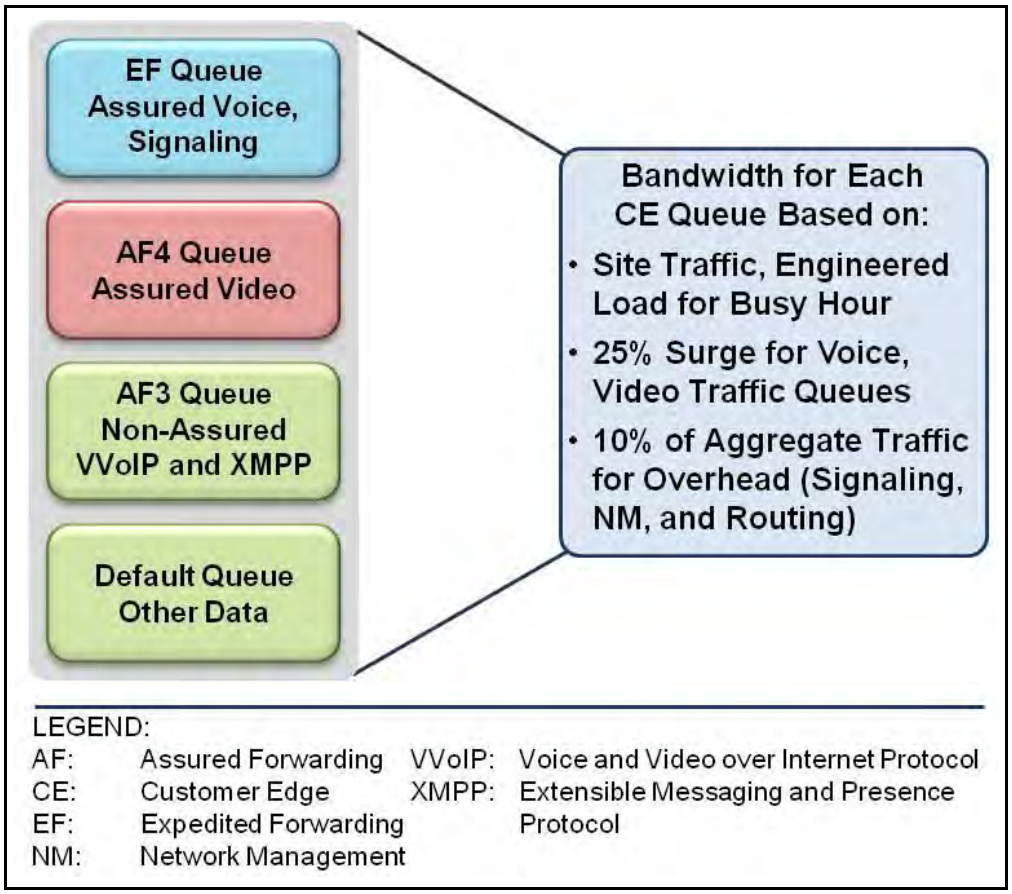


Figure 7.2-6. Four-Queue Design

b. Assigning any incoming access/user-side "tagged" session to any of the queues for prioritization onto the egress (trunk-side/network-side) interface.

c. Supporting Differentiated Services (DS), Per-Hop Behaviors (PHBs), and traffic conditioning IAW RFCs 2474, 2597, and 3246:

   (1) Expedited Forwarding (EF).

   (2) Assured Forwarding (AF).

   (3) Best Effort (BE).

   (4) Class Selector (CS).

   (5) PHB Identification Codes.

d. All queues shall be capable of having a bandwidth (BW) assigned (i.e., queue 1: 200 Kbps, queue 2: 500 kbps) or percentage of traffic (queue 1: 25 percent, queue 2: 25 percent). The BW or traffic percentage shall be fully configurable per queue from 0 to full BW or 0 to 100 percent. The sum of configured queues shall not exceed full BW or 100 percent of traffic.

e. Core, Distribution, and Access products shall meet the traffic conditioning (policing) requirements of Section 6.2.4 as follows:

(1) The product shall calculate the bandwidth associated with traffic conditioning, which requires that the queue size should account for the Layer 3 header (i.e., IP header), but not the Layer 2 headers (i.e., Point-to-Point Protocol [PPP], MAC, and so on) within a margin of error of 10 percent. When the other queues are not saturated, the Best Effort traffic may surge beyond its traffic-engineered limit.

EDG-000150 [**Optional**] Provide a minimum of six queues (see Six-Queue Design).

a. Assigning any incoming access/user-side "tagged" session to any of the queues for prioritization onto the egress (trunk-side/network-side) interface.

b. Supporting DS, PHBs, and traffic conditioning IAW RFCs 2474, 2597, and 3246:

(1) Expedited Forwarding (EF).

(2) Assured Forwarding (AF).

(3) Best Effort (BE).

(4) Class Selector (CS).

(5) PHB Identification Codes.

c. All queues shall be capable of having a bandwidth (BW) assigned (i.e., queue 1: 200 Kbps, queue 2: 500 kbps) or percentage of traffic (queue 1: 25 percent, queue 2: 25 percent). The BW or traffic percentage shall be fully configurable per queue from 0 to full BW or 0 to 100 percent. The sum of configured queues shall not exceed full BW or 100 percent of traffic.

d. Core, Distribution, and Access products shall meet the traffic conditioning (policing) requirements of Section 6.2.4 as follows:

(1) The product shall calculate the bandwidth associated with traffic conditioning in accordance with RFC 3246, which requires that the queue size should account for the Layer 3 header (i.e., IP header), but not the Layer 2 headers (i.e., PPP, MAC, etc.) within a margin of error of plus or minus 10 percent. When the other queues are not saturated, the Best Effort traffic may surge beyond its traffic-engineered limit.

(2) Core and Distribution products have been engineered for a blocking factor not to exceed 2:1. The aggregation of the Assured Forwarding and Expedition Forwarding queues should be configured to guarantee prioritization correctly, given the blocking factor. Priority queues (EF, AF4, and AF3) shall be configured as not to exceed 50 percent of the egress link capacity.

(3) Access devices have been engineered for a blocking factor of 8:1 or less. Traffic prioritization is accomplished primarily to minimize latency. VoIP traffic is estimated at 2 (for dual appearances) bidirectional calls at 100 Kbps each or 400 Kbps

(0 percent of 100 Mbps); video traffic is estimated at 500 Kbps bidirectional or 1 Mbps total (1.0 percent). With estimated blocking factor (8:1), 12.5 percent of the traffic is non-blocking. Based on traffic engineering outlined, the three priority queues should be set up not to exceed 12 percent of the egress link capacity.

NOTE: Bandwidth calculation assumes highest bandwidth use codec of G.711.

EDG-000160 [**Required**] The product shall support the Differentiated Services Code Point (DSCP) plan, as shown in Table 7.2-3, DSCP Assignments. DS assignments shall be software configurable for the full range of six bit values (0-63 Base10) for backwards compatibility with IP precedence environments that may be configured to use the Type of Service (TOS) field in the IP header but do not support DSCP.

Table 7.2-3. DSCP Assignments

AGGREGATED SERVICE CLASS	GRANULAR SERVICE CLASS	PRIORITY/ PRECEDENCE	DSCP BASE10	DSCP BINARY	DSCP BASE8
Network Control	Network Signaling (OSPF, BGP, etc.)	N/A	48	110 000	60
Inelastic Real-Time	User Signaling (AS-SIP, H.323, etc.)	N/A	40	101 000	50
	Short Message	FO	32	100 000	40
	Assured Voice (Includes SRTCP)	FO	41	101 001	51
		F	43	101 011	53
		I	45	101 101	55
		P	47	101 111	57
		R	49	110 001	61
	Non-Assured Voice*	N/A	46	101 110	56
	Assured Multimedia Conferencing (voice, video, and data) (code points 34, 36, and 38 are for Non-Assured Multimedia Conferencing)	FO	33	100 001	41
		F	35	100 011	43
		I	37	100 101	45
		P	39	100 111	47
		R	51 [34,36,38]**	110 011	63
	Broadcast Video	N/A	24	011 000	30
Preferred Elastic	Multimedia Streaming	FO	25	011 001	31
		F	27	011 011	33
		I	29	011 101	35
		P	31	011 111	37
		R	26 [28,30]**	011 010	32

AGGREGATED SERVICE CLASS	GRANULAR SERVICE CLASS	PRIORITY/ PRECEDENCE	DSCP BASE10	DSCP BINARY	DSCP BASE8
	Low-Latency Data: (IM, Chat, Presence)	FO	17	010 001	21
		F	19	010 011	23
		I	21	010 101	25
		P	23	010 111	27
		R	18 [20,22]**	010 010	22
	High Throughput Data	FO	9	001 001	11
		F	11	001 011	13
		I	13	001 101	15
		P	15	001 111	17
		R	10 [12,14]**	001 010	12
	OA&M	N/A	16	010 000	20
Elastic	Best Effort	N/A	0	000 000	00
	Low Priority Data	N/A	8	001 000	10

LEGEND:

AS-SIP: Assured Services Session Initiation Protocol	N/A: Not Applicable
BGP: Border Gateway Protocol	OA&M: Operations, Administration, and Maintenance
DSCP: Differentiated Services Code Point	OSPF: Open Shortest Path First
F: FLASH	P: PRIORITY
FO: FLASH OVERRIDE	R: ROUTINE
I: INTERMEDIATE	SRTCP: Secure Real-Time Transport Control Protocol
IM: Instant Messaging	

* For a definition, see UC Framework 2013, Appendix C, Definitions, Abbreviations and Acronyms, and References.
** Code points in brackets are reserved for nonconformance marking.

7.2.1.7 Network Monitoring

EDG-000170 [**Required: Core, Distribution, and Access Products**] The Core, Distribution, and Access products shall support the following network monitoring features:

a. Simple Network Management Protocol Version 3 (SNMPv3) IAW RFCs 3411, 3412, 3413, 3414, 3415, 3416, and 3417.

b. Remote Monitoring (RMON) IAW RFC 2819. The product shall minimally support the following FRC 2819 groups: Ethernet statistics, history control, eithernet history, and alarm.

c. Coexistence between Version 1, Version 2, and Version 3 of the Internet-standard Network Management Framework IAW RFC 3584.

d. The Advanced Encryption Standard (AES) Cipher Algorithm in the SNMP User-based Security Model IAW RFC 3826.

7.2.1.8 Security

EDG-000180 [**Required: Core, Distribution, and Access Products**] The Core, Distribution, and Access products shall meet the security protocol requirements listed in Section 4, Information Assurance, as follows: Core and Distribution products shall meet all requirements annotated as Router (R) and LAN Switch (LS). Access switches shall meet the IA requirements annotated for LS. In addition to wireless IA requirements previously specified, Wireless Local Area Network Access Systems (WLASs) and Wireless Access Bridges (WABs) shall meet all IA requirements for LSs. Wireless End Instruments (WEIs) shall meet all IA requirements annotated for End Instruments (EIs). When conflicts exist between the Unified Capabilities Requirements (UCR) and STIG requirements, the STIG requirements will take precedence.

7.2.2 LAN Switch and Router Redundancy

The following paragraphs outline the redundancy requirements for the LAN products.

EDG-000190 [**Required: Core, Distribution, and Access Products**] The ASLAN (High and Medium) shall have no single point of failure that can cause an outage of more than 96 IP telephony subscribers. A single point of failure up to and including 96 subscribers is acceptable; however, to support mission-critical needs, FLASH/FLASH OVERRIDE (F/FO) subscribers should be engineered for maximum availability. To meet the availability requirements, all switching/routing platforms that offer service to more than 96 telephony subscribers shall provide redundancy in either of two ways:

a. The product itself (Core, Distribution, or Access) provides redundancy internally.

b. A secondary product is added to the ASLAN to provide redundancy to the primary product (redundant connectivity required).

7.2.2.1 Single Product Redundancy

EDG-000200 [**Optional: Core, Distribution, and Access Products**] If a single product is used to meet the redundancy requirements, then the following requirements are applicable to the product:

a. Dual Power Supplies. The platform shall provide a minimum of two power supplies, each with the power capacity to support the entire chassis. Loss of a single power supply shall not cause any loss of ongoing functions within the chassis.

b. Dual Processors (Control Supervisors). The chassis shall support dual-control processors. Failure of any one processor shall not cause loss of any ongoing functions within the chassis (e.g., no loss of active calls). Failure of the primary processor to secondary must meet 5-second failover without loss of active calls.

c. Termination Sparing. The chassis shall support a (N + 1) sparing capability for available 10/100 Base-T modules used to terminate to an IP subscriber.

d. Redundancy Protocol. Routing equipment shall support a protocol that allows for dynamic rerouting of IP packets so that no single point of failure exists in the ASLAN that could cause an outage to more than 96 IP subscribers. Redundancy protocols will be standards based as specified in this document.

e. No Single Failure Point. No single point shall exist in the LAN that would cause loss of voice service to more than 96 IP telephony instruments.

f. Switch Fabric or Backplane Redundancy. Switching platforms within the ASLAN shall support a redundant (1 + 1) switching fabric or backplane. The second fabric's backplane shall be in active standby so that failure of the first shall not cause loss of ongoing events within the switch.

NOTE: In the event of a component failure in the network, all calls that are active shall not be disrupted (loss of existing connection requiring redialing) and the path through the network shall be restored within 5 seconds.

7.2.2.2 Dual Product Redundancy

EDG-000210 [**Optional: Core, Distribution, and Access Products**] If the System Under Test (SUT) provides redundancy through dual products, then the following requirements are applicable:

a. The failover over to the secondary product must not result in any lost calls. The secondary product may be in "standby mode" or "active mode," regardless of the mode of operation the traffic engineering of the links between primary and secondary must meet the requirements provided in Section 7.5.19, Traffic Engineering.

NOTE: In the event of a primary product failure, all calls that are active shall not be disrupted (loss of existing connection requiring redialing) and the failover to the secondary product must be restored within 5 seconds.

7.2.3 LAN Product Requirements Summary

Table 7.2-4, Core, Distribution, and Access Product Requirements Summary, summarizes product requirements.

Table 7.2-4. Core, Distribution, and Access Product Requirements Summary

REQUIREMENTS	FEATURES	REFERENCES	APPLICABILITY		
			C	D	A
Physical Ports	Serial Port	EIA/TIA	C	C	C
	10Base-TX	IEEE 802.3i	C	C	R1
	10Base-FX	IEEE802.3j	C	C	R1
	100Base-TX	IEEE 802.3u	R1	R1	R1
	100Base-FX	IEEE 802.3u	R1	R1	R1
	1000Base-TX	IEEE 802.3ab	C	C	R1
	1000Base-X	IEEE 802.3z	R	R	R1
	10GBase-X	IEEE 802.3ae, 802.3ak, 802.3an, 802.3aq, 802.3av	C	C	C
	40GBase-X	IEEE 802.3ba	C	C	C
	100GBase-X	IEEE 802.3ba	C	C	C
Port Parameters	Auto-negotiation	IEEE 802.3	R	R	R
	Force Mode	IEEE 802.3	R	R	R
	Flow Control	IEEE 802.3x	C	R	R
	Filtering	RFC 1812	R	R	R
	Link Aggregation	IEEE 802.3AX	R	R	C
	Rapid Spanning Tree Protocol	IEEE 802.1D	C	R	R
	Multiple Spanning Tree Protocol	IEEE 802.1Q	C	R	R
	Rapid Reconfiguration of Spanning Tree	IEE 802.1w	C	R	R
	Port Based Access Control	IEEE 802.1x 2	C	R	R
Traffic Prioritization	CoS Traffic Classes (PCP Field)	IEEE 802.1Q	C	C	C
	DSCP	RFC 2474	R	R	R
VLANs	Port Based	IEEE 802.1Q	R	R	R
IPv4 Protocols	IPv4 features	Section 7.2.1.5, Protocols	R	R	R
IPv6 Protocols	IPv6 features	Section 5	R	R	R
QoS	DS PHBs	RFCs 3246, 2597	R	R	R
	Minimum 4 queues	QoS GTP	R	R	R
	Minimum 6 queues	UCR	C	C	C
Security	Security requirements are contained in the IA portion of the document		R	R	R

NOTE 1. Product need only provide one of the specified interfaces.
NOTE 2. Only between end-user and product, not trunks.

REQUIREMENTS	FEATURES	REFERENCES	APPLICABILITY		
			C	D	A
NOTE 3. One of these queuing mechanisms is required to implement EF PHB. NOTE 4. This requirement is not required for 18 months. (18 month rule applies)					
LEGEND					
C: Optional	EIA: Electronics Industries Alliance	PQ: Priority Queuing			
CB-WFQ: Class-Based Weighted Fair Queuing	FIFO: First-in First-out	R: Required			
CoS: Class of Service	IEEE: Institute of Electrical and Electronic Engineers	RFC: Request for Comment			
CQ: Custom Queuing	IPv4: IP Version 4	TIA: Telecommunications Industry Association			
DISR: DoD Information Technology Standards Registry	IPv6: IP Version 6	VLAN: Virtual LAN			
DS: Differentiated Services	MAC: Media Access Control	WFQ: Weighted Fair Queuing			
EF: Expedited Forwarding	PHB: Per Hop Behavior				

7.2.4 Multiprotocol Label Switching in ASLANs

The implementation of ASLANs sometimes may cover a large geographical area. For large ASLANs, a data transport technique referred to as Multiprotocol Label Switching (MPLS) may be used to improve the performance of the ASLAN core layer. The following paragraphs define the requirements for MPLS when used within the ASLAN.

7.2.4.1 MPLS

7.2.4.2 MPLS ASLAN

EDG-000220 [**Optional: Core and Distribution Products**] An ASLAN product that implements MPLS must still meet all the ASLAN requirements for jitter, latency, and packet loss. The addition of the MPLS protocol must not add to the overall measured performance characteristics with the following caveats:

a. The MPLS device shall reroute data traffic to a secondary pre-signaled Label Switched Path (LSP) in less than 5 seconds upon indication of the primary LSP failure.

EDG-000230 [**Optional: Core and Distribution Products**] Assured Services LAN Core and Distribution products are not required to support MPLS. Services and Agencies may choose to implement MPLS in the ASLAN to take advantage of the inherent technological advantages of MPLS. The ASLAN Core and Distribution products that will be used to provide MPLS services must support the RFCs contained in Table 7.2-5, ASLAN Product MPLS Requirements. RFCs are listed as being REQUIRED (R), OPTIONAL (O), or CONDITIONAL (C). Optionally required RFCs are based on implementation of a particular feature, such as Virtual Private Networks (VPNs).

Table 7.2-5. ASLAN Product MPLS Requirements

REQUIREMENT	REQUIRED/ CONDITIONAL	FEATURE SUPPORTED	REMARKS
RFC 5462, "Multiprotocol Label Switching (MPLS) Label Stack Entry: "EXP" Field Renamed to "Traffic Class" Field"	C	MPLS	
RFC 5420, "Encoding of Attributes for MPLS LSP Establishment Using Resource Reservation Protocol Traffic Engineering (RSVP-TE)"	C	RSVP-TE/ MPLS	Required if RSVP-TE implemented
RFC 5332, "MPLS Multicast Encapsulations"	O	MPLS	
RFC 5331, "MPLS Upstream Label Assignment and Context-Specific Label Space"	O	MPLS	
RFC 5151, "Inter-Domain MPLS and GMPLS Traffic Engineering – Resource Reservation Protocol-Traffic Engineering (RSVP-TE) Extensions"	C	RSVP-TE/ MPLS	Required if RSVP-TE implemented
RFC 5129, "Explicit Congestion Marking in MPLS"	O	MPLS	
RFC 5063, "Extensions to GMPLS Resource Reservation Protocol (RSVP) Graceful Restart"	C	GMPLS	Required if GMPLS RSVP implemented
RFC 5036, "LDP Specification"	C	MPLS, VPLS	Required if LDP implemented
RFC 4974, "Generalized MPLS (GMPLS) RSVP-TE Signaling Extensions in Support of Calls	C	RSVP-TE/ GMPLS	Required if GMPLS RSVP-TE implemented
RFC 4874, "Exclude Routes – Extension to Resource Reservation Protocol-Traffic Engineering (RSVP-TE)	C	RSVP-TE/ MPLS	Required if RSVP-TE implemented
RFC 4873, "GMPLS Segment Recovery"	C	GMPLS	Required if GMPLS implemented
RFC 4872, "RSVP-TE Extensions in Support of End-to-End (E2E) Generalized Multi-Protocol Label Switching (GMPLS) Recovery	C	RSVP-TE/ GMPLS	Required if RSVP-TE implemented
RFC 4783, "GMPLS – Communication of Alarm Information"	C	GMPLS	Required if GMPLS implemented
RFC 4762, "Virtual Private LAN Service (VPLS) Using Label Distribution Protocol (LDP) Signaling"	R	VPLS	
RFC 4761, "Virtual Private LAN Service (VPLS) Using BGP for Auto-Discovery and Signaling" (Updated by RFC 5462)	O	VPLS	Required if L2VPN implemented via BGP
RFC 4684, "Constrained Route Distribution for Border Gateway Protocol/Multiprotocol Label Switching (BGP/MPLS) Internet Protocol (IP) Virtual Private Networks (VPNs)	C	BGP/MPLS VPNs	Required if L3VPN implemented

REQUIREMENT	REQUIRED/ CONDITIONAL	FEATURE SUPPORTED	REMARKS
RFC 4448, "Encapsulation Methods for Transport of Ethernet over MPLS Networks"	R	VPLS	
RFC 4447, "Pseudowire Setup and Maintenance Using the Label Distribution Protocol (LDP)"	C	VPLS	Required if LDP implemented
RFC 4379, "Detecting Multi-Protocol Label Switched (MPLS) Data Plane Failures"	C	MPLS; BGP/MPLS VPNs	Required if L3VPN implemented
RFC 4364, "BGP/MPLS IP Virtual Private Networks (VPNs)" (replaces RFC 2547)	C	MPLS VPNs	Required if L3VPN implemented
RFC 4328, "Generalized Multi-Protocol Label Switching (GMPLS) Signaling Extensions for G.709 Optical Transport Networks Control"	C	GMPLS	Required if SONET optical interface implemented
RFC 4201, "Link Bundling in MPLS Traffic Engineering (TE)"	R	MPLS	
RFC 4182, "Removing a Restriction on the use of MPLS Explicit NULL"	R	MPLS	
RFC 4090, "Fast Reroute Extensions to RSVP-TE for LSP Tunnels" The device shall be able to locally repair an RSVP-TE LSP by rerouting the LSP traffic around the failure using both the one-to-one backup and the facility backup methods as specified in Internet Engineering Task Force (IETF) RFC 4090.	C	MPLS	Required if RSVP-TE implemented
RFC 4003, "GMPLS Signaling Procedures for Egress Control"	C	GMPLS	Required if GMPLS implemented
RFC 3936, "Procedures for Modifying the Resource Reservation Protocol (RSVP)"	C	MPLS/RSVP	Required if RSVP implemented
RFC 3564, "Requirements for support of Differentiated Services-aware MPLS Traffic Engineering"	O	MPLS	
RFC 3479, "Fault Tolerance for the Label Distribution Protocol (LDP)"	C	MPLS	Required if LDP implemented
RFC 3478, "Graceful Restart Mechanism for Label Distribution Protocol"	C	MPLS	Required if LDP implemented
RFC 3473, "Generalized Multi-Protocol Label Switching (GMPLS) Signaling Resource Reservation Protocol-Traffic Engineering (RSVP-TE) Extensions" (Updated by RFCs 4003, 4201, 4783, 4874, 4873, 4974, 5063, 5151, and 5420)	C	MPLS	Required if RSVP-TE implemented
RFC 3471, "Generalized Multi-Protocol Label Switching (GMPLS) Signaling Functional Description" (Updated by RFCs 4201, 4328, and 4872)	R	MPLS	

REQUIREMENT	REQUIRED/ CONDITIONAL	FEATURE SUPPORTED	REMARKS
RFC 3443, "Time To Live (TTL) Processing in Multi-Protocol Label Switching (MPLS) Networks"	R	MPLS	
RFC 3392, "Capabilities Advertisement with BGP-4"	C	BGP; BGP/MPLS VPNs	Required if BGP implemented
RFC 3270, "Multi-Protocol Label Switching (MPLS) Support of Differentiated Services" (Updated by RFC 5462)	R	MPLS	
RFC 3210, "Applicability Statement for Extensions to RSVP for LSP-Tunnels"	O	MPLS VPNs	
RFC 3209, "RSVP-TE: Extensions to RSVP for LSP Tunnels" (Updated by RFCs 3936, 4874, 5151, and 5420)	C	MPLS VPNs	Required if RSVP-TE implemented
RFC 3140, "Per Hop Behavior Identification Codes"	CR	MPLS	
RFC 3107, "Carrying Label Information in BGP-4"	C	BGP/MPLS VPNs	Required if BGP implemented
RFC 5037, "LDP Applicability"	O	MPLS	
RFC 3032, "MPLS Label Stack Encoding" (Updated by RFCs 3270, 3443, 4182, 5129, 5332, and 5462)	R	MPLS	
RFC 3031, "Multi-Protocol Label Switching Architecture"	R	MPLS	
RFC 2961, "RSVP Refresh Overhead Reduction Extensions"	C	RSVP	Required if RSVP implemented
RFC 2917, "A Core MPLS IP Architecture"	O	MPLS	
RFC 2747, "RSVP Cryptographic Authentication" and RFC 3097, RSVP Cryptographic Authentication (Updated Message Type Value)	C	RSVP	Required if RSVP implemented
RFC 2702, "Requirements for Traffic Engineering Over MPLS"	R	MPLS	
RFC 2685, "Virtual Private Networks Identifier"	R	MPLS	

LEGEND:

ASLAN: Assured Services Local Area Network	L2VPN: Layer 2 Virtual Private Network	RFC: Request for Change
BGP: Border Gateway Protocol	L3VPN: Layer 3 Virtual Private Network	RSVP: Resource Reservation Protocol
C: Conditional	LAN: Local Area Network	RSVP-TE: Resource Reservation Protocol-Traffic Engineering
EXP: Experimental	LDP: Label Distribution Protocol	SONET: Synchronous Optical Network

REQUIREMENT	REQUIRED/ CONDITIONAL	FEATURE SUPPORTED	REMARKS
GMPLS: Generalized Multiprotocol Label Switching	LSP: Label Switched Path	TE: Traffic Engineering	
G.709: ITU-T Recommendation G.709, "Interfaces for the optical transport network (OTN)"	MPLS: Multiprotocol Label Switching	TTL: Time To Live	
	O: Optional	VPLS: Virtual Private LAN Service	
IP: Internet Protocol	R: Required	VPN: Virtual Private Network	
ITU-T: International Telecommunication Union – Telecommunication Standardization Sector			

7.2.4.3 MPLS VPN Augmentation to VLANs

The MPLS supports both Layer 2 and Layer 3 VPNs. A Layer 2 MPLS VPN, also known as L2VPN, is a point-to-point pseudo-wire service. An L2VPN can be used to replace existing physical links. The primary advantage of this MPLS VPN type is that it can replace an existing dedicated facility transparently without reconfiguration, and that it is completely agnostic to upper-layer protocols. A Layer 3 MPLS VPN, also known as L3VPN, combines enhanced routing signaling, MPLS traffic isolation, and router support for Virtual Routing/Forwarding (VRF) to create an IP-based VPN.

7.2.4.3.1 MPLS Layer 2 VPNs

EDG-000240 [**Required: Core and Distribution Products Supporting MPLS**] The ASLAN Core or Distribution products will provide Layer 2 MPLS VPNs by minimally supporting the following:

a. RFC 4762, "Virtual Private LAN Service (VPLS) Using Label Distribution Protocol (LDP) Signaling."

The product may additionally support the following:

b. RFC 4761, "Virtual Private LAN Services (VPLS) Using BGP for Auto-Discovery and Signaling."

These methods are commonly referred to as "VPLS" even though they are distinct and incompatible with one another.

EDG-000250 [**Optional: Core and Distribution Products**] The ASLAN products used to support L2VPNs, RFC 4761, or RFC 4762 may support RFC 5501, "Requirements for Multicast Support in Virtual Private LAN Services."

7.2.4.3.2 MPLS Layer 3 VPNs

EDG-000260 [**Required: Core and Distribution Products Supporting MPLS**] The ASLAN Core or Distribution products will provide Layer 3 MPLS VPNs by supporting RFC 4364, "BGP/MPLS IP Virtual Private Networks (VPNs)."

EDG-000270 [**Required: Core and Distribution Products Supporting MPLS**] The ASLAN products used to support L3VPNs by RFC 4364 shall support the following RFCs:

a. RFC 4382, "MPLS/BGP Layer 3 Virtual Private Network (VPN) Management Information Base."

b. RFC 4577, "OSPF as the Provider/Customer Edge Protocol for BGP/MPLS IP Virtual Private Networks (VPNs)."

c. RFC 4659, "BGP-MPLS IP Virtual Private Network (VPN) Extension for IPv6 VPN."

d. RFC 4684, "Constrained Route Distribution for Border Gateway Protocol/Multiprotocol Label Switching (BGP/MPLS) Internet Protocol (IP) Virtual Private Networks (VPNs)."

7.2.4.3.3 MPLS QoS

EDG-000280 [**Required: Core and Distribution Products Supporting MPLS**] The MPLS device must support QoS in order to provide for assured services. The product must support one of the following QoS mechanisms:

a. DSCP mapping to 3 bit EXP field (E-LSP).

b. Label description of PHB (L-LSP).

7.3 WIRELESS LAN

Wireless LAN implementations are considered as extensions of the physical layer. This section outlines the requirements when using wireless Ethernet technologies in a LAN to provide VoIP service to subscribers. In particular, this section defines four wireless areas that may apply to VoIP subscribers: Wireless End Instruments (WEIs), Wireless LAN Access System (WLAS), Wireless Access Bridges (WABs), and general requirements for wireless LANs (WLANs). For LANs supporting VoIP subscribers, wireless transport may be used only as the following:

- To provide wireless Access Layer functionality via a wireless access point.
- Between two or more LANs as a "bridge" technology.

The components of a wireless network are certified along with an ASLAN, while wireless VoIP devices are certified with the VoIP solution.

The requirements for each of the wireless technologies (i.e., WEIs, WLAS, and WABs) are contained in the following sections.

7.3.1 General Wireless Product

EDG-000290 [**Required: Wireless Products**] The following general wireless requirements must be ASLAN wireless components:

a. If an IP interface is provided in any of the wireless components, then it shall meet the IP requirements detailed in the DoD Profile for IPv6.

b. 802.11 wireless products must be WiFi Alliance Certified and shall be certified at the Enterprise level for WiFi Protected Access 2 (WPA2). The products will also be Wi-Fi multimedia (WMM) certified.

c. For wireless products that provide transport to more than 96 (I/P) telephony users, the wireless products shall provide redundancy, and WLAS and/or associated controller/ switches that provide and/or control voice services to more than 96 WEIs shall provide redundancy through one of the following:

   (1) Single Product Redundancy. Shall have the following as a minimum: Dual power supplies/processors/radio systems/Ethernet ports and no single point of failure for more than 96 subscribers. It should be noted that single point of failure may exist for more than 96 subscribers if 96 or fewer are IP telephone subscribers (i.e., 50 data, 20 video, and 50 IP telephony = 120 subscribers).

   (2) Dual Product Redundancy. Shall be collocated or co-adjacent and shall have the following as a minimum: Traffic engineering to support all users on a single product upon failure of the other product. Secondary product may be on full standby or traffic sharing, supporting 50 percent of the traffic before failure rollover. Products must support a redundancy protocol.

d. All wireless connections shall be Federal Information Processing Standard (FIPS) 140-2 Level 1 certified (connections may either be WEI to WLAS if both support FIPS 140-2 Level 1, or WEI to a FIPS 140-2 compliant product through a WLAS if the WLAS is not capable of FIPS 140-2 Level 1). Wireless products that comprise the WLAN shall be secured in accordance with their wireless security profile as follows:

   (1) FIPS 140-2, Level 1. Wireless components must be operated from within a "limited access, secure room" and be under user positive control at all times. However, if the wireless end item is designed to be left unattended or is designed as an item that can be left behind, such as a wireless free-standing desk telephone, then that wireless end item must be Level 2 compliant.

   (2) FIPS 140-2, Level 2. Wireless components can be operated in an open public area such as an "open hallway," but the use of a "limited access, secure room" if available and/or operationally feasible is recommended.

e. The use of wireless in the LAN as a bridging function shall not increase latency by more than 10 ms for each bridging pair. The use of wireless via an access point shall not increase LAN latency by more than 15 ms (see UCR Framework 2013 on wireless).

f. The wireless products shall support LAN Traffic Prioritization and QoS IAW the following based on the wireless interface type:

(1) 802.11 Interfaces. Wireless products using 802.11 shall use the settable Service Class tagging/QoS parameters within 802.11-2012 to implement mapping to the prescribed DSCP values. The product shall support WMM. Wireless mobile devices shall also support WMM Power Save.

(2) 802.16 Interfaces. Wireless products using 802.16 QoS/Service Class tagging shall meet the following requirements:

(a) The WLAN products may use 802.16 (IAW 802.16-2012) to provide QoS over the wireless portion of the transport.

(b) The WLAS and WABs shall mark traffic traversing into the wired portion of the LAN with appropriate wired DSCPs (see Table 7.3-1, 802.16 Service Scheduling).

Table 7.3-1. 802.16 Service Scheduling

AGGREGATE SERVICE CLASS	GRANULAR SERVICE CLASS	802.16 SERVICE	RADIO SERVICE TRAFFIC PRIORITY	WIRED LANS DEFAULT DSCPS	
				BASE 2	BASE 10
Control	Network Control	N/A	N/A	110 000-110 111	48-56
Inelastic/ Real-Time	User Signaling	UGS	7	101 000-101 111	40-47
	Circuit Emulation	UGS	6		
	Voice	UGS	6		
	Short messages	ertPS	5		
	Video/VTC	ertPS	4	100 000-100 111	32-39
	Streaming	rtPS	3	011 000-011 111	24-31
Preferred Elastic	Interactive Transactions and OA&M	nrtPS	2	010 000-010 111	16-23
	File Transfers and OA&M	nrtPS	1	001 000-001 111	8-15
Elastic	Default	BE	0	000 000-000 111	0-7

LEGEND

BE: Best Effort	NA: Not Applicable	rtPS: Real-Time Polling Service
DSCP: Differentiated Services Code Point	nrtPS: Non Real-Time Polling Service	UGS: Unsolicited Grant Service
ertPS: Extended Real-Time Polling Service	OA&M: Operations, Administration, and Management	VTC: Video Teleconferencing
LAN: Local Area Network	N/A: Not Applicable	

g. Wireless products shall meet the security requirements as stipulated in the Wireless Security Technical Implementation Guide (STIG) and the following specified requirements:

(1) All 802.11 wireless components shall do the following:

(a) Use the AES-Counter with Cipher Block Chaining-Message Authentication Code Protocol (CCMP) (AES-CCMP). It will be implemented in 802.11-2012 system encryption modules.

(b) Implement the Extensible Authentication Protocol – Transport Layer Security (EAP-TLS) mutual authentication for the EAP component of Wi-Fi Protected Access (WPA2).

h. Wireless access systems shall meet the access product requirements in Section 7.2.

EDG-000290.a [**Optional**] Wireless systems may use the Control and Provisioning of Wireless Access Points (CAPWAP) Protocol IAW RFC 5415 and RFC 5416.

7.3.2 Wireless Interface

EDG-000300 [**Required: WEI and WLAS**] If a wireless product is used, the wireless product shall support at least one of the following approved wireless LAN standards interfaces:

a. 802.11a IAW 802.11-2007 – 5 GHz.

b. 802.11b IAW 802.11-2007 – 2.4GHz.

c. 802.11g IAW 802.11-2007 – 2.4 GHz.

d. 802.11n-2009 – 2.4 GHz and 5 GHz.

e. 802.16-2012.

EDG-000310 [**Required: WEI and WLAS**] For any of the 802.11 interfaces, the wireless product must minimally support the following two 802.11 standards:

a. 802.11e – Part 11. Wireless LAN Medium Access Control (MAC) and Physical Layer (PHY) specifications and Amendment 8: Medium Access Control (MAC) Quality of Service Enhancements. See, for priority bit assignment.

b. 802.11i – Part 11. Wireless LAN Medium Access Control (MAC) and Physical Layer (PHY) specifications and Amendment 6: Medium Access Control (MAC) Security Enhancements.

EDG-000320 [**Required: WEI and WLAS**] For the 802.11a interface, the wireless product must support the standard 802.11h – Part 11: Wireless LAN Medium Access Control (MAC) and Physical Layer (PHY) specifications, Amendment 5: Spectrum and Transmit Power Management Extensions in the 5 GHz band in Europe.

EDG-000330 [**Required: WEI and WLAS**] For any of the 802.16-2012 interfaces, the wireless product must support the following 802.16-2012 standards dependent on whether the end item attached to the WLAS is “fixed” or “nomadic.”

Fixed WEIs are those WEIs that access a single WLAS during the session and are not expected to traverse between WLASs so that handoffs are not required. Fixed WEIs must support 802.16-2012 requirements.

Nomadic WEIs are those WEIs that are mobile and may traverse different WLASs during a single session (i.e., handoffs are seamless from the user perspective). Nomadic WEIs must support 802.16-2012.

7.3.3 Wireless End Instruments

EDG-000340 [**Required: WEIs**] The following requirements apply.

a. Wireless VoIP EIs are certified as part of the VoIP solution (i.e., Session Controller [SC]) unless they are wireless Audio End Instruments (Wireless Audio End Instruments shall meet all Audio End Instrument requirements as well as meet the wireless interface requirements listed in this section).

b. Access to/from a WEI shall be provided by either 802.11 or 802.16. Two methods that an IP subscriber can use to access voice services are dedicated wireless service or shared wireless service (see Figure 7.3-1, Access Methods for the Wireless Access Layer End Item Product Telephones). The dedicated access method provides wireless access service for a single type of traffic (i.e., voice, video, or data – three devices are required to support all traffic types). The shared access method allows a single wireless WLAS to provide for all traffic types supported (i.e., voice, video, and data – one device provides all three traffic types), on all computer types and/or Personal Electronic Device (PED) to connect to the wireless WLAS.

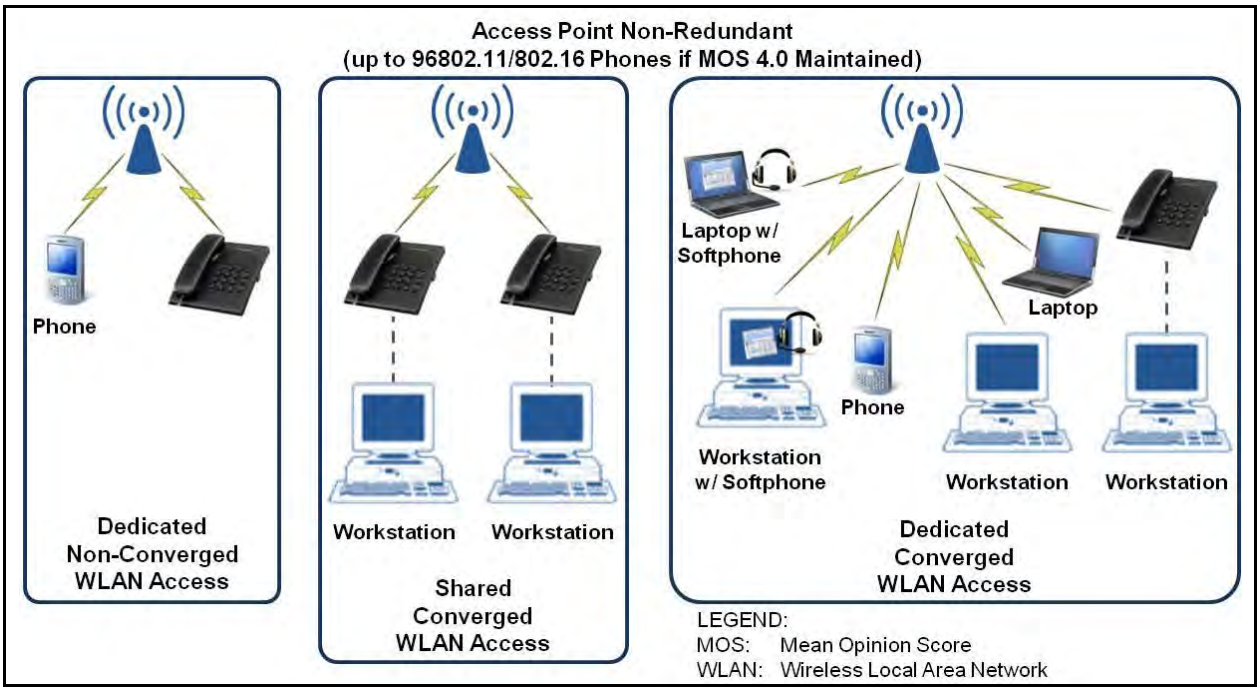


Figure 7.3-1. Access Methods for the Wireless Access Layer End Item Product Telephones

c. WEIs may use either method separately or a combination to provide wireless access (see Figure 7.3-1, Access Methods for the Wireless Access Layer End Item Product Telephones).

d. WEIs or soft clients on workstations acting as WEIs shall authenticate to the VoIP system call control. Authentication shall be IAW UCR IA-specified requirements.

e. The WEI is associated with the supporting IP telephone switch. The WEI shall be functionally identical to a traditional IP wired telephone and will be required to provide voice features and functionality IAW other UCR specified requirements unless explicitly stated.

f. Minimally, all WEIs shall be FIPS 140-2 Level 2 compliant.

g. If the WEI loses connection with the VoIP switch when using a WLAN, the call will be terminated by the VoIP switch. The termination period shall be determined by the VoIP switch using a configurable time-out parameter with a time-out range of 0–60 seconds; default shall be set to 5 seconds. The subscriber line will be treated as if it were out of service until communication is re-established with the wireless voice end instrument.

7.3.4 Wireless LAN Access System

A WLAS implementation is considered to be the replacement of the physical layer of the wired Access Layer of a LAN. A WLAS that is used may range in size from 96 voice IP subscriber services for non-redundant WLAS(s) to more than 96 voice IP subscriber services for a

redundant WLAS(s). Wireless products that support 96 or less voice users are not required to be redundant.

EDG-000350 [**Required: WLAS**] If a WLAS is used as part of the LAN design supporting VoIP subscribers, the following requirements must be met:

a. Failure of a WLAS shall not cause the loss of a call as the connection transfers from the primary to alternate system. However, it may allow a single momentary 5-second delay in voice bearer traffic in both directions of the wireless link as wireless VoIP telephone clients are re-authenticated to the standby system. The 5-second voice delay will not be factored into the overall Mean Opinion Score (MOS).

b. The WLAS shall support the following maximum number of EIs per Table 7.3-2, Maximum Number of EIs Allowed per WLAS, for converged or non-converged access for redundant and non-redundant WLAS; while not degrading any of the individual EIs' voice quality below the specified MOS of 3.8 for strategic, 3.4 for wireless strategic-tactical, and 3.0 for tactical.

Table 7.3-2. Maximum Number of EIs Allowed per WLAS

WLAN CONVERGENCE TYPE	ACCESS TYPE	WLAS REDUNDANCY	L2/L3 SWITCH LINK(S)	L2/L3 CONNECTION LINK ETHERNET SPEED	MAXIMUM # WIRELESS PHONE SUBSCRIBERS
Non-Converged	Non-Sharing	Non-Redundant	Single	10 Mbps	96
		Redundant	Link Pair	10 Mbps	100
				100 Mbps	1,000
				1 Gbps	10,000
				10 Gbps	100,000
Converged	Shared and/or Dedicated	Non-Redundant	Single	100 Mbps	96
		Redundant	Link Pair	100 Mbps	250
				1 Gbps	2,500
				10 Gbps	25,000

NOTE: This table defines the maximum number of telephones allowed. This number greatly exceeds the expected WLAS capability for maintaining appropriate MOS (Strategic 3.8, Strategic-to-Tactical 3.4, and Tactical-to-Tactical 3.0) when all telephones are off-hook simultaneously.

LEGEND:

Gbps: Gigabits per second	MOS: Mean Opinion Score
L2: OSI Layer 2	OSI: Open System Interconnect
L3: OSI Layer 3	WLAN: Wireless Local Area Network
Mbps: Megabits per second	WLAS: Wireless LAN Access System

c. At the point when voice quality degradation occurs, defined as a MOS score below appropriate levels (i.e., Strategic 4.0, Strategic-to-Tactical 3.6, and Tactical-to-Tactical 3.2), when all telephones are off-hook simultaneously, this becomes the maximum number of telephones and/or other wireless non-voice end item products that the WLAS can support for the WLAS transmitter coverage distance.

d. The WLAS shall not drop an active call as the WEI roams from one WLAS transmitter zone into another WLAS transmitter zone. The source and destination WLAS transmitters involved in the roaming are connected to the same WLAS controller or are otherwise part of the same WLAS.

e. The addition of the WLAS shall not cause the one-way delay measured from ingress to egress to increase by more than 3 ms, averaged over any 5-minute period.

f. The addition of WLAS shall not increase the LAN jitter requirements previously specified in this section by more than an additional 3 ms.

g. Minimally, WLAS products shall provide one of the following trunk-side interface (ASLAN network side) rates (other rates and IEEE standards may be provided as optional interfaces):

- 10 Mbps IAW IEEE 802.3i.
- 10 Mbps IAW IEEE 802.3j.
- 100 Mbps IAW IEEE 802.3u.
- 1000 Mbps IAW IEEE 802.3z.
- 1000 Mbps IAW IEEE 802.3ab.

7.3.5 Wireless Access Bridge

Wireless access bridges can be used to replace the physical layer of the wired Open System Interconnect (OSI) Layer 2/3 (L2/L3) Access Layer of the ASLAN or non-ASLAN with wireless technology. IEEE 802.11 and/or 802.16 systems can be used to provide a wireless communications link (or bridge) between two or more wired LANs, typically located in adjacent buildings. The WAB functions within the LAN primarily as a wireless NE. The hardware used in a wireless LAN bridge is similar to a WLAS, but instead of connecting only wireless clients to the wired network, bridges are used primarily to connect other wireless LAN bridges to the network. Simultaneously, the WAB may provide connection services to wireless end item products too (i.e., act simultaneously as a WLAS). An example of a combination WLAS/WAB and WAB is provided in Figure 7.3-2, Example of Combined WLAS/WAB and Second Layer WAB (a combination protocol WLAN/WAB [802.11 WLAS with 802.16]).

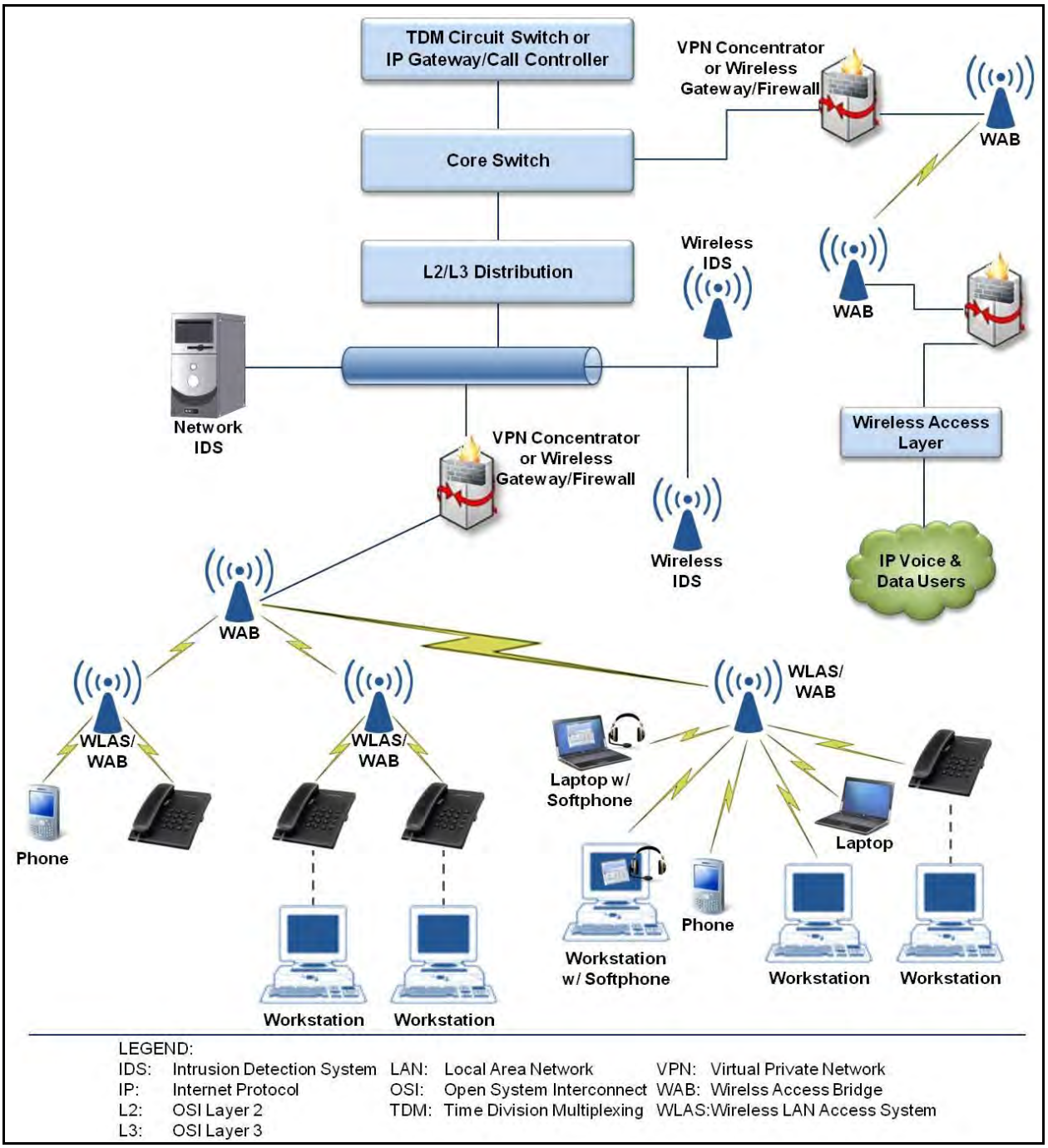


Figure 7.3-2. Example of Combined WLAS/WAB and Second Layer WAB

EDG-000360 [**Required: WAB**] the WAB will be required to meet all the following requirements for each individual type interface.

a. The WAB shall minimally provide one wireless interface that serves as the communication path between WAB components. The WAB shall also provide a wired interface to connect to the ASLAN components. Minimally, WAB products shall provide

one of the following wired trunk-side (ASLAN network side) interface rates (other rates and IEEE standards may be provided as optional interfaces):

- 10 Mbps IAW IEEE 802.3i.
- 10 Mbps IAW IEEE 802.3j.
- 100 Mbps IAW IEEE 802.3u.
- 1000 Mbps IAW IEEE 802.3z.
- 1000 Mbps IAW IEEE 802.3ab.

In addition, the WAB must provide one of the following wireless interfaces:

(1) 802.16 interfaces. If supported, the WAB must support 802.16-2012. The product must support 802.16 QoS specified in Section 7.3.1, General Wireless Product.

(2) 802.11 interfaces, the WAB must meet a minimum of one of 802.11standards (802.11a, b, g, or n). The product must support 802.11 QoS specified in Section 7.3.1.

(3) For the wireless interface, vendors may support a pair-wise proprietary wireless technology. The interface must support a QoS mechanism (e.g., DSCP or 802.1 L2 tag [aka 802.1p]) to support assured services transport of prioritized traffic (if congestion or over subscription is possible). The interface must transport and not modify the existing layer 3 DSCP value.

b. The maximum number of voice calls transported across the WAB shall be in accordance with Section 7.15.19, Traffic Engineering. Maximum voice users will be determined by the smallest link size (i.e., Ethernet connection to the WAB or the WAB wireless link speed of the WAB itself).

c. The introduction of WAB(s) shall not cause the End-to-End (E2E) average MOS to fall below appropriate levels (Strategic 4.0, Strategic-to-Tactical 3.6, and Tactical-to-Tactical 3.2) as measured over any 5-minute time interval.

d. The introduction of WAB(s) shall not increase packet loss by more than 20 percent over the LAN requirement of 0.015 percent.

e. The WAB shall not modify call control signals that are transported through it.

f. The addition of WAB(s) shall not cause the one-way delay measured from ingress to egress to increase by more than 3 ms for each WAB used, averaged over any 5-minute period.

g. The addition of WAB(s) shall not increase the LAN jitter requirements previously specified in this section by more than an additional 3 ms.

A WAB may simultaneously act as a WLAS.

h. A WAB may optionally support mesh networking. If provided, mesh networking must meet the requirements of IEEE 802.11s-2011.

EDG-000370 [**Required: WLAS/WAB**] The WLAS/WAB combination must meet all the requirements for access (WLAS) and bridging (WAB).

a. The WAB(s) and/or WLAS/WAB shall support Service Class tagging/QoS as previously specified in this section.

7.3.6 Survivability

Network survivability refers to the capability of the network to maintain service continuity in the presence of faults within the network. This can be accomplished by recovering quickly from network failures quickly and maintaining the required QoS for existing services.

For the ASLAN, survivability needs to be inherent in the design. The following guidelines are provided for the ASLAN:

- Layer 3 Dynamic Rerouting. The ASLAN products that route (normally the Distribution and Core Layers) shall use routing protocols IAW the DoD Information Technology (IT) Standards Registry (DISR) to provide survivability. The minimum routing protocols that must be supported are as follows:
  - Border Gateway Protocol (BGP) for inter-domain routing (Required: Core products).
  - Open Shortest Path First (OSPF), Version 2, for IPv4 and OSPF Version 3 for IPv6, July 2008, and IAW RFC 5340 (Required: Core and Distribution products).
  - OSPFv2 Graceful restart (RFC 3623) and OSPFv3 Graceful Restart (RFC 5187) are required (18-month rule) for Core and Distribution products. It is not applicable to access devices unless routing (OSPF) provided.
  - Graceful Restart for BGP (RFC 4724) is required (18-month rule) for core and distribution infrastructure products.
- Layer 2 Dynamic Rerouting:
  - Virtual Router Redundancy Protocol (VRRP) – RFCs 2787 and RFC 5798. VRRP is able to provide redundancy to Layer 2 switches that lose connectivity to a Layer 3 router. The Distribution product shall employ VRRP to provide survivability to any product running Layer 2 (normally the Access Layer).

7.4 DIGITAL SUBSCRIBER LINE (DSL)

7.4.1 Introduction

This section includes requirements for using DSL access technologies to link buildings within DoD Bases at UC locations worldwide. This section also describes how newer Ethernet in the First Mile over Copper (EFMCu) access technologies, could be used to link buildings within Bases at these UC locations.

7.4.2 DSL Product

The requirements that follow are specified for the DSL products that implement the DSL operational framework utilized by DISA. The DSL products are categorized into the following types:

- Access Devices.
- Concentrators.
- Repeaters.

7.4.3 Physical Layer

EDG-000380 [**Required: Access Devices, Concentrators, Repeaters**] DSL products shall provide at least one of the following DSL interface types:

a. ADSL ITU G.992.1 (G.DMT).

b. ADSL ITU G.992.2 (G.Lite).

c. ADSL2 ITU G.992.3.

d. ADSL2+ ITU G.992.5.

EDG-000390 [**Optional: Access Devices, Concentrators, Repeaters**] Access Devices, Concentrators, and Repeaters shall provide the following DSL interface types:

a. SHDSL ITU G.991.2.

b. VDSL ITU G.993.1.

c. HDSL ITU G.991.1.

d. VDSL2 ITU G.993.2.

e. Long reach 2BASE-TL IEEE Std 802.3ah.

f. Short reach 10PASS-TS IEEE Std 802.3ah.

EDG-000400 [**Required: Access Devices, Concentrators**] DSL products shall provide at least one of the following Ethernet interface types (other types may be provided as optional interfaces):

a. 10 Mbps IEEE Std 802.3i (10-BaseT Ethernet).

b. 100 Mbps IEEE Std 802.3u (100-BaseT Fast Ethernet).

EDG-000410 [**Optional: Access Devices, Concentrators**] DSL products may also provide at least one of the following Ethernet interface types:

c. 1000 Mbps IEEE Std 802.3z (1000-Base X Gigabit Ethernet over Fiber-Optic).

d. 1000 Mbps IEEE Std 802.3ab (1000-Base T Gigabit Ethernet over Twisted Pair).

7.4.4 Data Link Layer

EDG-000420 [**Optional: Access Devices, Concentrators**] DSL products may meet at least one of the following DSL bonding capabilities:

a. Asynchronous Transfer Mode (ATM)-based multi-pair bonding ITU G.998.1.

b. Ethernet-based multi-pair bonding ITU G.998.2.

c. Multi-pair bonding using time-division inverse multiplexing ITU G.998.3.

d. Multilink Point-to-Point Protocol bonding RFC 1990.

EDG-000430 [**Required: Access Devices, Concentrators**] DSL products shall meet the Ethernet Media Access Control (MAC) capabilities defined in IEEE Std 802.3-2002.

EDG-000440 [**Required: Access Devices, Concentrators**] DSL products shall meet the Ethernet MAC bridging capabilities defined in IEEE Std 802.1D-2004.

EDG-000450 [**Required: Access Devices, Concentrators**] DSL products shall meet the Ethernet Virtual Local Area Network (VLAN) capabilities defined in IEEE Std. 802.1Q.

EDG-000460 [**Optional: Access Devices, Concentrators**] DSL products may meet the Ethernet in the First Mile bonding requirements specified in IEEE Std 802.3ah.

EDG-000470 [**Optional: Access Devices, Concentrators**] DSL products may meet the ATM capabilities defined in International Telecommunications Union (ITU) I.361.

EDG-000480 [**Optional: Access Devices, Concentrators**] DSL products may meet the ATM Adaptation Layer 5 (AAL5) capabilities defined in ITU I.363.5.

7.4.5 Network Layer

EDG-000490 [**Required: Access Devices, Concentrators**] DSL products shall meet all of the IPV4 protocol requirements for UC Access products as listed in Table 7.2-4, Core, Distribution, and Access Product Requirements Summary.

EDG-000500 [**Required: Access Devices**] DSL products shall meet all of the IPV6 protocol requirements for LAN Switch products as listed in Table 5.2-3, UC End Instruments (EI), of Section 5, IPv6.

EDG-000510 [**Required: Concentrators**] DSL products shall meet all of the IPV6 protocol requirements for LAN Switch products as listed in Table 5.2-6, LAN Switch (LS), of Section 5, IPv6.

7.4.6 Information Assurance

EDG-000520 [**Required: Access Devices, Concentrators, Repeaters**] The Information Assurance requirements are contained in Section 4, Information Assurance.

7.4.7 DSL Support for Analog Voice Services

The following Access Device and Concentrator requirements are based on the Base Configuration Supporting Analog Voice and VoIP using DSL Modems and a Digital Subscriber Line Access Multiplexer (DSLAM). These requirements apply to Analog Voice services, and do not apply to VoIP or Video over IP Services.

EDG-000530 [**Conditional: Concentrators**] If the Concentrator (DSLAM) routes analog voice traffic (or analog voice traffic multiplexed onto a T1) to/from a VoIP Media Gateway and UC SC for voice call completion, the Concentrator's interface to the VoIP Media Gateway shall match the Media Gateway interface requirements in Section 2.14, Media Gateway.

When the Concentrator is a DSLAM that supports analog voice traffic, analog phones can also be supported at the DSL Access Devices (the DSL Modems). In this scenario, the analog voice signal is transmitted together with the digital DSL signal over the DSL copper lines.

EDG-000540 [**Conditional: Concentrators**] If the Concentrator (DSLAM) supports analog voice traffic, the side of the DSLAM that terminates the Voice Grade Copper lines shall use a splitter to separate the analog phone traffic from the digital DSL traffic at each of the lines. In this case, the DSLAM shall also route the analog phone traffic to the point of analog voice distribution (the local VoIP Media Gateway, End Office, or Private Branch Exchange [PBX]) and route the digital DSL traffic to the DSL components within the DSLAM. This DSLAM-based splitter shall also act as a filter to prevent interference between the analog phone service and the DSL IP data service (including VoIP and Video over IP services when they are used).

EDG-000550 [**Conditional: Access Devices**] If the Access Device (DSL Modem) supports an analog phone connection, then the Access Device shall contain a low pass filter that is located between the analog phone line (DSL modem user side) and the DSL line (DSL modem network side). This low pass filter shall prevent interference between the analog phone service and the DSL IP data service (including VoIP and Video over IP services when they are used).

7.4.8 Device Management

EDG-000560 [**Required: Access Devices, Concentrators, Repeaters**] DSL products shall meet the device management requirements for Management Options, Fault Management, Loopback Capability, and Operational Configuration Restoral, as specified in Section 7.4.8, Device Management.

EDG-000570 [**Required: Access Devices, Concentrators, Repeaters**] DSL products shall meet the device management requirements that allow network managers to monitor, configure, and control all aspects of the network and observe changes in network status.

EDG-000580 [**Required: Access Devices, Concentrators, Repeaters**] DSL products shall support the following device management functions that secure access to these devices:

a. Password-protected user accounts that are either defined for each individual device, or centrally controlled for multiple devices using a Radius server.

b. Secure Shell (SSH) interfaces that provide encryption, authentication and data integrity.

c. Graphical User Interface (GUI) applications that can be used for local and remote management of all DSL elements served by the management function.

EDG-000590 [**Required: Access Devices, Concentrators, Repeaters**] DSL products shall support the Simple Network Management Protocol (SNMP) Version 3 network management protocol and have the ability to send SNMP traps to up to four defined trap destinations. The DSL products shall allow the SNMP agent parameters and trap destinations to be defined on an individual element basis (per Access Device, Concentrator, and Repeater) and on a group-of-elements basis.

7.5 PASSIVE OPTICAL NETWORK (PON) TECHNOLOGY

This section establishes the requirements for the products used in PON technology within ASLAN, Non-ASLAN, and WAN environments.

7.5.1 Definition of PON

Passive Optical Network (PON) is a technology composed of an Optical Line Terminal (OLT), a varying number of Optical Network Units/Terminals (ONUs/ONTs) with fiber optic cable and splitters connecting them. Interface from the backbone network (Network-to-Network Interface [NNI] or Ingress) is provided by the OLT while the user interface (User Network Interface [UNI] or Egress) is provided by the ONT. Typical PON network connectivity is illustrated in Figure 7.5-1, Typical PON Network Connectivity. A PON is a converged transport schema that is designed to carry multiple services such as VoIP, Data, IP Video, and Radio Frequency (RF) Video. Organizations that plan to deploy PON with ONTs on the desktop should be aware that power to the ONT is not provided via the fiber network. Power would be needed provided via copper (which could be included with fiber in the network cable). Backup power to the desktop could also be provided via other mechanisms.

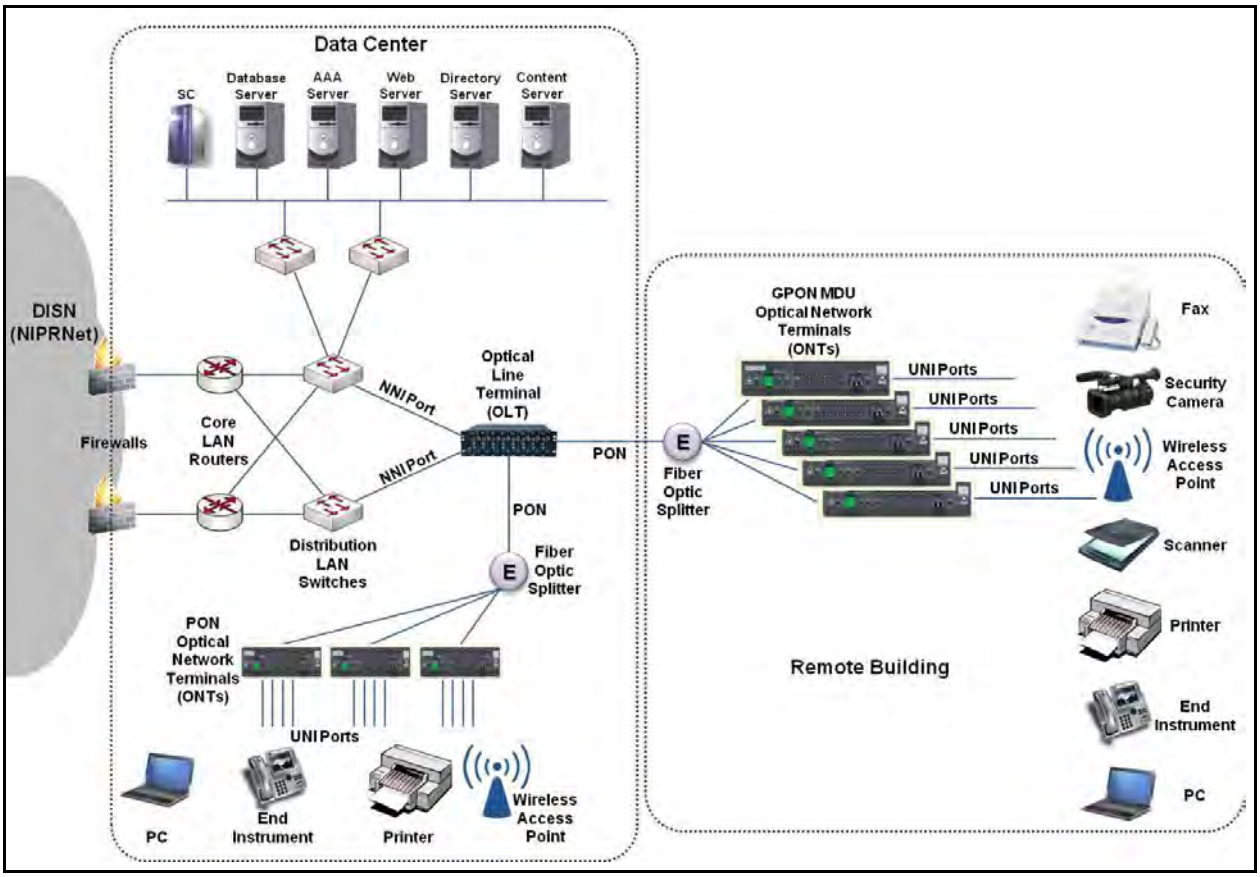


Figure 7.5-1. Typical PON Network Connectivity

The common PON operational framework technologies in use are Ethernet PON (EPON), Broadband PON (BPON) and Gigabit PON (GPON). The first PON technology introduced was BPON. The most current versions are EPON and the newer standard of GPON, which are rapidly replacing the older BPON networks.

BPON conforms to the ITU T G983.1 specification, which includes 622 Mbps download speed with 155 Mbps upload speed per PON port on the OLT. GPON conforms to the ITU T G984 series (G.984.1 through G.984.7) and provides bit rates above 1 Gbps. EPON conforms to the IEEE 802.3ah and 802.3av specifications with options for 1/1 Gbps 10/1 Gbps and 10/10 Gbps.

At a high level, a PON consists of a head-end device called an OLT. The OLT may be deployed at the Distribution (e.g., Main Communication Node or Area Distribution Node), and Access (e.g., End User Building) Layers. End user endpoints are equipped with ONTs that provide Ethernet, 2-wire analog Plain Old Telephone Service (POTS), and even RF video. As many as 64 (and in some cases more) ONTs connect to a PON port via a single, single mode fiber whose optical signals are combined at a passive splitter. A PON utilizes Wavelength Division Multiplexing (WDM), using one wavelength for downstream traffic and another for upstream traffic across one single, single-mode fiber optic cable. The PON specifications provide downstream traffic to be transmitted over a single fiber on the 1490 nanometer (nm) wavelength

and upstream traffic to be transmitted at 1310 nm. A third 1550 nm band is allocated for overlay services, in this case, RF (analog) video.

The following figures display two different connectivity solutions utilizing the GPON network operational framework. Figure 7.5-2, PON Connectivity in the DoD operational framework, shows a typical installation utilizing the OLT in the Distribution (ADN) and Access (EUB) Layers of the DoD UC model. Figure 7.5-3, PON Connectivity in a Collapsed DoD Backbone Operational Framework, shows a collapsed backbone where fibre splitters are the only equipment required at the ADN.

PON systems are typically deployed as a single SUT (i.e., it is not expected that one vendor's OLTs will work with another vendors ONTs).

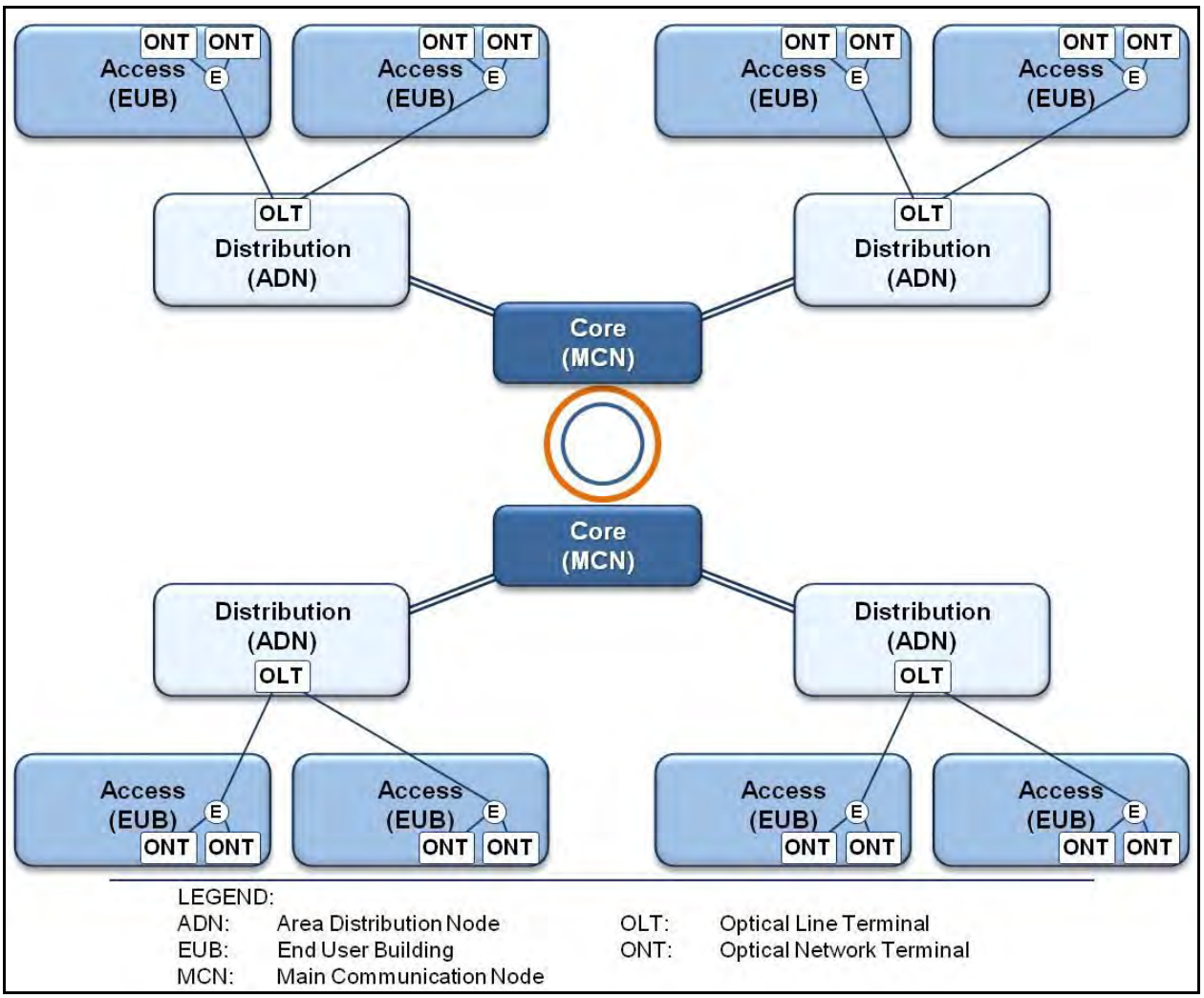


Figure 7.5-2. PON Connectivity in the DoD Operational Framework

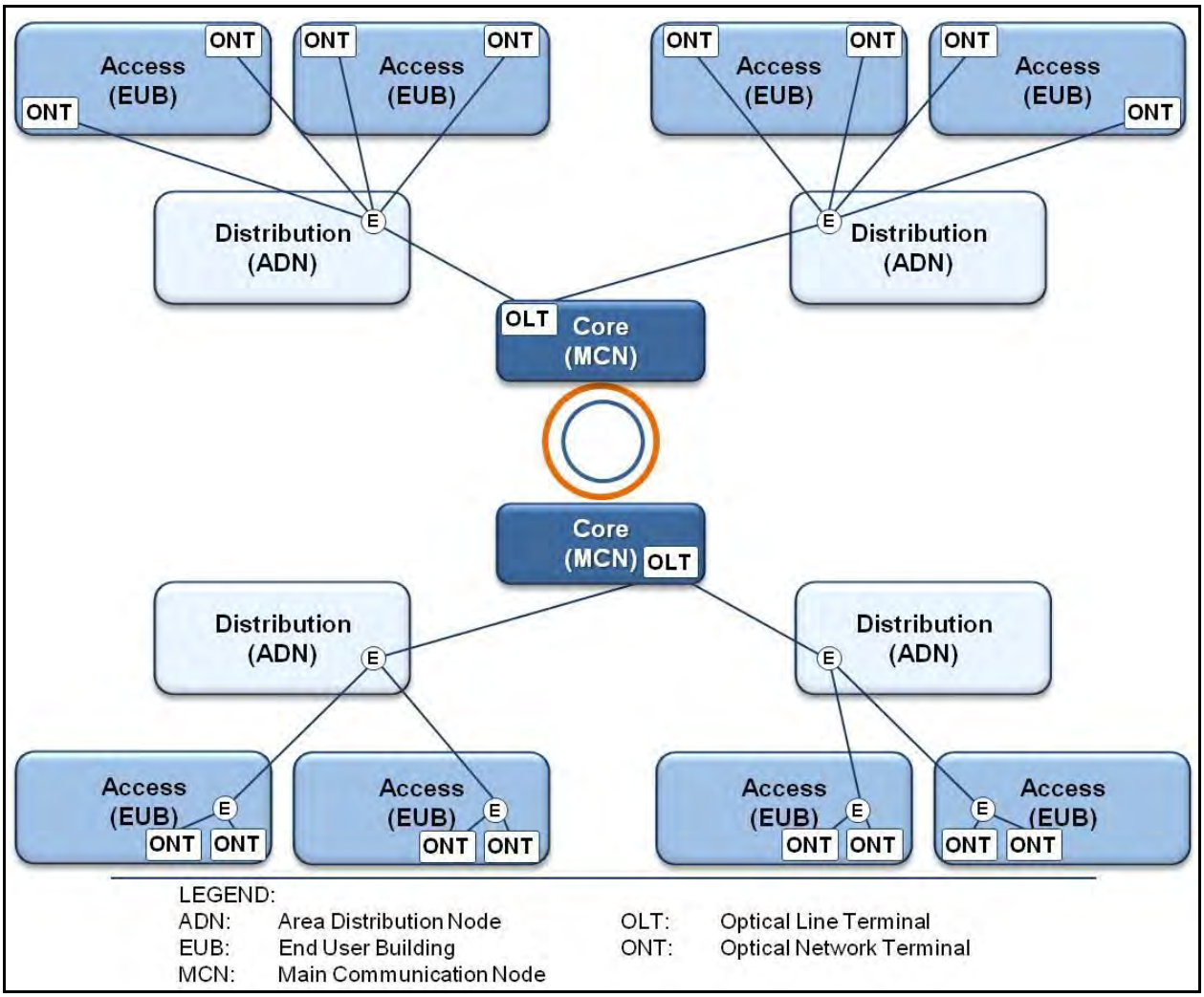


Figure 7.5-3. PON Connectivity in a Collapsed DoD Backbone Operational Framework

7.5.2 Interfaces

PONs can be composed of BPON, EPON, and GPON, and the requirements do not delineate between the different types. The UCR defines four types of interfaces in a typical PON: NNI: Ingress, OLT to ONT (PON), Network Management, and UNI.

7.5.2.1 NNI Interface

EDG-000600 [**Required: PON**] The NNI interface is composed of the uplink between the OLT and the Core network (LAN or WAN). This interface shall minimally be an IEEE 802.3 interfaces; the SUT may provide a Fibre channel interface IAW ANSI INCITS T11.2 and T11.3 (previously known as X3T9.3).

a. Minimally, the NNI shall be one of the following interface rates (other rates and IEEE standards may be provided as Optional interfaces):

(1) 100 Mbps IAW IEEE 802.3u.

(2) 1000 Mbps IAW IEEE 802.3z.

b. The NNI ports shall provide the following parameters on a per port basis as specified:

(1) Auto-negotiation IAW IEEE 802.3. Interfaces shall support auto-negotiation even when the IEEE802.3 standard has it as optional. This applies to 10/100/1000-T Ehternet Standards (i.e., IEEE, Ethernet Standard 802.3, 1993; or IEEE, Fast Ethernet Standard 802.3u, 1995; and IEEE, Gigabit Ethernet Standard 802.3ab, 1999).

(2) Force mode IAW IEEE 802.3.

(3) Flow control IAW IEEE 802.3x.

(4) Filtering IAW RFC 1812.

(5) Link Aggregation IAW IEEE 802.1AX (formerly 802.3ad).

(6) Spanning Tree Protocol IAW IEEE 802.1D.

(7) Multiple Spanning Tree IAW IEEE 802.1s.

(8) Rapid Configuration of Spanning Tree IAW IEEE 802.1w.

c. If the Fibre Channel Interface is provided the interface must meet:

(1) RFC 4338 Transmission of IPv6, Ipv4 and Address Resolution Protocol (ARP) Packets over Fibre channel.

(2) RFC 4044 Fibre Channel Management.

7.5.2.2 OLT to ONT PON Interface

EDG-000610 [**Required: PON**] The PON system shall provide one of the following PON (OLT-ONT) technologies:

a. GPON IAW G.984 series (G.984.1 through G.984.7).

b. EPON IAW 802.3ah. (1 Gbps).

c. GEPON IAW 802.3av (10 Gbps).

d. BPON IAW G.983.

EDG-000620 [**Conditional: PON**] If the PON supports GPON, then the OLT to ONT interface is defined by the ONT Management Control Interface (OMCI) protocol and was standardized and defined by the ITU standard G.984.4. This interface is composed of the PON port on the OLT and the Fiber port on the ONT. Between these ports is a single strand of Single Mode Fiber and one or more optical splitters. Bi directional transmission is accomplished by use of separate wavelengths (1310 nm and 1490 nm) for transmission. The number of splitters is driven by local requirements, and does not exceed the ITU T G.984 specification for fiber loss per PON port between the OLT and ONT. There may be one to 64 (some vendors support more) ONTs on a

single PON port. The number of ONTs is driven by the required bandwidth for each user and in accordance with the traffic engineering guidelines in Section 7.5.19, Traffic Engineering. The OLT to ONT interface will support the Telcordia Standards shown in Table 7.5-1, OLT to ONT Signaling Standards.

Table 7.5-1. OLT to ONT Signaling Standards

TELCORDIA STANDARDS:	GR-63-CORE	NEBS Generic Equipment Requirements
	GR-078-CORE	Physical Design and Manufacture Generic Requirements
	GR-199-CORE	Memory Administration Messages
	GR-418-CORE	Generic Reliability Requirements
	GR-472-CORE	Network Element Configuration Management
	GR-474-CORE	Alarm and Control for Network Elements
	GR-499-CORE	Transport System Generic Requirements
	GR-815-CORE	Generic Requirements for NE/NS Security
	GR-831-CORE	Language for Operations Application Messages
	GR-833-CORE	NE and Transport Surveillance Messages
	GR-1093-CORE	Generic State Requirements for Network Elements
	GR-1250-CORE	Generic Requirements for SONET File Transfer
	SR-1665	NMA Operations System Generic Transport NE Interface Support
	TR-NWT-000835	NE and Network System Security Administration Messages
	TR-TSY-000480	User System Interface – Directory for TR-TSY-000824 & 000825
ETSI STANDARDS:	ETSI-300-119-2, ETSI-300-119-3, ETSI-300-119-4	
ANSI STANDARDS:	T1.231, T1.264	
ITU-T STANDARDS:	G.664, G.671, G.681, G.692, G.703, G.704, G.707, G.709, G.775, G.783, G.798, G.806, G.808.1, G.823, G.825, G.831, G.841, G.842, G.871, G.872, G.873, G.874, G.875, G.957, G.958, G.959, G.7710, G.8251, X.721, X.744, M.3100, Q.822	

7.5.2.3 Network Management Interface

EDG-000630 [**Required: PON**] The PON products shall support the following network monitoring features:

a. Simple Network Management Protocol (SNMP) IAW RFCs 1157, 3410, 3411, 3412, 3413, and 3414.

b. SNMP Traps IAW RFC 1215.

c. RMON IAW RFC 2819. The product shall minimally support the following RFC groups: ethernet statistics, history control, Ethernet history, and alarm.

d. Coexistence between Version 1, Version 2, and Version 3 of the Internet-standard Network Management Framework IAW RFC 3584.

e. The Advanced Encryption Standard (AES) Cipher Algorithm in the SNMP User-based Security Model IAW RFC 3826.

7.5.2.4 UNI Interface

EDG-000640 [**Required: PON**] PON products shall provide at least one of the following user interface rates:

a. 10 Mbps IAW IEEE 802.3i.

b. 100 Mbps IAW IEEE 802.3u.

c. 1000 Mbps IAW IEEE 802.3z.

d. 1000 Mbps IAW IEEE 802.3ab.

In addition, PON must support traffic conditioning, which will ensure that the required bandwidth is available for all prioritized traffic.

7.5.2.4.1 UNI Ports

EDG-000650 [**Required: PON**] The UNI interface shall provide the following parameters on a per port basis as specified:

a. Auto-negotiation IAW IEEE 802.3.

b. Force mode IAW IEEE 802.3.

c. Flow control IAW IEEE 802.3x.

d. Filtering IAW RFC 1812.

e. Port-Base Access Control IAW 802.1x.

f. **[Optional: PON]** Link Layer Discover – Media Endpoint Discovery IAW ANSI TIA 1057.

EDG-000660 [**Optional: PON**] Link Aggregation IAW IEEE 802.1AX (formerly 802.3ad).

EDG-000670 [**Optional: PON**] The UNI ports may provide the following features parameters on a per port basis as specified:

a. Data Terminal Equipment (DTE) Power via Media Dependent Interface (MDI) PoE for Optional Interfaces IEEE 802.3af.

b. PoE Plus or Data Terminal Equipment (DTE) Power via Media Dependent Interface (MDI) for Optional Interfaces IEEE 802.3at.

7.5.3 Class of Service Markings

EDG-000680 [**Required: PON**] The PON network shall comply with access product requirements, Section 7.2.1.3, Class of Service Markings, Class of Service Markings, paragraph 1 (a, b, and c).

7.5.4 Virtual LAN Capabilities

EDG-000690 [**Required: PON**] The NNI and UNI PON ports shall comply with Section 7.2.1.4, Virtual LAN Capabilities.

7.5.5 Protocols

EDG-000700 [**Optional: PON**] The PON network shall support bridging at Layer 2 of the OSI model. Bridging will provide for higher survivability as well as reducing traffic congestion on the uplinks to the Distribution or Core Layers of the network. Bridging at Layer 2 will be supported for packets that do not require Layer 3 handling.

7.5.6 Quality of Service Features

EDG-000710 [**Required: PON**] The PON shall comply with the Access product requirements listed in Section 7.2.1.6, Quality of Service Features. PON products targeted for non-assured services are not subject to the Layer 3 queuing requirements in this section and the conditions of fielding will state whether the PON can support Assured Services or not.

7.5.7 Voice Services

7.5.7.1 Latency

EDG-000720 [**Required: PON**] The PON shall have the capability to transport prioritized voice IP packets, media, and signaling, with no more than 6 ms latency end-to-end (E2E) across the PON System Under Test (SUT) as measured under congested conditions. Congested conditions are defined as 100 percent of link capacities (as defined by baseline traffic engineering ~~25 percent voice/signaling, 25 percent IP video, 25 percent preferred data, and 25 percent best effort traffic~~). The latency shall be achievable over any 5 minute measured period under congested conditions.

7.5.7.2 Jitter

EDG-000730 [**Required: PON**] The PON shall have the capability to transport prioritized voice IP packets across the PON SUT with no more than 3 ms of jitter. The jitter shall be achievable over any 5-minute measured period under congested conditions. Congested conditions are defined as 100 percent of link capacities (as defined by baseline traffic engineering

(e.g., 25 percent voice/signaling, 25 percent IP video, 25 percent preferred data, and 25 percent best effort traffic).

7.5.7.3 Packet Loss

EDG-000740 [**Required: PON**] The PON shall have the capability to transport prioritized IP packets across the PON SUT with packet loss not to exceed configured traffic engineered (queuing) parameters. Actual measured packet loss across the PON shall not exceed 0.045 percent within the defined queuing parameters. The packet loss shall be achievable over any 5-minute measured period under congested conditions. Congested conditions are defined as 100 percent of link capacities (as defined by baseline traffic engineering (e.g., 25 percent voice/signaling, 25 percent video, 25 percent preferred data, and 25 percent best effort traffic).

7.5.8 Video Services

7.5.8.1 Latency

EDG-000750 [**Required: PON**] The PON shall have the capability to transport prioritized video IP packets with no more than 30 ms latency across the PON SUT. Latency is increased over prioritized voice IP packets because of the increased size of the packets (230 bytes for voice packets and up to 1518 bytes for video). The latency shall be achievable over any 5-minute measured period under congested conditions. Congested conditions are defined as 100 percent of link capacities (as defined by baseline traffic engineering (e.g., 25 percent voice/signaling, 25 percent video, 25 percent preferred data, and 25 percent best effort traffic).

7.5.8.2 Jitter

EDG-000760 [**Required: PON**] The LAN shall have the capability to transport prioritized video IP packets across the PON SUT with no more than 30 ms of jitter. The jitter shall be achievable over any 5-minute measured period under congested conditions. Congested conditions are defined as 100 percent of link capacities (as defined by baseline traffic engineering (e.g., 25 percent voice/signaling, 25 percent video, 25 percent preferred data, and 25 percent best effort traffic).

7.5.8.3 Packet Loss

EDG-000770 [**Required: PON**] The PON shall have the capability to transport prioritized video IP packets across the PON SUT with packet loss not to exceed configured traffic engineered (queuing) parameters. Actual measured packet loss across the PON shall not exceed 0.15 percent within the defined queuing parameters. The packet loss shall be achievable over any 5 minute measured period under congested conditions. Congested conditions are defined as 100 percent of link capacities (as defined by baseline traffic engineering (e.g., 25 percent voice/signaling, 25 percent video, 25 percent preferred data, and 25 percent best effort traffic).

7.5.9 Data Services

7.5.9.1 Latency

EDG-000780 [**Required: PON**] The PON shall have the capability to transport prioritized data IP packets with no more than 45 ms latency across the PON SUT. Latency is increased over voice IP packets because of the increased size of the packets (230 bytes for voice packets and up to 1518 bytes for data). The latency shall be achievable over any 5-minute measured period under congested conditions. Congested conditions are defined as 100 percent of link capacities (as defined by baseline traffic engineering (e.g., 25 percent voice/signaling, 25 percent video, 25 percent preferred data, and 25 percent best effort traffic).

7.5.9.2 Jitter

There are no jitter requirements for preferred data IP packets.

7.5.9.3 Packet Loss

EDG-000790 [**Required: PON**] The PON shall have the capability to transport prioritized data IP packets across the PON SUT with packet loss not to exceed configured traffic engineered (queuing) parameters. Actual measured packet loss across the LAN shall not exceed 0.15 percent within the defined queuing parameters. The packet loss shall be achievable over any 5-minute period measured under congested conditions. Congested conditions are defined as 100 percent of link capacities (as defined by baseline traffic engineering (e.g., 25 percent voice/signaling, 25 percent video, 25 percent preferred data, and 25 percent best effort traffic).

7.5.10 Information Assurance

EDG-000800 [**Required: PON**] All systems must comply with the applicable Security Technical Implementation Guides (STIGs).

7.5.11 PON Network Management

EDG-000810 [**Required: PON**] Network managers must be able to monitor, configure, and control all aspects of the network and observe changes in network status. The PON infrastructure components shall have a Network Management (NM) capability that leverages existing and evolving technologies and has the ability to perform remote network product configuration /reconfiguration of objects that have existing DoD Global Information Grid (GIG) management capabilities. The PON infrastructure components must be able to be centrally managed by an overall Network Management System (NMS). In addition, Management Information Base (MIB) II shall be supported for SNMP. In addition, if other methods are used for interfacing between PON products and the NMS, they shall be implemented in a secure manner, such as with the following methods.

7.5.11.1 Secure Shell Version 2

EDG-000820 [**Required: PON**] Secure Shell version 2 (SSHv2). The PON products shall support RFC 4251 through RFC 4254 inclusive.

7.5.11.2 Telnet

EDG-000830 [**Required: PON**] The PON product shall be configured by default not to accept Telnet.

7.5.11.3 HTTPS

EDG-000840 [**Optional: PON**] HyperText Transfer Protocol Secure (HTTPS). HTTPS shall be used instead of HyperText Transfer Protocol (HTTP) because of its increased security as described in RFC 2818.

7.5.11.4 LAN Products

EDG-000850 [**Optional: PON**] The LAN products shall support RFC 3414 for SNMP.

7.5.11.5 Other Methods for Interfacing

EDG-000860 [**Optional: PON**] If other methods are used for interfacing between LAN products and the NMS, they shall be implemented in a secure manner.

7.5.12 Configuration Control

EDG-000870 [**Required: PON**] Configuration Control identifies, controls, accounts for, and audits all changes made to a site or information system during its design, development, and operational life cycle [DoD Chief Information Officer (CIO) Guidance IA6 8510 IA]. Local area networks shall have an NM capability that leverages existing and evolving technologies and has the ability to perform remote network product configuration/reconfiguration of objects that have existing DoD GIG management capabilities. The NMS shall report configuration change events in near-real time (NRT), whether or not the change was authorized. The system shall report the success or failure of authorized configuration change attempts in NRT. NRT is defined as within 5 seconds of detecting the event, excluding transport time.

7.5.13 Operational Changes

EDG-000880 [**Required: PON**] The PON shall meet the requirements detailed in the following text. The PON shall report the status of networks and associated assets in NRT 99 percent of the time (with 99.9 percent as an Objective Requirement). NRT is defined as receiving operational changes within 5 seconds of querying the status (polled) or within 5 seconds of receiving status changed (pushed), excluding transport time.

7.5.14 Performance Monitoring

EDG-000890 [**Required: PON**] The PON shall meet the requirements specified. All PON infrastructure components shall be capable of providing status changes 99 percent of the time (with 99.9 percent as an Objective Requirement) by means of an automated capability in NRT. An NMS will have an automated NM capability to obtain the status of networks and associated assets 99 percent of the time (with 99.9 percent as an Objective Requirement) within 5 seconds of querying the status (polled) or within 5 seconds of receiving status changes (pushed) from the monitored device. The NMS shall collect statistics and monitor bandwidth utilization, delay, jitter, and packet loss.

7.5.15 Alarms

EDG-000900 [**Required: PON**] The PON shall meet the requirements. The PON shall report alarms as TRAPs via SNMP in NRT. More than 99.95 percent of alarms shall be reported in NRT. NRT is defined as receiving alarm changes within 5 seconds of querying the status (polled) or within 5 seconds of receiving alarm changes (pushed) from the monitored device.

EDG-000910 In addition to the alarms defined in this section, the OLT shall support the alarms as defined by ITU G994.4.

7.5.16 Reporting

EDG-000920 [**Required: PON**] The PON shall meet the following requirements. The PON shall have the NM capability of automatically generating and providing an integrated/correlated presentation of network and all associated networks. In addition, the PON system must also report optical errors to include degraded optical conditions.

7.5.17 Fiber Media

EDG-000930 [**Required: PON**] Fiber Optic Cable used for the PON shall be Single Mode Fiber. The single mode fiber shall be in compliance with ITU G.652/TIA OS1/International Electrotechnical Commission (IEC) B1.1.

7.5.18 RF-over-Glass (RFoG) Video

EDG-000940 [**Optional: PON**] If the PON system supports GPON, then it may optionally support RFoG via PON and its RF overlay framework. ITU-T G.984.5 defines this band as an Enhancement band for video distribution services. This ITU forum also specifies a wavelength of 1150 nm to 1560 nm. This video capacity is in addition to the 2.4 Gbps downstream and 1.2 upstream capacity of GPON. It is the responsibility of the ONT to either block or separate the RFoG from the downstream GPON signal of 1480 to 1500 nm.

The spectrum is allocated as follows:

- 40 Analog channels at 54 to 550 MHz.
- 63 Digital 256 Quadrature Amplitude Modulation (QAM) channels at 225 to 870 MHz.
- One Quadrature Phase-Shift Keying (QPSK) Out of Band (OOB) channel at 71 to 125 MHz.

7.5.19 Traffic Engineering

EDG-000950 [**Required: PON**] Bandwidth required per subscriber must be in compliance with the requirements in this section and additional DoD regulations as applicable.

7.5.20 VLAN Design and Configuration

EDG-000960 [**Required: PON**] VLAN Design and Configuration for all PON networks must be in compliance with Distribution and Access Layer Network Elements as defined in this section.

7.5.21 Power Backup

EDG-000970 [**Required: ASLAN Network PON – Optional: Non-ASLAN Network PON**] To meet Chairman of the Joint Chiefs of Staff (CJCS) requirements, the PON network must be in compliance with the requirements in this section. Required or Optional adherence shall be based on whether the PON Network Element is being placed into an ASLAN or a Non-ASLAN.

7.5.22 Availability

Availability of a PON network will be determined the same as for active Ethernet networks as defined in this section. PON Network Elements that are utilized in ASLANs and Non-ASLANs must meet the availability requirements for the appropriate LAN.

EDG-000980 [**Optional: PON**] If the PON system supports GPON, then it may optionally support Type B PON Protection as defined in ITU-T G.984.1 3/2008 to provide increased reliability for all services carried on the PON, including data.

7.5.23 Redundancy

The following paragraphs outline the redundancy requirements for the PON Network.

EDG-000990 [**Required: PON in ASLAN – Optional: PON in Non-ASLAN**] The PON product shall have no single point of failure that can cause an outage of more than 96 IP telephone subscribers. It should be noted that a PON may be used with a single point of failure for more than 96 subscribers if 96 or less are IP telephone subscribers (i.e., 50 data, 20 video, and 50 IP telephony = 120 subscribers).

7.5.23.1 Single Product Redundancy

EDG-001000 [**Optional: PON**] If redundancy is met through single product, the following requirements are applicable:

a. Dual Power Supplies. The platform shall provide a minimum of two power inputs each with the power capacity to support the entire chassis. Loss of a single power input shall not cause any loss of ongoing functions within the chassis.

b. Dual Processors (Control Supervisors). The chassis shall support dual control processors. Failure of any one processor shall not cause loss of any ongoing functions within the chassis (e.g., no loss of active calls). Failure of the primary processor to secondary must meet 5-second failover without loss of active calls.

c. Redundancy Protocol. PON equipment shall support a protocol that allows for dynamic rerouting of IP packets so that no single point of failure exists in the PON that could cause an outage to more than 96 IP subscribers. It should be noted that a PON may be used with a single point of failure for more than 96 subscribers if 96 or less are IP telephone subscribers (i.e., 50 data, 20 video, and 50 IP telephony = 120 subscribers). Redundancy protocols will be standards based as specified in this document.

d. Backplane/Bridging Redundancy. Bridging platforms within the PON shall support a redundant (1+1) switching fabric or backplane. The second fabric's backplane shall be in active standby so that failure of the first shall not cause loss of ongoing events within the OLT.

NOTE: In the event of a component failure in the network, all calls that are active shall not be disrupted (loss of existing connection requiring redialing) and the path through the network shall be restored within 5 seconds.

7.5.23.2 Dual Product Redundancy

EDG-001010 [**Optional: PON**] In the case where a secondary product has been added to provide redundancy to a primary product, the failover over to the secondary product must not result in any lost calls. The secondary product may be in "standby mode" or "active mode," regardless of the mode of operation the traffic engineering of the links between primary and secondary links must meet the requirements provided in Section 7.5.19, Traffic Engineering.

NOTE: In the event of a primary product failure, all calls that are active shall not be disrupted (loss of existing connection requiring redialing) and the failover to the secondary product must be restored within 5 seconds.

7.5.24 Survivability

Network survivability refers to the capability of the network to maintain service continuity in the presence of faults within the network. This can be accomplished by recovering quickly from network failures and maintaining the required QoS for existing services.

EDG-001020 [**Required: PON**] For PON Survivability, the PON shall support a Layer 2 Dynamic Rerouting protocol. Failover shall occur in no more than 5~~1~~ seconds.

7.5.25 Summary of PON Requirements by Subscriber Mission

EDG-001030 [**Required: PON**] The PON Network Elements shall meet the same requirements as specified in Table 7.1-1, Summary of LAN Requirements by Subscriber Mission, as applicable for the LAN the Network Element will be included within to include meeting the IPv6 requirements as defined in Section 5, IPv6. The PON shall meet all the following IPv6 requirements: RFC 2464 and FRC 2474 ~~applicable as defined for a LAN access switch (Table 5.2-6, LAN Switch)~~.

7.6 CUSTOMER EDGE ROUTER (CER)

7.6.1 Traffic Conditioning

EDG-001040 [**Required: CER**] The product shall be capable of performing traffic conditioning (policing and shaping) on inbound and outbound traffic. This may involve the dropping of excess packets or the delaying of traffic to ensure conformance with SLAs. The product shall meet the requirements for "core" products defined within Section 7.5.6, Quality of Service Features.

EDG-001050 [**Required: CER**] The product shall be capable of traffic conditioning the bandwidth associated with a service class.

7.6.2 Differentiated Services Support

EDG-001060 [**Required: CER**] The product shall be capable of supporting DS IAW RFCs 2475 and 2474 as specified in Section 7.2.1.3, Class of Service Markings.

7.6.3 Per-Hop Behavior Support

EDG-001070 [**Required: CER**] The product shall be capable of supporting the PHBs. The product shall meet "core" behavior requirements are defined in Section 7.2.1.6, Quality of Service Features.

NOTE: The product shall be capable of supporting EF PHBs IAW RFC 3246.

EDG-001080 [**Required: CER**] The product shall be capable of supporting the AF PHB IAW RFC 2597.

7.6.4 Interface to the SC/SS for Traffic Conditioning

EDG-001090 [**Optional: CER**] The CER shall be capable of interfacing to the SC/SS in real time to adjust traffic conditioning parameters based on the updated SC/SS budgets.

NOTE: For example, if the SC budget decreases from ten Voice sessions to five Voice sessions, then the traffic conditioning parameters should change from 10 x 110 equals 1100 kbps to 5 x 110 equals 550 kbps in both directions. Initially, the process will be a manual process to configure the PHB allocations statically. This assumes that traffic conditioning occurs before applying the PHBs.

7.6.5 Interface to the SC/SS for Bandwidth Allocation

EDG-001100 [**Optional: CER**] The product shall be capable of interfacing to the SC/SS in real time to adjust the PHB bandwidth allocations based on the updated SC/SS budgets.

NOTE: For example, if the SC budget decreases from ten Voice sessions to five Voice sessions, then the EF queue bandwidth allocation should change from 10 x 110 equals 1100 kbps to 5 x 110 equals 550 kbps in both directions. Initially, the process will be a manual process to configure the PHB allocations statically. This assumes that traffic conditioning occurs before applying the PHBs.

7.6.6 Network Management

EDG-001110 [**Required: CER**] The product shall support Fault, Configuration, Accounting, Performance, and Security (FCAPS) Network Management functions as defined in the Section 2.19, Management of Network Appliances.

7.6.7 Availability

The four types of CERs are High Availability, Medium Availability without System Quality Factors (SQFs), Medium Availability with SQF, and Low Availability. Defining four types of CERs is driven by cost factors, and the availability that can be provided by commercial off-the-shelf (COTS) products.

Locations serving F/FO users and I/P users and R users with PRIORITY and above precedence service should install High Availability CERs. The Medium Availability (two types) and Low Availability CER provide a cost-effective solution for locations that serve R users.

EDG-001120 [**Required: High Availability CER**] The product shall have an availability of 99.999 percent, including scheduled hardware and software maintenance (non-availability of no more than 5 minutes per year). The product shall meet the requirements specified in Section 2.8.2, Product Quality Factors.

EDG-001130 [**Required: Medium Availability CER Without SQF**] The product shall have an availability of 99.99 percent, including scheduled hardware and software maintenance (non-availability of no more than 52.5 minutes per year). The product does not need to meet the requirements specified in Section 2.8.2, Product Quality Factors.

EDG-001140 [**Optional: Medium Availability CER With SQF**] The product shall have an availability of 99.99 percent, including scheduled hardware and software maintenance (non-availability of no more than 52.5 minutes per year). The product shall meet the requirements specified in Section 2.8.2, Product Quality Factors.

EDG-001150 [**Optional: Low Availability CER**] The product shall have an availability of 99.9 percent, including scheduled hardware and software maintenance (non-availability of no more than 8.76 hours per year). The product does not need to meet the requirements specified in Section 2.8.2, Product Quality Factors.

NOTE: The vendor will provide a reliability model for the product showing all calculations for how the availability was met.

7.6.8 Packet Transit Time

EDG-001160 [**Required: CE Router**] The CER shall meet the following requirements:

a. The CER shall be non-blocking (see Section 7.2.1, General LAN Switch and Router Product, for definitions and conditions.)

b. The CER shall meet the latency requirements for "core" products specified in Section 7.2.1 with the exception that T1, E1, or lower rate interfaces shall be increased from 2 ms to 15 ms.

c. The CER shall meet the Jitter requirements specified for "core" products in Section 7.2.1.

d. The CER shall meet the packet loss requirements specified for "core" products in Section 7.2.1.

This transit time shall be in addition to the serialization delay for voice packets as measured from the input interface to output interface under congested conditions to include all internal functions. For example, the serialization delay of a 100BT Interface is 0.017 ms, which would allow for voice packet latency from input to Ethernet output under congested conditions of 2.017 ms.

NOTE: Internal functions do not include Domain Name Service (DNS) lookups and other external actions or processes.

7.6.9 Customer Edge Router Interfaces and Throughput Support

The CER supports an ASLAN-side connection to the Session Border Controller (SBC) and a WAN-side connection to the Defense Information Systems Network (DISN) WAN.

EDG-001170 [**Required: CER**] The ASLAN-side interface shall be an Ethernet interface (10 Base-X [TX or FX], [**Optional**] 100 Base-X Mbps, [**Optional**] 1 Gigabit Ethernet, or [**Optional**] 10GbE [full duplex]), and at least one of the WAN-side interfaces shall be an Ethernet interface (10 Base-X, [**Optional**] 100 Base-X, [**Optional**] 1 Gigabit Ethernet, or [**Optional**] 10GbE [full duplex]).

EDG-001180 [**Optional: CER**] The WAN-side access connection interface can also be Time Division Multiplexing (TDM) based (i.e., DS1, DS3, or E1). These are all full-duplex interfaces, and support two-way simultaneous information exchange at the "line rate" for the interface (i.e., 1.5 Mbps for DS1, 45 Mbps for DS3, 2.0 Mbps for E1).

EDG-001190 [**Optional: CER**] The WAN-side access connection interface can also be Synchronous Optical Network (SONET) based (i.e., OC-x; e.g., OC3, OC12, OC48 or OC192). These are all full-duplex interfaces, and support two-way simultaneous information exchange at the "line rate" for the interface.

The CER needs to support information "throughput" in two directions: from the ASLAN side to the WAN side, and from the WAN side to the ASLAN side. The CER also needs to support this throughput in full-duplex mode, which means that the CER needs to support the maximum possible throughput on the WAN-side interface for packets sent in the ASLAN-to-WAN direction. At the same time, the CER needs to support the maximum possible throughput on the WAN-side interface for packets sent in the WAN-to-ASLAN direction. The maximum possible throughput for an interface is the maximum line rate for that interface, as provisioned on the CER.

A CER may support multiple interfaces on the ASLAN side, such as two 100 BTs to an SBC and a data firewall, and on the WAN side, such as two DS1s to two different DISN SDNs. These requirements assume that the CER only has one WAN-side interface active. They also assume that the line rate for the WAN-side interface is less than or equal to the sum of the line rates for the ASLAN-side interfaces.

EDG-001200 [**Required: CER**] The CER shall support the maximum possible throughput on the WAN-side interface for a full traffic load of all traffic types sent in the ASLAN-to-WAN direction.

EDG-001210 [**Required: CER**] The CER shall support the maximum possible throughput on the WAN-side interface for a full traffic load of all traffic types sent in the WAN-to-ASLAN direction.

EDG-001220 [**Required: CER**] The CER shall support the maximum possible throughput on the WAN side interface in a full-duplex mode, for a full traffic load of UC packets sent simultaneously in both the ASLAN-to-WAN and WAN-to-ASLAN directions.

EDG-001230 [**Required: CER**] The Maximum Possible Throughput (MPT) on the WAN-side interface shall be the maximum line rate that the WAN-side interface is provisioned for on the CER. The following MPTs shall apply for the different WAN-side interfaces:

a. 10 Base-X: 10 Mbps.

b. 100 Base-X: 100 Mbps [**Optional**].

c. 1 Gigabit Ethernet: 1 Gbps [**Optional**].

d. 10 Gigabit Ethernet: 10 Gbps [**Optional**].

e. DS1: 1.5 Mbps [**Optional**].

f. DS3: 45 Mbps [**Optional**].

g. E1: 2.0 Mbps [**Optional**].

h. OC3: 155 Mbps [**Optional**].

i. OC12: 622 Mbps [**Optional**].

j. OC48: 2.5 Gbps [**Optional**].

k. OC192: 9.6 Gbps [**Optional**].

These MPTs may not be attainable on some interfaces on some products. If a vendor cannot meet one of the MPTs listed, they should identify the actual MPT that their product supports. If this actual MPT depends on frame size, the vendor should document how the frame size should be used to calculate the actual MPT.

EDG-001240 [Required: CER] The CER must minimally support the following routing protocols:

a. LAN-side interfaces must support OSPF IAW RFCs 2328, 2740, 3623, 5187, and 5340.

b. WAN-side interfaces shall support BGP IAW RFCs 1772, 2439, 4271, and 4760. The CER shall support both external BGP (eBGP) and internal BGP (IBGP). The CER shall support route reflectors (RFC 4456) and confederations (RFC 5065).

EDG-001250 [**Required: CER**] The CER must meet the IA requirements specified for Router "R."

EDG-001260 [**Required: CER**] The CER must meet the IPv6 Requirements in Section 5 specified for Router "R."

SECTION 8
MULTIFUNCTION MOBILE DEVICES

8.1 INTRODUCTION

This section addresses the requirements for an array of mobile devices and their associated supporting infrastructure elements. A Multifunction Mobile Device (MMD) is defined as an advanced, yet highly portable, computing platform that supports one or more compact input interfaces (e.g., touch screens, stylus, and miniature keyboard) to facilitate user interaction. These devices provide network access through primarily wireless means, though wired connectivity may also be a feature of these products. An MMD can assume any number of form factors including, but not limited to, a smartphone, Personal Digital Assistant (PDA), or small form factor wireless tablet. A more detailed discussion on multifunction mobile devices, supporting infrastructure, and DoD approved use cases can be found in Unified Capabilities Framework (UCF) 2013, Section 8, Multifunction Mobile Devices.

The MMD category of the Department of Defense (DoD) Unified Capabilities (UC) Approved Products List (APL) encompasses all of the products and systems discussed in this Unified Capabilities Requirements (UCR) section. Products listed on the DoD UC APL will have been certified to comply with the subsequently defined UCR requirements and applicable Defense Information Systems Agency (DISA) Field Security Office (FSO) Security Technical Implementation Guidelines (STIGs) and Security Requirements Guides (SRGs).

~~NOTE: Currently, the UCR defines two primary multifunction mobile device-related product categories: the MMD itself and the MMD backend supporting services. However, the UC Steering Group is reviewing proposals to add new product categories or refine these categories to include Mobile Device Manager (MDM), MMD Operational Support System (MOSS), Mobile Application Store (MAS), and other components related to MMDs. The outcome of this decision may result in changes to the current MMD section of this UCR.~~

8.1.1 Use Cases for Multifunction Mobile Devices

In the context of the UCR, the scenarios in which MMDs may be used for UNCLASSIFIED applications are currently grouped into two primary use cases, as shown in Table 8.1-1, Multifunction Mobile Device Use Cases. Additional discussion regarding these uses cases occurs in UC Framework 2013, Section 8, Multifunction Mobile Devices.

Table 8.1-1. Multifunction Mobile Device Use Cases

USE CASE NUMBER	TITLE	HIGH LEVEL DESCRIPTION
#1	Non Enterprise Activated Use Case: No Connectivity to DoD Network and No Processing of CUI Data Use Case No connectivity to DoD e-mail	MMD that has no connectivity to a DoD network and processes only publicly available DoD data information (Data as defined in this context is clarified in Section 8 of the UCF)
#2	Full Connectivity to DoD Network and Processing of Sensitive UNCLASSIFIED Information Use Case	MMD that supports access to DoD Networks either directly or via a secure tunnel established across public networks Securely processes and stores DoD information at the CUI level
#3	Full Connectivity to DoD Network and Processing of Sensitive UNCLASSIFIED Information Use Case Full Connectivity to DoD UC Services	MMD that supports access to DoD Networks either directly or via a secure tunnel established across public networks Securely processes and stores DoD information at the CUI level. This MMD has full connectivity to DoD UC Services

8.1.2 Multifunction Mobile Devices and Components

Table 8.1-2, Acronyms and Appliances Specifying Type of Component, shows the acronyms and appliances that represent a specific UC APL product.

Table 8.1-2. Acronyms and Appliances Specifying Type of Component

ACRONYM	APPLIANCES
MMD	MMD [Includes the platform hardware, Operating System (OS), applications, and ancillary devices such as Bluetooth Common Access Card (CAC) readers]
UC_MMD_App	Unified Capabilities MMD Application [Applications residing on a Use Case #2 MMD providing IP-based connectivity to DoD UC services including VVoIP and Extensible Messaging and Presence Protocol (XMPP) services]
MDM	Mobile Device Management system defined in the DISA FSO "MDM SRG Overview" document as the "systems (server and mobile device agent) used to manage mobile devices that are DoD-administered or connected to DoD networks."
MBSS	MMD Backend Support System (Includes ~~the~~ any additional system hardware, OSs, applications, and any required ancillary equipment to support MMDs beyond the MDM) (The term MMD Operational Support System may replace this term in subsequent UCR revisions)

8.2 REQUIREMENTS

8.2.1 IO and IA Test Report Considerations

Beginning with UCR 2013, all UCR requirements will be adjudicated as Technical Deficiency Reports (TDRs) and will appear only in Interoperability (IO) test reports. The DISA FSO STIGs and SRGs shall form the basis for any Information Assurance (IA) findings appearing in IA test

reports. As a result, some requirements have been removed from this section in order to minimize duplication between IA findings and IO TDRs in test reports.

8.2.2 The [Alarm] Tag: Generation of Alarms

If the [Alarm] tag appears after a requirement's applicability statement (e.g., Required or Conditional), then this tag has the same meaning as defined in Section 4.2.1, The [Alarm] Tag: Generation of Alarms.

8.2.3 Requirements for Multifunction Mobile Devices Conforming to Use Case #1

MMD-010000 [**Conditional: MMD, MBSS, MDM**] If the system conforms to Use Case #1, then the system shall comply with all requirements defined within the appropriate DISA FSO STIG(s) and SRG(s).

NOTE: At the time of this writing, the DISA FSO General Mobile Device (Non-Enterprise Activated) STIG serves as one of the primary baselines for Use Case #1.

8.2.4 Requirements for Multifunction Mobile Devices Conforming to Use Case #2

MMD-020000 [**Conditional: MMD, MBSS, MDM**] If the system conforms to Use Case #2, then the system shall comply with all requirements defined within the appropriate DISA FSO STIGs and SRGs.

NOTE: At the time of this writing, the DISA FSO Wireless STIGs and SRGs contain the most directly applicable Information Assurance (IA) requirements for Use Case #2 mobile devices.

8.2.5 Requirements for Multifunction Mobile Devices Conforming to Use Case #3

MMD-030000 [**Conditional: MMD, MBSS, MDM**] If the system conforms to Use Case #3, then the system shall comply with all requirements identified in this UCR for Use Case #2 devices.

MMD-040000 [**Conditional: UC_Multifunction_Mobile_App**] If the MMD supports a UC MMD Application to allow direct connectivity to DoD-provided UC services, then the application shall comply with the following requirements:

MMD-040010 [**Required: UC_Multifunction_Mobile_App**] The application shall conform to all IO and IA interoperability requirements specified for End Instruments (EIs) or Assured Services Session Initiation Protocol (AS-SIP) EIs (AEIs) if the

application implements AS-SIP) in the UCR, with the exception of the following requirements:

NOTE: This includes the capability to support operation on IPv6-enabled MMD platforms and connected networks.

MMD-040020 [**Conditional: UC_Multifunction_Mobile_App**] If the application does not support all codec types specified in Section 2.9, End Instruments, for EIs and AEIs, then this noncompliance is permitted, provided that the application's homed MBSS transcodes appropriately when communicating with the Session Controller (SC) (Softswitch [SS]), thereby maintaining interoperability with normal EIs and AEIs that do support these codecs.

NOTE: This requirement is intended to accommodate bandwidth-constrained wireless networks where codecs such as G.711 may consume too much bandwidth.

MMD-040030 [**Conditional: UC_Multifunction_Mobile_App**] When the UC MMD Application connects to its homed SC via the MBSS, it is not required to support the capability to support Multilevel Precedence and Preemption (MLPP) or display the precedence level of calls. However, if it does so, then it must do so in accordance with (IAW) the requirements in Section 2, Session Control Products.

MMD-040040 [Required: UC_Multifunction_Mobile_App] The cryptographic interoperability profile (algorithms used for confidentiality, integrity, etc.) used to establish secure connectivity from the UC MMD Application to the MBSS to transmit signaling information shall be equal to or stronger than the profiles specified for the Transport Layer Security (TLS) and Internet Protocol Security (IPSec) in Section 4, Information Assurance.

MMD-040050 [**Required: UC_Multifunction_Mobile_App**] For VVoIP media traffic, the cryptographic profile shall be equal to or stronger than the profile defined for Secure Real-Time Transport Protocol (SRTP) in Section 4, Information Assurance.

MMD-040060 [**Conditional: UC_Multifunction_Mobile_App**] If the application connects directly to a DoD-controlled WLAN enclave and bypasses its homed MBSS to connect to its SC, then the application and its associated platform shall conform to all requirements applicable to Wireless End Instruments (WEIs) specified in Section 7, Network Edge Infrastructure Requirement.

MMD-040070 [**Conditional: UC_Multifunction_Mobile_App**] Any chat or collaboration capabilities provided by the UC MMD Application shall be IAW UC XMPP 2013.

NOTE: This conditional requirement is in addition to any applicable STIGs and STIG checklists such as the Instant Messaging STIG.

MMD-050000 [**Conditional: MBSS**] If the MBSS provides connectivity to the SC (or SS) on behalf of any served UC MMD Applications, then the product shall conform to the subtended requirements:

MMD-050010 [**Conditional: MBSS**] If the system supports UC MMD applications, unless explicitly stated otherwise by the subtended requirements, on the interface used by the MBSS to communicate with its homed SC or SS, then the MBSS shall act as any other EI or AEI and so comply with all functional and Information Assurance interoperability requirements in this UCR for EIs or AEIs as appropriate.

MMD-050020 [**Conditional: MBSS**] If the VVoIP media traffic transmitted between the UC MMD Application and the MBSS does not use one of the codecs required in Section 2.9, End Instruments, then the system shall support a transcoding function that securely translates this media traffic into a format compatible with the SC line-side protocol.

MMD-050030 [**Conditional: MBSS**] If the system supports UC MMD applications, then the system shall ensure that VVoIP media, signaling, IM, and any other supported UC traffic originating from the MMD that traverses the MBSS are marked with the appropriate Differentiated Services Code Point (DSCP) value specified in Section 6, Network Infrastructure End-to-End Performance, upon entrance into the enclave UC network.

NOTE: Ideally, the MBSS should place UC VVoIP traffic onto a Virtual Local Area Network (VLAN) that is separate from the VLAN used for other non-UC VVoIP related services (e.g., email).

MMD-050040 [**Conditional: MBSS**] If the served UC MMD Applications do not support MLPP, then the MBSS shall interface with its homed SC and use the procedures defined in Section 2, Session Control Products, to handle calls received above the ROUTINE level that cannot be forwarded to the UC MMD Application (e.g., forwarding to an attendant).

MMD-050050 [**Conditional: MBSS**] If the system supports UC MMD applications, then the system shall provide secure connectivity to the served UC MMD applications by, at a minimum, implementing Back-to-Back User Agent (B2BUA) (SBC-like) application layer gateway functionality or alternatively providing Virtual Private Network (VPN) functionality when communicating with served UC MMD Applications.

MMD-050060 [**Conditional: MBSS**] If the system supports UC MMD applications, then the UC VVoIP network-related traffic (VVoIP media, signaling) that appears on the network as it transits the system shall remain encrypted at all points with cryptographic strength consistent with the TLS and IPSec profiles (signaling) and SRTP profile (for media) specified in this Section of the UCR. The system must not rely on physical safeguards alone to provide confidentiality for data in transit.

NOTE: The MBSSs that provide UC VVoIP capabilities also must conform to the VVoIP Intrusion Detection System (IDS) monitoring requirements in Section 4.2.4, Ancillary Equipment; Section 13, Security Devices; and Section 4.2.9, Confidentiality.

MMD-050070 [**Conditional: MBSS**] If the system supports UC MMD applications, then the product shall support either an onboard VVoIP IDS/Intrusion Prevention System (IPS) capability that can monitor all VVoIP signaling and media traffic in decrypted form, or the capability to present all signaling and bearer traffic to an external VVoIP IDS/IPS in a secure manner.

MMD-050080 [**Conditional: MBSS**] [Alarm] If the system supports UC MMD applications, then the VVoIP IDS/IPS threat detection capabilities shall be IAW the VVoIP IDS/IPS functional requirements specified in Section 13, Security Devices. The product shall support the capability to generate and transmit an alarm to the Network Management System (NMS) when these threats are identified.

MMD-050090 [**Conditional: MBSS**] If the product provides the capability to transmit decrypted media and signaling to an external VVoIP IDS/IPS platform, then the product shall, at a minimum, provide FIPS-compliant confidentiality and integrity for this information in a manner that conforms to the cryptographic profiles specified for TLS and IPSec in Section 4, Information Assurance.

MMD-050100 [**Conditional: MBSS**] If the product provides the capability to transmit decrypted VVoIP media and signaling to an external IDS/IPS platform, then this interface shall use publicly accessible specifications and standards.

NOTE: The intent of this requirement is to ensure that third-party IDS/IPS vendors have the information necessary to create an interface that can accept and process the received VVoIP information.

SECTION 9
VIDEO DISTRIBUTION SYSTEM

A Video Distribution System (VDS) is a complement of audio and video equipment designed for interfacing, switching/bridging, and distributing digital and/or analog audio and video signals sourced from multiple devices and destined to multiple devices. Unlike a Video Teleconferencing (VTC) Multipoint Conferencing Unit (MCU), which performs solely many-to-one audio and video signal bridging, the VDS can perform many-to-one, one-to-many, and many-to-many bridging. The VDS can distribute signal feeds to geographically dispersed locations and may include types of "METADATA" that might include intelligence about the feed (e.g., signal feed coordinates, Predator target) or industry standard information such as Extended Display Identification Data (EDID), which is a data structure that provides additional information about the intended display devices.

VDS architectures are composed of sub-systems that may include the following:

1. VDS Distribution Devices (One-to-Many). Includes systems that receive signals sourced from one device which are then repeated to multiple destination devices or video displays.
2. VDS Switching Devices (Many-to-One). Includes systems that receive signals sourced from multiple devices which are then repeated to one destination device or video display. Sources are connected to a common central device that can actively select (switch) between any one of the sourced signals.
3. VDS Matrix Switching Devices (Many-to-Many). Includes systems that receive signals sourced from multiple devices which are then repeated to multiple destination devices or video displays. Sources are connected to a common central matrix device that can actively select (switch) from any source device(s) to one or multiple destination devices simultaneously without compromising signal quality.
4. VDS Peripherals. Normally devices that enable users to interact with the VDS system. They include the following:
    a. Source Devices. Computer workstations, laptop computers, VTC codecs, video playback devices (DVD, Blu-ray, and media players), cable television tuners, and live video camera feeds.
    b. Destination Devices. Desktop monitors, television monitors, video projectors, video signal processors, video recording devices, and video wall signal processor systems.
    c. Control Devices. Keyboards, mice, and other user interface components that enable control of the VDS.
5. VDS Peripheral Connectors. Modular standard components that provide different options for interfacing VDS peripheral devices; they include Multiformat Serial Digital Interface (SDI), Digital Visual Interface (DVI), Video Graphics Array (VGA), High Definition Multimedia Interface (HDMI), and Component HD.

6. VDS Peripheral Connector Conversion Devices. Devices that convert between different types of peripheral connector standards (e.g., HDMI to VGA).
7. VDS Cabling. Includes common copper and optical cabling for passing the electrical signals that enable audio and video, from source devices to destination devices.
8. Analog-to-Digital Converter (ADC) and Digital-to-Analog Converter (DAC). Devices that convert a digital (e.g., binary) code to an analog signal (e.g., current, voltage, or electric charge), and vice versa.

9.1 GENERAL VDS SYSTEM

General VDS configuration requirements apply to all VDS devices in both the Closed VDS system configuration as described in Section 9.2, VDS System, and VDS over Internet protocol (IP) configurations as described in Section 9.3, VDS over IP (VDS-IP).

VDS-000010 [**Required**] The VDS system shall fall into one of two categories:

a. Closed VDS System. These are VDS systems that are inaccessible from Department of Defense (DoD) IP-routed networks. Closed VDS systems shall follow the requirements as specified in Section 9.2, VDS System.

b. VDS over IP (VDS-IP) System. These are VDS systems that are accessible and interface with DoD IP-routed networks. VDS-IP systems shall follow the requirements as specified in Section 9.3, VDS over IP (VDS-IP).

NOTE: This section leverages the DoD Architecture Framework (DoDAF) baseline for a Closed System; therefore, the VDS shall be Closed if the system is inaccessible from external networks such as Non-Secure Internet Protocol Router (NIPR) or Secure Internet Protocol Router (SIPR).

VDS-000020 [Conditional] If the Closed VDS System requires IP-routed control of its Matrix Switch, then the system shall utilize Out-of-Band Management (OBM) in accordance with the Security Technical Implementation Guidelines (STIGs).

VDS-000030 [**Optional**] The VDS system shall have the ability to be controlled from an external master control system.

VDS-000040 [**Optional**] The VDS system shall provide at least one sub-control position with System Administrator permission access control.

9.1.1 IP Requirements for VDS Systems

VDS-000050 [**Optional**] If the VDS system is inaccessible from DoD IP-routed networks, then the VDS system is considered a Closed VDS System, and support of the IPv4 profile as defined in Section 7.2.1.5, Protocols, and of the IPv6 profile as described in Section 5, IPv6, is optional. Otherwise, if the VDS systems connect to IP-routed networks, then the VDS system is

considered a VDS over IP System, and support of the IPv4 profile as defined in Section 5, IPv6, and of the IPv6 profile as described in Section 5, IPv6, is required.

9.1.2 VDS System Signal

VDS-000060 [**Required**] The VDS system shall provide the ability to transfer audio and video signals in a variety of configurations, including, but not limited to, seat console to seat console, seat console to destination display device, seat console to video conversion device, seat console to VTC, and source devices to seat console.

VDS-000070 [**Required**] The VDS system shall be scalable for distributing incoming signal feeds from multiple video sources and shall route to multiple video display receivers as needed by operational requirements.

VDS-000080 [**Required**] The VDS system shall be dynamic, transparent, and capable of understanding the capabilities of the display based on the input source, to provide the necessary equipment resolutions and information required by the peripheral equipment connected.

VDS-000090 [**Required**] The VDS system shall support both analog and digital input signals. This provides the flexibility to support both legacy analog sources and digital displays.

VDS-000100 [**Required**] The VDS system shall provide the ability to display signals from any source device to any compatible destination device, including intermediate display aggregators (e.g., Wall Controllers, Multi-View display processors).

VDS-000110 [**Required**] The VDS system shall maintain native audio and video signals from input interface to output interface without signal degradation, loss of data compression, color sub-sampling, frame rate conversion, auxiliary data loss or signal resolution formatting.

VDS-000120 [**Required**] Any type of signal processing to modify the original audio or video signal information shall be documented and verified by maintenance and/or operator inquiry.

VDS-000130 [**Required**] The VDS system shall be capable of processing and maintaining a minimum of 4:2:2 chroma subsampling in color space, preserving single pixel detail through the encoding, streaming, and decoding processes.

VDS-000140 [**Required**] The VDS system shall support internal scaling to allow the end user to specify different input or output resolutions as required, matching the configuration of installed equipment.

VDS-000150 [**Required**] The VDS system shall utilize VDS Peripheral Connector Conversion (VPCC) devices (Section 9.1.3, VDS System Peripheral) to modify audio and video signals to a single common interface standard for use in the VDS system.

NOTE: Possible applications of this method would convert high-resolution computer graphics DVI interfaces to production television HD-SDI interface formats for switching and distribution. These HD-SDI signaling interface formats are then

typically converted back to DVI or HDMI interfaces for use with common display devices.

VDS-000160 [**Optional**] The VDS system shall provide methods to modify or customize EDID information reported to source devices in order to allow proper configuration of video source devices to match the overall capabilities of the VDS core switching, VDS destination devices, and display devices connected to the VDS system.

VDS-000170 [**Optional**] The VDS system shall provide EDID signaling standard in accordance with the Video Electronics Standards Association (VESA) Enhanced Extended Display Identification, Version 1.3.

9.1.3 VDS System Peripheral

VDS-000180 [**Optional**] VDS Peripherals shall fall into one of two categories:

a. Source Devices. Signal generators that output video, audio and other waveforms which are used in the communication and synchronization of VDS subcomponents, using a signal type that is processed by the VDS Switch system. Examples include computer workstations, laptop computers, VTC codecs, video playback devices (DVD, Blu-ray, and media players), cable television tuners, and live video camera feeds.

b. Destination Devices. Signal receivers that accept the signal from the VDS Switching system; process the video, audio, and other waveforms; and provide the necessary feedback that enables VDS. Examples include Desktop monitors, television monitors, video projectors, video signal processors, video recording devices, and video wall signal processor systems.

NOTE: Some devices, such as VTC codecs and recording devices, may serve as a source and/or destination device.

VDS-000190 [**Optional**] Destination devices shall support scan rates between 23.95 and 85 Hz.

VDS-000200 [**Optional**] Destination devices shall support video input resolutions of: 480i, 525i, 625i, 1080i, 480p, 720p, and 1080p for 50 Hz and 60 Hz progressive and interlaced scan formats.

VDS-000210 [**Optional**] Destination devices shall support video and picture graphics in their native resolution (without any visual artifacts), without additional processing and decoding, to maintain the original native resolution without use of image processing to resize or scale the original signal feed.

9.1.4 VDS Signal Extenders

VDS source and destination devices may be physically separated by long geographical distances that exceed the maximum specifications of the original audio and video signal format. In these

scenarios, the VDS system can utilize signal extenders to convert or condition the original signal for transmission over longer cabling distances.

VDS-000220 [**Required**] VDS Signal Extenders shall condition, amplify, and provide physical media conversion (i.e., copper to fiber optic or coaxial video to video over twisted pair) for audio and video signals to extend the maximum cabling distances from source devices to destination device.

VDS-000230 [**Required**] VDS Signal Extenders shall support, at a minimum, one of the following interconnects: coaxial, twisted pair, or fiber optical.

9.1.5 VDS System Peripheral Connectors

VDS subcomponents interface with one another using peripheral connectors, which are simply modular components that provide different options for interfacing audio and video interface formats and VDS subcomponents. Table 9.1-1, Summary of Connector Types, lists the various connector types.

Table 9.1-1. Summary of Connector Types

CONNECTORS
BNC
DVI
VGA
HDMI
RCA
Fiber (LC, SC, etc.)
Modular Connectors (RJ11, RJ45, 8P8C, etc.)

VDS-000240 [**Conditional**] If the VDS system supports analog VGA and DVI computer connectors, then the following formats shall be supported:

a. High resolution [up to 1920x1200 pixels Wide Ultra eXtended Graphics Array (WUXGA)] computer video resolutions operating at up to 60 Hz vertical refresh rate, or up to165 MHz total un-compressed pixel clock bandwidth.

b. Analog VGA connectors with RGBHV, RGBS, or RGsB coaxial high definition video formats through use of RGBHV to VGA cabling adaptors.

c. DVI connectors compatible with the Digital Display Working Group (DDWG) DVI 1.0 Specification, April 2, 1999.

VDS-000250 [**Conditional**] If the VDS system supports Multi-Rate SDI connectors, then the following Society of Motion Picture and Television Engineers (SMPTE) formats shall be supported:

a. SMPTE 259M: Standard Definition SDI (SD-SDI).

b. SMPTE 344M: Enhanced Definition SDI (ED-SDI).

c. SMPTE 292M: High Definition SDI (HD-SDI).

d. SMPTE 424M: 3-Gbps SDI (3G-SDI).

e. SMPTE 291M: Ancillary Data Packet and Space Formatting.

VDS-000260 [**Conditional**] If the VDS system supports HDMI video connectors and provides support for digital video sources with and without High-Bandwidth Digital Content Protection (HDCP) copy protection, then the following HDMI features shall be supported:

a. High-resolution (up to 1920x1200 pixels WUXGA) computer video resolutions operating at up to 60 Hz vertical refresh rate, or up to165 MHz total un-compressed pixel clock bandwidth.

b. 24-bit color pixel depth and RGB and YCbCr color space.

c. Embedded 2 CH Stereo Uncompressed Pulse Code Modulation (PCM) audio signaling over HDMI interface connections.

VDS-000270 [**Optional**] The VDS system shall support EDID for VGA, DVI, and HDMI connectors. EDID support shall be provided by a VDS connector to describe the capabilities of the VDS system interface to a connected video source device. EDID interface signaling provided by the VDS to the source video device shall include the following:

a. VDS Manufacturer ID.

b. VDS Product Identification.

c. Digital or analog capability of VDS Interface.

d. Supported video resolutions and video timing modes of the VDS system.

e. Preferred video resolution and video timing mode of the VDS system.

9.1.6 VDS Peripheral Connector Conversion Devices

VPCC devices are system appliances that operate and provide gateway like capabilities and allow for different types of VDS subcomponents to interoperate by coupling unlike peripherals.

VDS-000280 [**Required**] VPCCs shall accept, couple, and convert from input to output for connector peripherals as described in Table 9.1-1, Summary of Connector Types.

VDS-000290 [**Required**] VPCCs shall accept high-resolution, up to 1920x1200 pixels WUXGA computer video resolutions, operating at up to 60 Hz vertical refresh rate, or up to165 MHz total un-compressed pixel clock bandwidth.

VDS-000300 [**Required**] VPCCs shall support upwards and downwards video resolution and frame rate signal processing.

VDS-000310 [**Required**] VPCCs shall use video scaling or signal processing to convert between different connector peripherals as described in Table 9.1-1, Summary of Connector Types.

VDS-000320 [**Required**] VPCCs shall allow for dynamic conversion or for user defined conversions to support display resolution formats with varying aspect ratios (4:3, 16:9, and 16:10).

VDS-000330 [**Conditional**] If VPCCs require local monitoring, then VPCCs shall support local HD-SDI/VGA/DVI/HDMI loop-through outputs (as needed for the video source format) for local monitoring.

VDS-000340 [**Required**] VPCCs shall auto-detect the type of peripheral present and provide video peripheral conversion and processing as needed to match the selected video peripheral of the attached video display or VDS subcomponent.

VDS-000350 [**Required**] VPCCs shall support Ethernet management interfaces for diagnostic information and control, including the following:

a. Complete information about the device.

b. Physical identification of hardware and a system error log.

9.1.7 VDS Master Control Switch

VDS-000360 [**Required**] The VDS Master Control switch shall allow the end user to select and verify the processing of any signal displayed.

VDS-000370 [**Required**] The VDS Master Control switch shall be able to perform the following functions on the VDS Matrix Switch:

a. Switch Single Input to Single Output.

b. Switch Single Input to Multiple Outputs.

c. Allow the user to “record” and “recall” presets of crosspoint routings over both the entire switch matrix and selected groupings of inputs and outputs.

VDS-000380 [Optional] The VDS Master Control shall be able to perform the following functions on the VDS Matrix Switch:

d. Switch Single Input to Single Output.

e. Switch Single Input to Multiple Outputs.

f. Enquire the status of any current configuration, by individual output, resulting in the current routed input information; by individual input, resulting in a listing of all current outputs; a master listing of all input names (if stored within the device); and a master listing of all current output assignments.

g. Clear the switching or crosspoint (route "0") based on input, where any output with the selected input will be automatically cleared, or based on output, where only the selected output crosspoints are cleared. Clearing must result in NO INPUT selected rather than using a "blank" or "un-assigned" input.

9.1.8 VDS Matrix Switch

VDS systems connect via a VDS Matrix Switch, which is a device capable of accepting multiple inputs from source devices and selectively distributing any one of these inputs to one or many destination devices.

VDS-000390 [**Required**] The VDS Matrix Switch shall accept original audio and video signals as defined in Section 9.1.2, VDS System Signal, and shall accept multiple connectors as defined in Section 9.1.4, VDS Signal Extenders, to interface to other VDS Matrix Switching Devices, VDS Distribution Devices, VDS Switching Devices, VDS Conversion Devices, and other VDS subcomponents.

VDS-000400 [**Required**] The VDS Matrix Switch shall support hot-swappable expansion modules.

VDS-000410 [**Required**] The VDS Matrix Switch shall support local and remote control management and control.

VDS-000420 [**Required**] The VDS Matrix Switch shall include a local primary control mode that supports a secondary external control mode as needed for redundancy.

NOTE: Best practices indicate a need for backup distributed control systems (dual processors) in any large-scale VDS installation.

VDS-000430 [**Optional**] If the VDS Matrix Switch is slated for specialized missions, the VDS Matrix Switch shall use custom rack mounts (e.g., Ship board operations). Otherwise, the VDS Matrix Switch shall support the industry standard 19-inch wide equipment racks.

VDS-000440 [**Optional**] If the VDS Matrix Switch is slated for mission-critical C2 operations, then the VDS Matrix Switch shall include two or more hot-swappable power supplies with two independent power cords for redundancy.

VDS-000450 [**Optional**] The VDS Matrix Switch shall provide at least one sub-control position with System Administrator permission access control.

9.1.9 VDS IA Security

VDS-000460 [**Required**] All VDS components shall adhere to the appropriate STIGs.

VDS-000470 [**Required**] All VDS components shall meet all appropriate Ports, Protocols, and Services Management (PPSM) guidelines and vulnerability and risk assessments to achieve

compliance for all information systems, applications, and services connected to the Global Information Grid (GIG).

VDS-000480 [**Required**] The VDS shall meet all appropriate Information Assurance (IA) and Vulnerability Assessment (IAVA) and National Institute of Standards and Technology (NIST)/National Information Assurance Partnership (NIAP) standards.

9.1.10 VDS Availability

Availability refers to the ability for the users to access the system, ensuring a prearranged level of operational performance, during a pre-determined contractual measurement period. Generally, the term downtime is used to refer to periods when a system is unavailable.

VDS-000490 [**Required**] The number of UI events shall be no more than 4.38 events per year.

NOTE: UI events are critical service affecting events impairing critical components (i.e., a Matrix Switch as opposed to a Peripheral Device). A UI is any condition identified by a user making the system not operational. Table 9.1-2, Unscheduled Interruption Event Counts, depicts the number of events per system uptime.

Table 9.1-2. Unscheduled Interruption Event Counts

PERCENT OPERATIONAL	PERCENT NON-OPERATIONAL	UI EVENTS/YEAR
99.000	1.000	87.6
99.900	0.100	8.76
99.950	0.050	4.38
99.990	0.010	0.876

VDS-000500 [**Required**] The duration of unscheduled interruption (DUI) events shall be no more than 2 hours per event. Table 9.1-3, Duration of Unscheduled Interruption Events, depicts the number of hours per event per year.

NOTE: An entire system integrity check must be performed for outages lasting longer than 2 hours.

Table 9.1-3. Duration of Unscheduled Interruption Events

UI/YEAR	HR/UI	DUI HRS/YEAR
87.6	4	350.4
8.76	3	26.28
4.38	2	8.76
0.876	1	0.876

VDS-000510 [**Required**] The duration of scheduled outages shall be no longer than 0.5 hours per month and 6 hours per year. Table 9.1-4, Scheduled Maintenance Event Durations, depicts the allowable hourly/yearly durations for scheduled outages.

NOTE 1: Scheduled maintenance is the duration of performing planned maintenance operations in which the system is not available to the user.

NOTE 2: An entire system integrity check must be performed for outages lasting longer than 0.5 hours.

Table 9.1-4. Scheduled Maintenance Event Durations

UI/YEAR	HR/UI	DUI HRS/YEAR
87.6	4	350.4
8.76	3	26.28
4.38	2	8.76
0.876	1	0.876

VDS-000520 [**Required**] All outages or service disruptions to the system shall be correctable within 2 hours using normal maintenance procedures.

9.1.11 VDS Diagnostics

System diagnostics verify and validate proper system operation and system status information.

VDS-000530 [**Required**] The VDS Matrix Switch, VPCCs, and VDS signal Extenders shall provide system diagnostics to verify and validate proper system operation and status.

VDS-000540 [**Required**] The VDS Matrix Switch shall provide complete information about the device, including all software and firmware revisions; type of device; model number; IP address; serial number; ~~Move, Add, Change (~~MAC~~)~~ address; input signal resolution; original signal resolution; physical location of the unit (based on customer input at time of installation); internal temperatures of the unit; fan speed and status of each fan associated with the unit; and an error log pertaining to the unit.

VDS-000550 [~~**Required**~~**Optional**] VPCCs and VDS signal Extenders shall be able to output an internally generated video signal in place of the input signal and an audio tone in place of the incoming audio.

VDS-000560 [**Required**] The VDS Matrix Switch, VPCCs, and VDS signal Extenders shall provide an interface capability to be monitored from a centralized monitoring and diagnostic VDS control location. ~~At a minimum, feedback information shall include signal presence (e.g., connected/disconnected) for coaxial cable, signal format, signal strength (fiber cable only), input/output/matrix card presence and status, power supply status information, fan operation,~~

~~internal operating temperatures, equipment error logging, and power received levels for all VDS cabling (fiber only) and audio/video signals supported by the equipment.~~

VDS-000570 [**Required**] The VDS Matrix Switch, VPCCs, and VDS signal Extenders shall support local and remote control ~~monitoring and remote control monitoring to a third-party interface, to include, at a minimum, feedback information that includes signal presence (e.g., connected/disconnected) for coaxial cable, signal format, signal strength (fiber cable only), input/output/matrix card presence and status, power supply status information, fan operation, internal operating temperatures, equipment error logging, and power received levels for all VDS cabling (fiber only) and audio/video signals supported by the equipment~~.

9.2 CLOSED VDS SYSTEM

A Closed VDS System is considered to be a traditional VDS that enables video distribution over non IP-based networks but can from time to time support IP capabilities in a closed environment. Closed VDS systems can leverage legacy standards, and, by definition, the Unified Capabilities Requirements (UCR) 2013 stipulates that Closed VDS Systems are inaccessible from DoD IP-routed networks.

VDS-000580 [**Required**] Closed VDS Systems shall comply with the General VDS System Requirements as outlined in Section 9.1, General VDS System.

VDS-000590 [**Optional**] Closed VDS Systems shall support the IPv4 profile as defined in Section 7.2.1.5, Protocols, and the IPv6 profile as described in Section 5, IPv6.

VDS-000600 [**Required**] Closed VDS Systems shall interface with a VDS Matrix Switch controller.

VDS-000610 [**Required**] Closed VDS Systems shall support serial RS-232, RS-422, or RS-485 interfaces as required by the system.

VDS-000620 [**Optional**] Closed VDS Systems shall support USB and Ethernet interfaces.

VDS-000630 [**Optional**] Closed VDS Systems shall support a web-based configuration and control.

9.3 VDS OVER IP (VDS-IP)

A VDS-IP is an extension of traditional VDS that enables added features such as enhanced compression procedures that allow for very low latency distribution over an IP transport. VDS-IP leverages standards based Moving Picture Compression Algorithms (MPCAs) and/or Picture Compression Algorithms (PCAs) to enable performance-driven features and advantages over traditional VDS. This approach allows for VDS-IP systems to extend and reach across networking infrastructures where Closed VDS systems have physical and architectural limitations. By definition, the UCR stipulates that VDS-IP systems are accessible from and interface with DoD IP-routed networks.

VDS-000640 [**Required**] VDS-IP Systems shall comply with the General VDS System Requirements as outlined in Section 9.1, General VDS System.

VDS-000650 [**Required**] VDS-IP Systems shall support the IPv4 profile as defined in Section 7.2.1.5, Protocols, and the IPv6 profile as described in Section 5, IPv6.

VDS-000660 [**Optional**] If the VDS-IP system uses standards-based video or picture conversion, compression, and encoding methods, then the VDS system shall be categorized as an Open Distribution VDS System. Otherwise, the system is a Proprietary Distribution VDS System.

a. Open Distribution. This type of VDS-IP system shall use standards-based video or picture conversion, compression, and encoding methods coupled with a STIG and PPSM approved IP transport mechanisms. Audio and video shall be viewable in hardware or software interfaces.

b. Proprietary Distribution. This type of VDS-IP system shall use STIG and PPSM-approved IP transport mechanisms, but is not required to use standards based video or picture conversion, compression and encoding methods.

VDS-000670 [**Optional**] VDS-IP Codecs shall use MPCA and/or PCA formats based on mission objectives.

NOTE: MPCA standards are defined in Section 3.4, UC Audio and Video Conference System.

VDS-000680 [**Required**] Open Distribution VDS-IP systems shall comply with all Unified Capabilities (UC) Audio and Video Conference System Requirements as defined in Section 3.4, UC Audio and Video Conference System.

VDS-000690 [**Required**] Proprietary Distribution VDS-IP systems shall comply with all IP Transport and Proprietary Codec requirements as defined in the UC Audio and Video Conference System Requirements as defined in Section 2.6, SC and SS Failover.

VDS-000700 [**Required**] VDS-IP Systems shall comply with the following PCA formats:

a. JPEG, JPEG2000, VC-1, Dirac, VP8 or other compression codecs based on Discrete Cosine Transform (DCT) or Discrete Wavelet Transform (DWT).

b. PNG.

VDS-000710 [**Required**] VDS-IP subcomponents shall support serial RS-232, USB, or Ethernet.

VDS-000720 [**Required**] VDS-IP systems shall support a web-based configuration and control.

VDS-000730 [**Required**] VDS-IP systems shall interface with a VDS Matrix Switch controller.

9.3.1 VDS-IP Codec

VDS-000740 [**Optional**] VDS-IP shall fall into one of two categories: VDS-IP Hardware Codec or VDS-IP Software Codec.

VDS-000750 [**Required**] VDS-IP Hardware Codecs shall accept computer graphic input resolutions to include VGA, SVGA, XGA, SXGA, SXGA+, UXGA, WUXGA, 1920x1080, and custom computer graphic resolutions and input modes.

VDS-000760 [**Required**] VDS-IP Hardware Codecs shall provide reliable decoding during live configuration changes or selection of new active audio and video data streams (e.g., decoding device does not require restart, resync, or reboot to acquire newly selected data stream).

9.4 VDS RECORDING

VDS recording relates to the capturing and archiving of video and audio, analog or digital signals that are stored for later retrieval in optical disc recording technologies (e.g., DVD, CDs), magnetic storage (e.g., hard drives), flash memory (e.g., memory cards, USB flash drives, solid state drives) or magnetic tape (e.g., video tape, compact cassette).

VDS-000770 [**Required**] VDS Recording Devices shall fall into one of two categories:

a. Video Tape Recorder (VTR). A device that captures and archives video and/or audio material on a magnetic tape (e.g., video tape, compact cassette).

b. Digital Video Recorder (DVR). A device or application software that captures and archives video and/or audio in a digital format to a disk drive, USB flash drive, Standard Definition (SD) memory card, or other local or networked mass storage device.

VDS-000780 [**Required**] VTR Recording Devices shall adhere to the requirements specified in Section 9.4.1, VDS Video Tape Recording (VTR).

VDS-000790 [**Required**] DVR Recording Devices shall adhere to the requirements specified in Section 9.4.2, VDS Digital Video Recording (DVR).

9.4.1 VDS Video Tape Recording (VTR)

VDS-000800 [**Required**] VTR devices shall accept standard and high-definition video using the following SMPTE formats:

a. SMPTE 259M: SD-SDI.

b. SMPTE 344M: ED-SDI.

c. SMPTE 292M: HD-SDI.

d. SMPTE 424M: 3G-SDI.

e. SMPTE 291M: Ancillary Data Packet and Space Formatting.

VDS-000810 [**Optional**] VTR devices shall accept standard and high-definition video using the following SMPTE formats:

a. SMPTE 372M: Dual-Link (DL) HD-SDI.

b. Digital Picture Exchange.

NOTE: The SMPTE defines the standard for many video tape recording (VTR) protocols.

9.4.2 VDS Digital Video Recording (DVR)

VDS-000820 [**Required**] DVR devices shall be capable of recording and replaying video and audio using MPCA and Audio Compression Algorithms (ACAs) as defined in Section 3.4, UC Audio and Video Conference System, and shall be able to capture Picture Compression Algorithms (JPEG and PNG).

VDS-000830 [**Optional**] DVR devices shall be capable of recording and replaying video using MPEG-4 Part 2, MPEG-2 .mpg, MPEG-2 .TS, VOB, and International Organization for Standardization (ISO) video.

VDS-000840 [**Optional**] DVR devices shall be capable of recording and replaying audio using MP3, AC3, and Ogg.

VDS-000850 [**Optional**] DVR devices shall integrate with the monitor and/or TV set.

VDS-000860 [**Optional**] DVR devices shall be VESA compatible.

VDS-000870 [**Optional**] DVR devices shall be able to interface with PC-based compatible devices running Microsoft Windows, Linux, or Mac OS.

SECTION 10
NETWORK INFRASTRUCTURE PRODUCTS

10.1 DISN TERRESTRIAL NETWORK OVERVIEW

Defense Information Systems Network (DISN) services include transport, data, voice, video, messaging, and other Unified Capabilities (UC) along with ancillary enterprise services, such as directories. The DISN services also provides less apparent but critical support services, such as timing and synchronization (T&S), Source Address (SA) of the network, address assignment services, and Domain Name Services.

The requirements are defined around functions. The products defined within this section can be deployed within the DISN or Camp/Post/Station infrastructure. The UC products contained within this section are as follows:

- Optical Transport System (OTS).
- Optical Digital Cross-Connect (ODXC).
- Multi-Service Provisioning Platform (MSPP).
- M13 Multiplexer (M13 Mux).
- Serial TDM Multiplexer (Serial TDM Mux).
- Serial to IP (STI).
- DISN Converged Access (DCA).
- Timing and Synchronization Product (T&S Product).
- DISN Router.

Products within this section may be certified and Approved Products List (APL) listed for one product category (e.g., OTS) or multiple products within the same device (e.g., OTS and ODXC).

10.2 DISN TERRESTRIAL NETWORK FUNCTIONS

The DISN network performs four distinct transport functions and a set of routing functions over fiber plant or leased bandwith. The transport functions are as follows:

- Fiber Plant.
- OTS Function.
- Transport Switching Function (TSF).
- Access Grooming Function (AGF).
- Access Aggregation (AAG) Function.

In addition, the DISN provides T&S for the DISN equipment, and circuits where needed.

The functions are provided by the following equipment suites:

1. Fiber.
2. The OTS Function, which consists of the following functional components:
   a. Optical Line Amplifier (OLA).
   b. End Terminal.
   c. Reconfigurable Optical Add Drop Multiplexer (ROADM).
3. The TSF efficiently packs high bandwidth OC-12/OC-48/OC-192 trunks with Synchronous Transport Signal-1 (STS-1) or STS-Xc channels. Within the current DISN, the Optical Digital Cross-Connect (ODXC) is used to satisfy this function at Class 1 sites and sometimes Class 2 sites.
4. The AGF efficiently packs OC-N and DS3 trunks with Virtual Tributary 1.5 (VT1.5), DS3, or STS-X/STS-Xc channels. It will also convert 1.544 Mbps circuits between the DS1 format and VT1.5 format and extract/pack DS3s with DS1s. Lastly, it will provide timing for DS1 circuits. Within the current DISN, the MSPP provides this function at Class 1 through 3 sites.
5. The AAG Function multiplexes lower speed circuits into higher bandwidth trunks but does not do grooming. This function can be fulfilled by a number of different devices, including the M13 (used in DISN currently) and Serial to IP, which is a future device for DISN.

The requirements that follow for fiber, OTS, and TSF will most often be used by Defense Information Systems Agency (DISA) in the DISN core network, and infrequently by Department of Defense (DoD) services and agencies. The Channel Access functions will be used both by DISA within the DISN for wide area communications and by DoD services and agencies for local or by intra-site level communications. The T&S applies to the DISN Class 1 through 3 sites and at larger DoD service and agency sites. The DISN T&S equipment will sometimes provide that capability to DoD service and agency site equipment.

10.3 REQUIREMENTS

10.3.1 Network Infrastructure (NI)

10.3.1.1 Product Functional

NI-000010 [**Required: OTS**] The OTS shall minimally meet the following requirements:

a. The OTS shall meet all non-optional requirements specified in Section 10.3.2. The OTS may optionally support other functions (TSF, AGF, etc.).
b. The OTS shall minimally meet all Section 4, Information Assurance, Information Assurance (IA) requirements specified for the Local Area Network (LAN) Switch (LS).

When conflicts arise between applicable STIGs and Section 4 LS requirements, the Security Technical Implementation Guideline (STIG) requirements take precedence.

c. The OTS shall meet Section 5, IPv6, IPv6 requirements specified for LS.

NI-000020 [**Required: ODXC**] The ODXC shall minimally meet the following requirements:

a. The ODXC shall meet all non-optional requirements specified in Section 10.3.3 for Transport Switch Function (TSF). The ODXC may optionally support other functions (e.g., AGF).

b. The ODXC shall minimally meet all Section 4 IA requirements specified for LS. When conflicts arise between applicable STIGs and Section 4 LS requirements, the STIG requirements take precedence.

c. The ODXC shall meet Section 5 IPv6 requirements specified for LS.

NI-000030 [**Required: MSPP**] The MSPP shall minimally meet the following requirements:

a. The MSPP shall meet all non-optional requirements specified in Section 10.3.4 for Access Grooming Function (AGF). The MSPP may optionally support other functions (e.g., TSF).

b. The MSPP shall minimally meet all Section 4 IA requirements specified for LS. Whenconflicts arise between applicable STIGs and Section 4 LS requirements, the STIG requirements take precedence.

c. The MSPP shall meet Section 5 IPv6 requirements specified for LS.

NI-000040 [**Required: M13 Mux**] The M13 shall minimally meet the following requirements:

a. The M13 Mux shall meet all non-optional requirements specified in Section 10.3.5.

b. The M13 Mux shall minimally meet all Section 4 IA requirements specified for LS. When conflicts arise between applicable STIGs and Section 4 LS requirements, the STIG requirements take precedence.

NI-000050 [**Required: Serial TDM Mux**] The Serial TDM Mux shall minimally meet the following requirements:

a. The Serial TDM Mux shall meet all non-optional requirements specified in Section 10.3.6.

b. The Serial TDM Mux shall minimally meet all Section 4 IA requirements specified for LS. When conflicts arise between applicable STIGs and Section 4 LS requirements, the STIG requirements take precedence.

NI-000060 [**Required: T&S Product**] The T&S Product shall minimally meet the following requirements:

a. The T&S Product shall meet all non-optional requirements specified in Section 10.4.

b. The T&S Product shall minimally meet all Section 4 IA requirements specified for LS. When conflicts arise between applicable STIGs and Section 4 LS requirements, the STIG requirements take precedence.

c. The T&S Product shall meet Section 5 IPv6 requirements specified for Network Appliance/Simple Server (NA/SS).

NI-000070 [**Required: DISN Router**] The DISN Router shall minimally meet the following requirements:

a. The DISN Router shall meet all non-optional requirements specified in Section 10.6.

b. The DISN Router shall minimally meet all Section 4 IA requirements specified for Router (R). Where conflicts arise between applicable STIGs and Section 4 LS requirements, the STIG requirements take precedence.

c. The DISN Router shall meet Section 5 IPv6 requirements specified for Router (R).

10.3.2 Optical Transport System

10.3.2.1 OTS Description

The OTS multiplexes the optical signals from various sources [i.e., router, TSF, Channel Access Grooming (CAG)] at the optical core site or customer-dedicated signals onto fiber and the transport signals to other optical core sites over the fiber plant. In 2009, OTS system supported 80 point-to-point channels using Dense Wavelength Division Multiplexing (DWDM), where each channel was 10 Gbps. It consists of the following components: Terminal, ROADM, and OLA. There is an optical supervisory channel (OSC) that runs between these elements. The terminal is composed of two elements: the transponder and the muxponder.

Definitions of terms in this section can be found in UC Framework 2013, Appendix C, Glossary and Terminology Description.

This section is organized as follows:

- Requirements applicable to all OTS elements.
- OLA.
- Muxponder element within the terminal.
- Transponder element within the terminal.
- ROADM.
- Requirements applicable to both transponder and ROADM.
- OSC.

10.3.2.2 Requirements Applicable to All OTS Products

10.3.2.2.1 Overall

NI-000080 [**Required**] The OTS shall support a minimum of 40 International Telecommunications Union – Telecommunication (ITU-T) Recommendation G.694.1 grid wavelengths per line-side optical fiber.

NI-000090 [**Optional**] The OTS shall support a minimum of 160 ITU-T Recommendation G.694.1 grid wavelengths per line-side optical fiber.

NI-000100 [**Required**] The OTS shall support mixed bit rate signals of 10 Gbps.

NI-000110 [**Optional**] The OTS shall support mixed bit rate signals of 40 Gbps and 100 Gbps.

NI-000120 [**Required**] The OTS shall use the ITU-T specified OSC for out-of-band management communication.

NI-000130 [**Required**] The OTS shall support all specified wavelengths for all specified bit rate and signal formats.

NI-000140 [**Required**] The OTS shall support standard single mode fiber in accordance with (IAW) ITU-T Recommendation G.652, and ITU-T Recommendation G.655.

NI-000150 [**Required**] The OTS shall support the ability of forty 10-Gbps wavelengths to traverse a minimum of five ROADMs using fibers specified previously for a minimum reach of 2,000 km without regeneration [optical-to-electrical-to-optical (OEO) conversion] at a Bit Error Rate (BER) of less than 1×10^{-15}.

NI-000160 [**Optional**] The OTS shall support the ability of forty 40-Gbps wavelengths to traverse a minimum of five ROADMs using fibers specified previously for a minimum reach of 1,500 km without regeneration (OEO conversion) at a BER less than 1×10^{-15}.

NI-000170 [**Optional**] The OTS shall support the ability of forty 100-Gbps wavelengths to traverse a minimum of five ROADMs using fibers specified previously for a minimum reach of 1,200 km without regeneration (OEO conversion) at a BER less than 1×10^{-15}.

NI-000180 [**Required**] The OTS shall support span length up to 150 km and span loss up to 50 dB. The reach shall not be limited by OSC performance.

NI-000190 [**Required**] The OTS shall allow the remote configuration of wavelengths added or dropped from the system.

NI-000200 [**Required**] Client interfaces available on the OTS shall meet the accepted standards or specifications for the interface (e.g., OC-192 Telcordia Technologies GR-253-CORE standards, Synchronous Transport Module [STM]-16 and STM-64 ITU-T Recommendations

G.707 standards, and Gigabit Ethernet [GbE] and 10GbE Institute of Electrical and Electronics Engineers [IEEE] 802.3 standards).

NI-000210 [**Required**] The OTS shall support remote shelf location with up to 6 dB optical power budget between terminal and remote locations.

NI-000220 [**Required**] The OTS shall support universal (or single part code) MUX/demultiplexer (DEMUX) circuit-packs at all terminals and ROADM nodes.

NI-000230 [**Required**]. The OTS shall enable pre- and post-dispersion compensation options at all nodes (terminals, ROADMs, and OLAs).

NI-000240 [Required] When one or more channels fail or are removed, the remaining channels shall not experience increased bit errors or loss of operating margin.

NI-000250 [Required] When failed channels are restored or new channels are added, the existing channels shall not experience any transient or long-term performance deterioration.

10.3.2.2.2 Performance

NI-000260 [**Required**] Jitter tolerance shall be in compliance with Telcordia Technologies GR-253-CORE (Issue 4, December 2005) Type II and ITU-T Recommendation G.958.

NI-000270 [**Required**] Jitter transfer shall comply with Telcordia Technologies GR-253-CORE (Issue 4, December 2005) and ITU-T Recommendation G.958.

NI-000280 [**Required**] In a single vendor environment, a wavelength shall traverse up to at least 20 transponders before termination before the signal requires regeneration (O-E-O) at a terminal or OADM site. This shall be true for all data rates specified.

NI-000290 [**Required**] The OTS shall tolerate a persistent input channel signal timing deviation of at least +/- 20 parts per million (ppm). This implies that the OTS must (1) operate properly in normal condition (i.e., without alarms) when any or all tributaries have long-term frequency offsets of up to +/- 20 ppm and (2) maintain the system performance objectives for concatenated OTS systems.

NI-000300 [**Required**] When a signal passes through concatenated OTS sections, the output jitter shall not exceed the network interface limits of ITU-T Recommendation G.825.

NI-000310 [**Required**] When one or more channel (up to 90 percent) fails or is removed (either instantaneously or sequentially), the remaining channels shall not experience increasing bit errors or loss of operating margin. In addition, when failed channels are restored or new channels are added, the existing channels shall not experience any transient or long-term performance deterioration.

NI-000320 NI-000300 [**Optional**] The maximum uncompensated Phase Modulation-Demodulation (PMD) that the system can tolerate at 40/100 Gbps shall not exceed that tolerated at 10 Gbps.

10.3.2.2.2.1 Reliability and Quality Assurance

NI-000330 [**Required**] The OTS equipment shall meet the following quality program requirements, unless specifically overridden or modified by another requirement in this document:

- Telcordia Technologies GR-282-CORE.
- Telcordia Technologies GR-2911-CORE.
- Telcordia Technologies TR-NWT-000179.
- Telcordia Technologies TR-NWT-000418.
- Telcordia Technologies SR-NWT-002419.

NI-000340 [**Required**] A list shall be available of country of origin of the critical components as well as final assembly location of the system.

10.3.2.2.3 Common Physical Design

NI-000350 [**Required**] Each OTS element, shelf, or circuit pack, whichever is the smallest independent load device of the OTS element, shall obtain power from two completely independent power units. Furthermore, the return path from the power units shall remain completely independent (Telcordia Technologies TR-NWT-000295). If one of the power units fails, then an alarm shall be generated and the load shall be carried by the other unit without manual intervention and without interruption of service or functionality. The other power unit shall support the operation of the element, shelf, or circuit pack until the problem with the faulty unit is corrected.

NI-000360 [**Required**] All OTS elements shall conform to the spatial and environmental criteria specified in Telcordia Technologies FR 796 and GR-63-CORE.

NI-000370 [**Required**] All OTS elements shall demonstrate an operational availability of all functions and services of 99.999 percent.

NI-000380 [**Required**] All OTS elements shall comply with the earthquake, office vibration, and transportation vibration criteria specified in Telcordia Technologies GR-63-CORE, Section 4.4, Earthquake, Office Vibration, and Transportation Vibration.

NI-000390 [**Required**] All OTS elements shall be fully Network Equipment-Building System (NEBS), Level 3 compliant.

NI-000400 [**Required**] All OTS elements shall meet the environmental conditions described in Telcordia Technologies GR-63-CORE.

NI-000410 [**Required**] All OTS elements shall meet the environmental conditions described in European Telecommunications Standards Institute (ETSI) 300 019.

NI-000420 [**Required**] All OTS elements shall be designed to operate in a communication equipment environment, adjacent to or in the vicinity of others types of equipment that may include digital radio equipment, fiber optic terminal equipment, frequency-division multiplexing (FDM) analog microwave, very high frequency (VHF)/ultra high frequency (UHF) base stations, satellite ground terminals, transfer trip and power line carrier equipment, and telephone signaling equipment.

NI-000430 [**Required**] All OTS elements shall meet the electromagnetic compatibility (EMC)/electromagnetic interference (EMI) requirements defined in Telcordia Technologies GR-1089-CORE.

NI-000440 [**Required**] All OTS elements shall meet the EMC/EMI requirements defined in Federal Communications Commission (FCC) Part 15 Class A.

NI-000450 [**Required**] All OTS elements shall meet the EMC/EMI requirements defined in ETSI EN 50082.

NI-000460 [**Required**] All OTS elements shall meet the EMC/EMI requirements defined in ETSI EN 55022.

NI-000470 [**Required**] All OTS elements shall meet the EMC/EMI requirements defined in ETSI EN 300-386.

NI-000480 [**Required**] All OTS elements shall be designed to operate continuously in the following environment ranges without degradation: Temperature: 0 to +50°C; Humidity: 5 to 95 percent relative humidity, without condensation.

NI-000490 [**Required**] All OTS elements shall be designed to be fully operational after transportation and/or storage in the following environment ranges: Temperature: -40 to +70°C; Humidity: 5 to 95 percent relative humidity, without condensation.

NI-000500 [**Required**] All OTS elements shall be designed to operate continuously in the following environment range without degradation: Altitude: -100 to 15,000 ft above mean sea level (AMSL).

NI-000510 [**Required**] All OTS elements shall adhere to NEBS Level 3 compliance standards for acceptable voltage ranges, EMI, and electrostatic discharge (ESD) safety and shall be operable using standard 48V direct current (dc) power as well as having redundant isolated power input feeds. For certain sites, an alternative alternating current (ac)/dc rectifier may need to be supplied to power the system and shall be able to switch 110/220V with redundant isolated power modules.

NI-000520 [**Required**] All OTS elements shall be fully operational throughout the battery voltage range of -41.5 to -56V dc (VDC).

NI-000530 [**Required**] All OTS elements shall not be damaged and recover to normal performance following application of the following maximum transient voltages for the durations given (nominal voltage 48 VDC): 75 VP-P for 1 ms, 60 VP-P for 500 ms.

NI-000540 [**Required**] All OTS elements in the transport layer primary operating system interface shall provide the capability for reporting alarms of external equipment and general housekeeping alarms. A minimum of 16 user-defined alarms shall be provided, with the option to expand to 32 user-defined alarm points. Capability shall be provided for a minimum of 8 user-defined remote control points for external functions. This capability shall be provided by relays, not Transistor-Transistor Logic.

NI-000550 [**Required**] The OTS shall support having all data cross connects stored locally and redundantly, and being automatically restored without user intervention, in the case of failure, within a period of 5 minutes.

NI-000560 [**Required**] The OTS shall provide the capability to roll back to the previous operational version of software without service impact on in-service channels.

NI-000570 [**Required**] The OTS shall conform to memory administration, and system administration and security standards as documented (Telcordia Technologies GR-472-CORE and GR-253-CORE Issue 4, December 2005).

NI-000580 [**Required**] The OTS shall support software upgrades that directly use or translate the previous versions configuration database.

NI-000590 [**Optional**] The software of the OTS shall be designed and upgraded in a modular fashion so that an entire code does not have to be replaced when a portion is upgraded.

NI-000600 [**Required**] The OTS shall be designed with an accessible file system to allow for multiple versions of software, logs, and file manipulation or integrity checks to be performed before upgrading or downgrading software and/or firmware.

NI-000610 [**Required**] All equipment shall have been tested and registered as compliant to the following electrical safety standards: UL-1950, EN60950, and International Electrotechnical Commission (IEC) 60950.

10.3.2.2.4 Protection and Restoration

NI-000620 [**Required**] The OTS shall support 1+1 wavelength protection and restoration.

10.3.2.3 Optical Amplifier

The OTS shall support OLAs that meet the following requirements:

NI-000630 [**Required**] The total optical power emitted from the OTS to be coupled into the fiber shall not exceed the power limit of IEC Class 3B (+27 dBm).

NI-000640 [**Required**] The OTS shall monitor and report on the operation of the Raman pumping lasers including power on, off, optical output power, operating current, and total optical return loss (ORL).

NI-000650 [**Required**] After detecting the failure of Raman pumping lasers, the OTS shall generate an alarm, but shall not shut off the system.

NI-000660 [**Required**] The OTS shall have an integrated power management algorithm, which invokes power monitoring and adjustment devices to compensate for power variations across the optical wavelengths.

NI-000670 [**Required**] The OLA system shall be able to balance individual wavelengths so that power output levels exhibit less than 0.5 dB variance from the mean output level without remote or direct intervention from a network operator.

NI-000680 [**Required**] The power management algorithm shall cause no interruptions in OSC communications at any time.

NI-000690 [**Required**] The OSC signals shall experience no increased errors at any time up to End of Life (EOL), including during wavelength provisioning or line equalization.

NI-000700 [**Required**] Amplifiers shall require less than 1 ms to return all wavelength power output levels to within 1 dB of preinsertion/drop levels; transient suppression statistics shall be provided for OLA systems.

NI-000710 [**Required**] The OLA shall maintain safe (Hazard Level 1) system operation in the event of input signal loss or fiber cut.

NI-000720 [**Required**] Chromatic dispersion compensation shall be able to fully compensate a 150 km span for each fiber type.

NI-000730 [**Required**] Chromatic dispersion compensation shall be provided for different fiber lengths in 10, 20, or 30 km increments, if the technique requires the compensation to be periodically dispersed.

NI-000740 [**Required**] The OTS shall enable pre- and post-dispersion compensation options.

NI-000750 [**Required**] A secured external monitor port is required at each OA. For devices that contain a full-featured internal Optical Spectrum Analyzer (OSA), an external monitor port shall still be required.

NI-000760 [**Optional**] Internal OSA functionality shall support 25 GHz ITU grid spacing with a minimum 5 percent wavelength accuracy.

NI-000770 [**Optional**] Internal OSA functionality shall provide a minimum accuracy of 0.2 dB for each wavelength.

NI-000780 [**Optional**] Internal OSAs shall provide sweep times of less than 1 second.

NI-000790 [**Optional**] Internal OSAs shall provide the ability to display all wavelengths simultaneously.

NI-000800 [**Optional**] Internal OSAs shall provide the ability to retrieve data to be stored at a remote storage site.

NI-000810 [**Optional**] Internal OSAs shall provide the ability to view various calculated data, such as gain tilt, output tilt, gain variation, gain difference, noise level, total received power, and total launched power.

NI-000820 [**Optional**] Internal OSAs shall provide the ability to report Quality (Q) factor (not critical).

NI-000830 [**Optional**] Internal OSAs shall have the ability to estimate Optical Signal to Noise Ratio (OSNR) for each wavelength.

NI-000840 [**Optional**] All measurements made available at the internal OSA shall be available at the external OSA port.

10.3.2.3.1 OLA Physical Design

NI-000850 [**Required**] The OLA shall support hot swappable modular components including, but not limited to, fans, amplifier modules, in-band/out-of-band management interfaces, power supplies, and control processor.

NI-000860 [**Required**] The OLA shall support redundant fans, management interfaces, power supplies, and control processors.

NI-000870 [**Required**] The OA shall be able to fit in either a standard 19-inch or a 23-inch rack with depth no greater than 30 inches and height no more than 84 inches.

NI-000880 [**Required**] The OLA power consumption shall be kept below 2000 watts for all equipment at an OLA site.

NI-000890 [**Required**] The vendor shall identify its OLA power and space requirements for all specified configurations.

NI-000900 [**Required**] The loss of one or more provisioned OC-192/STM-64 inputs to a 4:1 10G multiplexer shall not affect the performance of any other provisioned OC-192/STM-64 on that multiplexed channel.

10.3.2.4 Transponder

The OTS shall support transponders. The minimum requirements for OTS transponders are as folows:

NI-000910 [**Required**] Transponders shall comply with the DWDM wavelength grid as specified in ITU-T Recommendation G.694.1.

NI-000920 [**Required**] Transponders shall support tunable lasers, which are tunable over whole band.

NI-000930 [**Optional**] All transponders shall support a built-in self BER test function.

NI-000940 [**Required**] All transponders shall support local and remote loopback capability on the line side for a built-in self BER test.

NI-000950 [**Optional**] All transponders shall support total end to end signal propagation delay (at transponder ingress to egress) reporting function.

NI-000960 [**Required**] All transponders shall support user selectable line side Forward Error Correction (FEC); i.e., no FEC, ITU-T Recommendation G.709-compliant standard FEC or Super FEC, enhanced FEC (EFEC), and vendor proprietary modes.

NI-000970 [**Required**] Transponders shall support ITU-T Recommendation G.709 specifications for OTN services.

NI-000980 [**Required**] Transponders shall support switching of framing protocols (OTN, SONET, 10GbE) without requiring downloading or switching of firmware or software, and physical removal of the transponder from the slot.

NI-000990 [**Required**] Transponders shall have non-intrusive SONET/SDH B1 monitoring capability.

NI-001000 [**Optional**] Transponders shall have integrated Electronic Dispersion Compensation (EDC) for all specified fiber types to support minimum unregenerated reach of 2000 km.

NI-001010 [**Required**] The vendor shall supply through-transponder(s) to eliminate unnecessary back to back Optical/Electrical (O/E) conversions for wavelength regeneration at ROADM, optical cross-connect (OXC), and regenerator sites.

NI-001020 [**Required**] The vendor shall provide a transponder to interface with 10 Gbps unframed wavelength services.

NI-001030 [**Required**] A transponder shelf shall support all types of transponders, or a combination of them. No slot shall be bit-rate specific.

NI-001040 [**Required**] There shall be no human intervention, including: manual wavelength tuning or power equalization via external attenuators after adding transponders.

NI-001050 [**Required**] Transponders shall support all wavelengths and required transmission rates with a minimum reach of 2000 km without OEO regeneration on all specified fiber types (ITU-T Recommendations G.652, G.655).

10.3.2.4.1 Interface

NI-001060 [**Required**] Transponders shall support an OC-192/STM-64 interface.

NI-001065 [**Required**] Transponders shall support an OC-768/STM-256 or OTU3 (ITU-T Recommendation G.709 interface.

NI-001070 [**Required**] Transponders shall support a 10GbE Wide Area Network (WAN) physical layer (PHY) interface.

NI-001080 [**Required**] Transponders shall support a 10GbE LAN PHY interface.

NI-001090 [Required] The transponders shall support SR, Long Reach (LR) (LR-1, LR-2, LR-3), and Intermediate Reach (IR) (IR-1, IR-2), client interface types per Telcordia Technologies GR-253-CORE.

NI-001100 [Required] The transponders shall support client interfaces at 1310 nm. The Transponder may optionally support 1550 nm.

10.3.2.5 ROADM

The OTS shall support ROADM. The minimum OTS ROADM requirements are as follows:

NI-001110 [**Optional**] The ROADM shall be capable of supporting a minimum of four network-side interfaces and perform both optical bypass and adds and drop functions.

NI-001120 [**Optional**] The ROADM shall support directionless wavelength routing.

NI-001130 [**Optional**] The ROADM shall be capable of colorless wavelength routing.

NI-001140 [**Required**] The system shall support cascading of a minimum of five ROADMs for a total unregenerated reach of 2000 km.

NI-001150 [**Required**] Any wavelength not explicitly dropped or added shall be passed through the ROADM.

NI-001160 [**Required**] It shall be possible to reuse wavelength at ROADM.

NI-001170 [**Required**] There shall be no restrictions on ADD/DROP and EXPRESS (pass through) wavelengths at ROADM site.

NI-001180 [**Required**] The ROADM shall be capable of supporting dynamic wavelength selection without precabling being required.

NI-001190 [**Required**] The ROADM shall be capable of dropping all wavelengths from each of eight line-side fiber connections to tributary-side optics.

NI-001200 [**Required**] The ROADM shall be capable of adding all wavelengths to each of eight line side fiber connections from tributary side optics.

NI-001210 [**Required**] The ROADM shall be capable of dropping any specific wavelength, independent of other wavelengths to be dropped.

NI-001220 [**Required**] The ROADM shall be capable of adding any specific wavelength, independent of other wavelengths to be added.

NI-001230 [**Required**] The activation of additional services on interfaces in the ROADM shall be non-service affecting to existing traffic and shall not cause any increase in bits errors.

NI-001240 [**Required**] The deletion of active services on interfaces in the ROADM shall be non-service affecting to the remaining traffic and shall not cause any increase in bits errors.

NI-001250 [**Required**] Hardware upgrades of the ROADM to support higher tributary interface density shall not disrupt operational traffic.

NI-001260 [**Required**] Hardware upgrades of the ROADM to support higher line interface density shall not disrupt operational traffic.

NI-001270 [**Required**] The ROADM shall provide a latching capability. (Latching is the ability of the ROADM to maintain its current state in the event of power failure.)

NI-001280 [**Optional**] The ROADM shall provide an optical multicasting capability. (Multicasting is the ROADM's ability to allow one input wavelength to be duplicated on multiple output tributary and line ports).

NI-001290 [**Required**] The ROADM shall support dynamic per-wavelength power leveling.

NI-001300 [**Required**] The addition or deletion of a wavelength service on the ROADM shall not cause an increase in BER or data loss on other wavelengths.

NI-001310 [**Required**] The ROADM shall not incur increased bit errors associated with wavelength provisioning or line equalization.

NI-001320 [**Required**] The failure of an upstream line system shall not cause the ROADM to increase in BER or lose data on the remaining active wavelengths.

NI-001330 [**Required**] The OSNR penalty for any signal passing through a ROADM shall be less than 0.5 dB.

NI-001340 [**Required**] The system is required to automatically redirect working paths to available spare fibers or wavelengths in the event of a primary path failure. The ROADM shall

not inhibit ring or linear protection switching initiated by an ODXC, MSPP, or other electronic device.

NI-001350 [**Required**] The ROADM shall support a 1+1 protection functionality with fully diverse routing. The ROADM shall not inhibit ring or linear protection switching initiated by an ODXC, MSPP, or other electronic device.

NI-001360 [**Required**] The ROADM shall support redirection of light paths via the Electronic Message System (EMS)/Network Management System (NMS).

NI-001370 [**Required**] The ROADM shall support linear protection topologies. The ROADM shall not inhibit ring or linear protection switching initiated by an ODXC, MSPP, or other electronic device.

NI-001380 [**Required**] The ROADM shall support ring protection topologies. The ROADM shall not inhibit ring or linear protection switching initiated by an ODXC, MSPP, or other electronic device.

10.3.2.5.1 ROADM Specific Physical Design

NI-001390 [**Required**] The vendor shall comply with all requirements listed in General Physical Requirements of this document. The vendor shall list all discrepancies.

NI-001400 [**Required**] The ROADM shall support hot swappable modular components including, but not limited to, fans, switch fabric, interface ports, power supplies, and control processor.

NI-001410 [**Required**] The ROADM shall support redundant fans, switching fabrics, power supplies, and control processors.

NI-001420 [**Required**] The fully configured ROADM (excluding the transponder shelves) shall not exceed one full 84-inch racks.

NI-001430 [**Required**] The fully configured 80 channel capable ROADM with 100% add/drop shall not exceed six full 84-inch racks.

NI-001440 [**Required**] The ROADM shall not require contiguous rack locations. The vendor shall describe the distance limitations when the racks are not contiguous.

NI-001450 [**Required**] The ROADM weight shall be so that the device can be mountable in a standard Telco rack or secure cabinet with standard rack screws and shall not require unusual hardware.

10.3.2.6 Requirements Common to Transponder and ROADM

10.3.2.6.1 Framed Formats

NI-001460 [**Required**] The OTS shall support the transport of the following SONET/SDH services: OC-192/STM-64.

NI-001465 [**Required**] Framed wavelength services shall be supported for 40 (ITU-T Recommendation G.709) and 100 Gbps (OTU4 (ITU-T Recommendation G.709 standard) signals.

NI-001470 [**Required**] The OTS shall support the transport of the following Ethernet services: 10GbE WAN PHY and 10GbE LAN PHY.

NI-001480 [**Required**] The OTS shall be transparent to the bit pattern of all optical channels (i.e., the OTS shall not modify the payload bit pattern of any signal that traverses it).

NI-001490 [**Optional**] The OTS shall support, in hardware and in software, the possibility to feed a specified ITU-T grid wavelength, with undefined framing, directly into the multiplexer through a "colored interface" that shall verify the wavelength and power levels (commonly known as alien wavelength) and to identify other characteristics of the tributary signal required to be known and monitored for proper OTS system operation with such tributary signals.

NI-001500 [**Required**] "Alien wavelength" regeneration shall be supported.

10.3.2.6.2 Unframed Formats

NI-001510 [**Required**] The OTS shall support unframed wavelength services (within previously specified interface rates).

NI-001520 [**Required**] The OTS shall support mixed framed and unframed wavelength services.

10.3.2.7 Optical Supervisory Channel

The OTS shall include an OSC linking the two OTS Gateway NEs (GNEs), with access at each OTS OLA site. All telemetry, data, and voice traffic originating at OTS OLA sites shall be routed over this service channel. A diagram of the OSC appears in Figure 10.3-1, Optical Supervisory Channel.

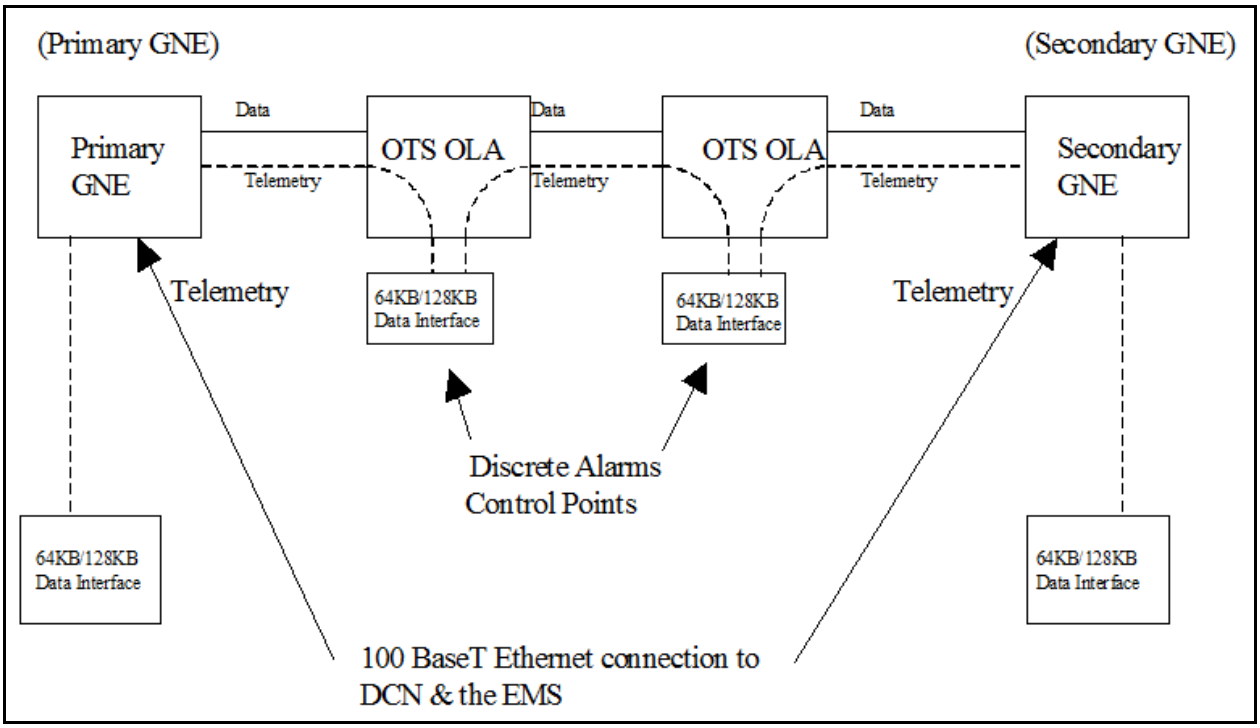


Figure 10.3-1. Optical Supervisory Channel

NI-001530 [**Required**] The OLA, ROADM, and end terminal (ET) elements shall terminate or insert an OSC with a wavelength that adheres to ITU-T specifications.

NI-001540 [**Required**] The OLA, ROADM, and ET elements shall use the ITU-T-specified OSC for out-of-band management communications.

NI-001550 [**Required**] The OLA, ROADM, and ET elements shall use the same OSC wavelength.

NI-001560 [**Required**] The internal diagnostics for OLA, ROADM, and ET elements shall report OSC failure.

NI-001570 [**Required**] It shall be possible to turn up and sustain transmission between two nodes in the absence of an OSC.

NI-001580 [**Required**] The OLA, ROADM, and ET elements shall report any OSC channel input/output failure (via out-of-band Data Communications Network [DCN]).

NI-001590 [**Required**] The OLA, ROADM, and ET elements shall report any OSC channel BER threshold violation.

NI-001600 [**Required**] The OLA, ROADM, and ET elements shall provide OSC interfaces that allow for interoperability with all adjacent equipment within the optical network (i.e., wavelength, modulation, protocol) from the same vendor.

NI-001610 [**Required**] The OSC shall be able to operate error free across 150 km of each specified fiber type with a span loss of 50 dB at the OSC frequency or wavelength. The span loss shall not be inclusive of the OSC insertion loss.

NI-001620 [**Required**] The OSC circuit pack shall report optical span loss between two adjacent nodes.

NI-001630 [**Required**] The OSC shall operate at 2 Mbps or higher data rates.

NI-001640 [**Required**] Architecturally, the OSC shall be passively optically and separated from the transport optical signals immediately after input connection of the OTS.

10.3.2.8 OTS Standards Compliance

The standards in effect when the equipment was first acquired are listed. Updates to the standards since that point in time are identified in brackets. When the manufacturer provides new components for the commercial off-the-shelf (COTS) items to the same device that satisfy updated standards, DISA will often purchase and install those components to accommodate growth, but will not replace existing components unless there is another reason to do so. As such, components will be operational within DISN that satisfy multiple versions of the standards. Testing will need to be undertaken using the standard release that applied to that component, when the revised standard cannot be satisfied by the original component.

NI-001650 [**Required**] ITU-T Recommendation G.652 (10/2000) (2005).

NI-001660 [**Required**] ITU-T Recommendation G.655 (10/2000) (2006).

NI-001670 [**Required**] ITU-T Recommendation G-694.1 (2002).

NI-001680 [**Required**] ITU-T Recommendation G.709/Y.1331.

NI-001690 [**Required**] ITU-T Recommendation G.825 (2000).

NI-001700 [**Required**] ITU-T Recommendation G.958 (1994), Digital Sections and Digital Line Systems.

NI-001710 [**Required**] Telcordia Technologies GR-63-CORE, Issue 1, October 1995 (Issue 3, March 2006).

NI-001720 [**Required**] Telcordia Technologies TR-NWT-000179, Issue 2, June 1993.

NI-001730 [**Required**] Telcordia GR-253-CORE, Issue 3, September 2000 (Issue 4, December 2005).

NI-001740 [**Required**] Telcordia Technologies GR-282-CORE, December 1997 (Issue 4, July 2006).

NI-001750 [**Required**] Telcordia Technologies TR-NWT-000295, Issue 2, July 1992.

NI-001760 [**Required**] Telcordia Technologies NWT-000418, December 1999.

NI-001770 [**Required**] Telcordia Technologies GR-472-CORE, Issue 2, November 1996.

NI-001780 [**Required**] Telcordia Technologies FR-796, Reliability and Quality Generic Requirements, Issue 5, April 2008.

NI-001790 [**Required**] Telcordia Technologies GR-1089-CORE, Issue 2, Revision 1, February 1999 (Issue 4, June 2006).

NI-001800 [**Required**] Telcordia Technologies SR-NWT-002419, Issue 1, 1992.

NI-001810 [**Required**] Telcordia Technologies GR-2911-CORE, 1995.

NI-001820 [**Required**] ETSI ETS 300 019, 1994.

NI-001830 [**Required**] ETSI ETS-FN-50022.

NI-001840 [**Required**] ETSI EN 50082.

NI-001850 [**Required**] ETSI EN 300 386.

NI-001860 [**Required**] British Standards Institution (BSI) EN 60950-1, August 6, 2006.

NI-001870 [**Required**] IEC 60950-1, 2006.

NI-001880 [**Required**] Code of Federal Regulations (CFR) FCC Part 15, Class A.

NI-001890 [**Required**] Network Equipment - Building System (NEBS), Level 3.

NI-001900 [**Required**] Underwriters Laboratories, Inc. (UL)-1950, Standard for Safety, Information Technology Equipment Including Electrical Business Equipment, First Edition 1989.

NI-001910 [**Required**] Electronic Industries Alliance (EIA) 310C.

10.3.3 Transport Switch Function

10.3.3.1 Description

The ODXC will minimally support the following requirements for TSF functionality. The ODXC is a cross-connect device that is located primarily at Class 1 sites, but it could also be deployed at select Class 2 sites.

At minimum, ODXC fabric will support STS-1 granularity. ODXC could also provide VT1.5 granularity switching.

10.3.3.2 TSF SONET/SDH Interface

NI-001920 [**Required**] The TSF shall support SDH or SONET on any combination of ports or port cards.

NI-001930 [**Required**] It shall be possible to use any port on the systems as network-side interfaces or tributary-side interfaces.

NI-001940 [**Required**] The TSF shall provide optical interfaces for OC-192, OC-48, OC-12, and OC-3 signals consistent with the SR-1, IR-1, IR-2, LR-1, LR-2, and LR-3 application specifications of Telcordia Technologies GR-253-CORE, Section 4.

NI-001950 [**Optional**] The TSF shall provide optical interfaces for OC-768 signals consistent with the SR-1, IR-1, IR-2, LR-1, LR-2, and LR-3 application specifications of Telcordia Technologies GR-253-CORE, Section 4.

NI-001960 [**Required**] The TSF shall provide optical interfaces for STM-64, STM-16, STM-4, and STM-1 signals consistent with the application codes I-n, S-n.x, and L-n.x in ITU-T Recommendation G.957. There should be no differences between single-channel optical interfaces for SONET terminations according to Telcordia Technologies GR-253-CORE and the level-comparable SDH optical interfaces specified in ITU-T Recommendation G.957-CORE.

NI-001970 [**Optional**] The ODXC may optionally support STM-256.

NI-001980 [**Required**] The TSF shall support the SR-1 interface and at least one of the IR-1, IR-2, or IR-3 interface for OC-3, OC-12, OC-48, and OC-192 signals consistent with the requirements in this document.

NI-001990 [**Optional**] The TSF shall support the SR-1 interface and at least one of IR-1, IR-2, or IR-3 interface for OC-768 signals consistent with the requirements elsewhere in this document.

NI-002000 [**Required**] The TSF shall support the Intra- office (I-x) interface and any Short-haul (S n.x) interface for STM-1 (if supported), STM-4, STM-16, and STM-64 signals consistent with the requirements in this document. The ODXC may support STM-256.

NI-002010 [**Optional**] The OC-192 SONET/STM-64 interfaces shall support Very Short Reach (VSR) optics as defined in ITU-T Recommendation G.693.

NI-002020 [**Required**] The TSF shall support the capability to provide physical loopback toward the line side and cross-connect matrix for all supported interfaces.

10.3.3.3 TSF Ethernet Interface

NI-002030 [**Required**] The TSF shall provide interfaces for GbE Services in conformance with the IEEE 802.3 for Ethernet LAN interfaces. The Logical Link Interworking Function (IWF)

shall terminate the Media Access Control (MAC) layer of Ethernet as described in the Ethernet Standard IEEE 802.3.

NI-002040 [**Optional**] The TSF interfaces shall include 100 GigE consistent with the application specifications of IEEE 803.

NI-002050 [**Required**] The TSF shall provide interfaces for 10GigE Services in conformance with the IEEE 802.3ae for Ethernet WAN PHY interfaces. The Logical Link IWF shall terminate the MAC layer of Ethernet as described in the Ethernet Standard IEEE 802.3.

NI-002060 [**Required**] The GigE interfaces shall accommodate Ethernet packets greater than 4470 bytes.

NI-002070 [**Required**] The 10GbE interfaces shall accommodate Ethernet packets greater than 4470 bytes.

NI-002080 [**Required**] The TSF shall be able to provision, monitor, and detect faults on, and restore GbE services in a standardized and automated fashion.

NI-002090 [**Required**] The TSF shall be able to provision, monitor, and detect faults on, and restore 10GbE services in a standardized and automated fashion.

NI-002100 [**Optional**] The TSF's Ethernet services shall support both port-based and flow-based Virtual LANs (VLANs) for multiple rates and customer interfaces as defined by IEEE Standard 802.1Q-1998, Virtual Bridged Local Area Networks.

NI-002110 [**Required**] The TSF shall not, by default, perform any Layer 3 routing. If the equipment has Layer 3 features, user shall be able to turn off ALL Layer 3 functions.

NI-002120 [**Optional**] The TSF shall support VLAN Tagging as specified by IEEE 802.1Q.

NI-002130 [**Required**] The TSF shall selectively provide point-to-point Ethernet services with dedicated non-shared bandwidth without queuing or buffering of Ethernet frames.

NI-002140 [**Required**] The TSF shall support ITU-T Recommendation G.7041/Y.1303 (2003).

NI-002150 [**Required**] The TSF shall support ITU-T Recommendation G.7043/Y.1343 (2004).

NI-002160 [**Required**] The TSF shall support ITU-T Recommendation G.7042/Y.1305 (2004).

10.3.3.4 TSF Framing

NI-002170 [**Required**] The TSF shall conform to the standard SONET STS-1, STS-N, and STS-Nc frame structures per Telcordia Technologies GR-253-CORE.

NI-002180 [**Required**] The TSF shall conform to the standard SDH optical interfaces, rates and formats documented in ITU-T Recommendation G.707 for each of the following optical interfaces: STM-1, STM-4, STM-16, and STM-64.

NI-002190 [**Required**] All SONET overhead bytes are to be defined, generated, and processed according to the specifications of Telcordia Technologies GR-253-CORE. All SDH overhead bytes are to be defined, generated, and processed according to the specifications of ITU-T Recommendation G.707.

NI-002200 [**Required**] The capability to read or write the 16-byte frame and format of ITU-T Recommendation G.707 and clause 3 of ITU-T Recommendation G.831 shall be provided for both the Section Trace (J0) and the Path Trace (J1) bytes.

NI-002210 [**Required**] The capability to read or write the 64-byte frame and format of ITU-T Recommendation G.707 and clause 3 of ITU-T Recommendation G.831 shall be provided for both the Section Trace (J0) and the Path Trace (J1) bytes.

10.3.3.5 TSF Switch Fabric

NI-002220 [**Required**] The SONET cross-connects shall have an STS-1 granularity.

NI-002230 [**Required**] The SDH cross-connects shall have a Virtual Circuit (VC) VC-3 VC-4 granularity.

NI-002240 [**Required**] The TSF shall not modify the user payload. Except for internetworking functions associated with optional Ethernet services, the system shall not perform any user protocol conversions.

NI-002250 [**Required**] The TSF shall not impart any errors onto the connections during cross-connects, grooming, or multiplexing.

NI-002260 [**Required**] The TSF shall support virtual concatenation as defined in American National Standards Institute (ANSI) T1.105-2001 or ITU-T Recommendation G.707.

NI-002270 [**Required**] No single failure in the switch fabric shall affect service. The system shall meet Telcordia Technologies GR-2996-CORE requirements for fabric availability.

NI-002280 [**Required**] The interface cards shall be capable of switching between the working and protection switch fabric in an errorless manner for manual operation, and in a hitless manner for automated operation. No bits shall be lost or corrupted with errorless switching. Bit errors are allowed with hitless switching. However, hitless switching shall not cause downstream reframing to occur.

10.3.3.6 TSF Performance

NI-002290 [**Required**] The TSF shall meet the jitter criteria for SONET systems in Telcordia Technologies GR-25-CORE, Section 5.6.

NI-002300 [**Required**] The TSF shall meet the jitter criteria for SDH systems according to ITU-T Recommendation G.825.

NI-002310 [**Required**] The jitter tolerance measured at the OC-N interface on the switch shall meet input jitter tolerance specification documented in ANSI T1.105.03-1994.

NI-002320 [**Required**] The jitter generation measured at an OC-N interface on the switch shall be less than 0.01 Unit Interval Root Mean Square (UIrms) when measured using a high-pass filter with 12-kilohertz (kHz) cutoff frequency as defined in ANSI T1.105.03-1994, Section A.3.3.

NI-002330 [**Required**] The maximum delay for a full STS passed through the Switch or for an STS add/drop from the switch shall not exceed the values defined in Telcordia Technologies GR-2996-CORE.

NI-002340 [**Optional**] The TSF shall perform hair-pinning, drop, continue, and drop-and-continue add-drop multiplexing (ADM) functions as specified in Telcordia Technologies GR-496-CORE.

NI-002350 [**Optional**] The TSF shall provide the ability to hub or nest lower STSs in a linear or ring configuration from line-side interfaces.

10.3.3.7 General Link Protection

NI-002360 [**Required**] It shall be possible to provision any SONET port for 1+1 Automatic Protection Switching (APS) per Telcordia Technologies GR-1400-CORE.

NI-002370 [**Required**] It shall be possible to provision any SDH port for 1+1 APS, 0:1 APS.

NI-002380 [**Required**] When the TSF participates in point-to-point UPSR or BLSR protection, switching shall take place in less than 50 ms. These protection mechanisms shall be definable and selectable from the EMS, and shall offer the selection of revertive and non-revertive restoration mechanisms.

NI-002390 [**Required**] Service restoration via a protection switch shall be automatic and accomplished without human or central management system intervention.

NI-002400 [**Required**] The protection switching mechanism shall be independent among separately managed network domains. A protection switch in one separately managed network domain shall not propagate or relay to another separately managed network domain.

NI-002410 [**Required**] The maximum detection time to determine if a signal's BER threshold is exceeded shall comply with Telcordia Technologies GR-253-CORE and ITU-T G.783.

NI-002420 [**Required**] Once a decision is made to switch, the terminal circuit pack switching shall take place within 50 ms, as described in Telcordia Technologies GR-253-CORE and ITU-T Recommendation G.783.

NI-002430 [**Required**] Catastrophic failures on a user-definable Excessive BER (EBER) condition shall be detected by an equipment-protected circuit pack in a terminal within 10 ms as described in Telcordia Technologies GR-253-CORE and ITU-T Recommendation G.783.

NI-002440 [**Required**] When equipped, each TSF shall be compliant with types and characteristics of SDH network protection architectures as defined in ITU-T Recommendation G.841.

NI-002450 [**Required**] When equipped, the TSF shall be compliant with interworking of SDH network protection architectures as defined in ITU-T Recommendation G.842.

10.3.3.8 Linear Protection

NI-002460 [**Required**] The linear switching protection mechanisms of the TSF shall be selectable as either revertive or non-revertive during network operation.

NI-002470 [**Required**] The SONET linear protection mechanisms of the TSF including APS functions shall conform to Telcordia Technologies GR-253-CORE. No proprietary APS byte definition and no proprietary linear APS protocol are allowed.

NI-002480 [**Required**] The TSF shall support 1+1 APS optical interface protection, unidirectional and bidirectional, and revertive and non-revertive, per ITU-T Recommendation G.841.

NI-002490 [**Required**] The SDH linear protection mechanisms of the system, including APS functions, shall conform to ITU-T Recommendation G.841. No proprietary APS byte definition or proprietary linear APS protocol is allowed.

NI-002500 [**Required**] When the high-speed interface of the TSF is configured for a linear protection system, it shall support linear protection switching with adjacent equipment. The system shall support both 1+1 and 1:1 protection switching across the network as per Section 5.3.2 of Telcordia Technologies GR-253-CORE and ITU-T Recommendation G.841.

NI-002510 [**Required**] When the TSF is configured as a 1:1 linear protection system, it shall support both unidirectional and bidirectional protection switching capabilities, as described in Telcordia Technologies GR-253-CORE and ITU-T Recommendation G.841.

NI-002520 [**Required**] The maximum length of protection switching time because of a fiber cut, signal failure, user definable EBER, or an equipment circuit pack failure in a network shall not exceed 60 ms per transmission direction, which includes 10 ms BER detection time as described in Telcordia Technologies GR-253-CORE and ITU-T Recommendation G.841.

NI-002530 [**Required**] When the TSF is configured as a 1:1 linear protection system, its default protection switching mode shall be revertive; i.e., the signal shall be automatically reverted to the working fibers after the fibers are repaired and the Wait to Restore (WTR) time has expired, as

described in Telcordia Technologies GR-253-CORE. A 1:1 linear system also shall be optionally configurable as non-revertive.

NI-002540 [**Required**] The linear protection configuration of the TSF shall:

a. Have a switch completion time in both directions of not more than 50 ms.

b. Provide the Signal Fail (SF), Signal Degrade (SD), and APS initiation criteria.

c. Support the WTR feature to prevent frequent oscillations between the working and the protection lines resulting from intermittent failures as described in Telcordia Technologies GR-253-CORE.

d. Provide a minimum WTR time of 5 minutes.

e. Provide a maximum WTR time of 12 minutes as described in Telcordia Technologies GR-253-CORE.

10.3.3.9 Fault Management

NI-002550 [**Required**] The TSF shall send the appropriate Alarm Indication Signal (AIS) and Remote Defect Indication (RDI) to adjacent systems, the EMS, and/or the higher level management system after detecting signal failure or degraded conditions for a specified alarm or indication activation time, as described in ANSI T1.231, Tables 2, 6, and 11.

NI-002560 [**Required**] The TSF shall remove the appropriate AIS and RDI after the source system has cleared the signal failure or degraded condition for a specified alarm or indication activation time, as described in ANSI T1.231, Tables 2, 6, and 11.

NI-002570 [**Required**] Alarms shall indicate circuit-level or signal alarms, as well as alarms in the MSPP itself, such as Span Failure, Line of Sight (LOS), Path Switch Complete/Fail, Laser Degradation, Card Failure, and Card Mismatch. These conditions will be reported to the EMS and high management system.

NI-002580 [**Required**] Standard SONET and SDH alarms shall be supported by the TSF including LOS, Loss of Pointer (LOP), Loss of Frame (LOF), Receive (Rx) AIS, RDI, and Remote Failure Indication (RFI). These conditions will be reported to the EMS and higher level management system.

NI-002590 [**Required**] The TSF shall indicate SONET T&S failures. The MSPP shall give an alarm showing the inability to establish a Phase Locked Loop (PLL). The MSPP shall have the ability to monitor the Building Integrated Timing Supply (BITS) incoming references (BITS-A and BITS-B). The system shall give an alarm when there is any timing change; e.g., a switch from BITS-A to BITS-B. These conditions will be reported to the EMS and higher level management system.

NI-002600 [**Required**] Each TSF shall detect, report, and clear the following signal failure events or conditions: LOS, LOF, LOP, Severely Errored Framing (SEF), AIS, and Out of Frame

(OOF), according to ANSI T1.231. These events and conditions will be reported to the EMS and higher management system.

10.3.3.10 Performance Management

NI-002610 [**Required**] The TSF shall calculate the Performance Monitoring (PM) parameter values for each SONET/SDH layer from block errors, rather than bit errors, per ITU-T Recommendation G.826.

NI-002620 [**Required**] The TSF shall gather PM data based on overhead bits, such as Bit Interleaved Parity-Number, at the section, line, and path layers, or on Ethernet frame overhead, as appropriate.

NI-002630 [**Required**] The TSF shall track PM data for appropriate service(s), e.g., SONET errors, Far-End Block Errors (FEBE), pointer adjustments; Ethernet statistics. All statistics shall be tracked in 5-minute intervals, with the ability to reduce intervals for testing and analysis.

NI-002640 [**Desired**] The TSF shall use tools such as OSAs and optical monitoring tools to verify optical power levels and detect unauthorized signals and other anomalous events on its interfaces.

NI-002650 [**Required**] The TSF shall support status and configuration reporting between nodes in Multi-Ring (Mixed UPSR, BLSR, and 1+1 APS), Linear ADM, Mesh, Regenerator, and Star/Hub node configurations. The NEs shall support near-end and far-end reporting.

NI-002660 [**Desired**] The TSF shall support reporting of Resilient Packet Ring (RPR) QoS/CoS parameters.

NI-002670 [**Required**] The TSF shall support reporting of trunk and port quality with user-configurable thresholds.

NI-002680 [**Required**] The TSF shall support reporting of Ethernet frames dropped.

NI-002690 [**Required**] The TSF shall be able to track near-end and far-end statistics in both receive and transmit directions. The TSF shall be able to track all the performance metrics defined in ITU-T Recommendation M.2101.

NI-002700 [**Required**] The TSF shall monitor each optical interface in accordance with ANSI T1.231-1993. Performance monitoring parameters shall include Severely Errored Framing Seconds (SEFS), Code Violation (CV), Errored Seconds (ES), Severely Errored Seconds (SES), Unavailable Seconds (UAS), Protection Switching Counts, and Pointer Justification.

NI-002710 [**Required**] For SONET traffic, the TSF shall be able to track section, line, and path errors. Further, it shall track the respective FEBEs and RDIs.

NI-002720 [**Desired**] The TSF shall support intermediate Path Monitoring.

10.3.3.11 EMS

EMS requirements are covered in Section 15.

10.3.3.12 Physical Design

NI-002730 [**Required**] All TSF elements shall meet the EMC/EMI requirements defined in FCC Part 15, Class A.

NI-002740 [**Required**] All TSF elements shall meet the EMC/EMI requirements defined in Telcordia Technologies GR-1089-CORE.

NI-002750 [**Required**] All TSF elements shall meet the EMC/EMI requirements defined in ETSI EN 50082.

NI-002760 [**Required**] All TSF elements shall meet the EMC/EMI requirements defined in ETSI EN 55022.

NI-002770 [**Required**] All TSF elements shall meet the EMC/EMI requirements defined in ETSI EN 300-386.

NI-002780 [**Required**] All TSF elements shall be designed to operate continuously in the following environment ranges without degradation: Temperature: 0 to +50°C; Humidity: 5 to 95 percent relative humidity, without condensation.

NI-002790 [**Required**] All TSF elements shall be designed to be fully operational after transportation and/or storage in the following environment ranges: Temperature: -40 to +70°C, Humidity: 5 to 95 percent relative humidity, without condensation.

NI-002800 [**Required**] All TSF elements shall be designed to operate continuously in the following environment range without degradation. Altitude: -100 to 15,000 ft AMSL.

NI-002810 [**Required**] All TSF elements shall be designed to be fully operational after transportation and/or storage in the following environment range: Transport Altitude: -100 ft to +40,000 ft AMSL.

NI-002820 [**Required**] All TSF elements shall adhere to NEBS Level 3 compliance standards for acceptable voltage ranges, EMI, and ESD safety, and shall be operable using standard 48V dc power as well as having redundant isolated power input feeds. For certain sites, an alternative ac/dc rectifier may need to be supplied to power the system and shall be able to switch 110/220V with redundant isolated power modules.

NI-002830 [**Required**] All TSF elements shall be fully operational throughout the battery voltage range of -41.5 to -56 VDC.

NI-002840 [**Required**] All TSF elements shall not be damaged and recover to normal performance following application of the following maximum transient voltages for the durations given (nominal voltage 48 VDC): 75 VP-P for 1 ms, 60VP-P for 500 ms.

NI-002850 [**Required**] All TSF elements shall be fully NEBS, Level 3 compliant.

NI-002860 [**Required**] All TSF elements shall be designed to operate continuously in the following environment ranges without degradation: Temperature: 0 to +50°C; Humidity: 5 to 95 percent relative humidity, without condensation.

NI-002870 [**Required**] All TSF elements shall be designed to be fully operational after transportation and/or storage in the following environment ranges: Temperature: -40 to +70°C, Humidity: 5 to 95 percent relative humidity, without condensation.

NI-002880 [**Required**] All TSF elements shall be designed to operate continuously in the following environment range without degradation: Altitude: -100 to 15,000 ft AMSL.

NI-002890 [**Required**] All TSF elements shall be designed to be fully operational after transportation and/or storage in the following environment range: Transport Altitude: -100 ft. to +40,000 ft AMSL.

NI-002900 [**Required**] All TSF elements shall adhere to NEBS Level 3 compliance standards for acceptable voltage ranges, EMI, and ESD safety, and shall be operable using standard 48V dc power as well as having redundant isolated power input feeds. For certain sites, an alternative ac/dc rectifier may need to be supplied to power the system and shall be able to switch 110/220V with redundant isolated power modules.

NI-002910 [**Required**] All TSF elements shall be fully operational throughout the battery voltage range of -41.5 to -56 VDC.

NI-002920 [**Required**] All equipment shall have been tested and register as compliant to the following Electrical Safety standards: UL-1950, EN60950, and IEC 60950.

10.3.3.13 Standards Compliance

The standards in effect when the equipment was first acquired are listed. Updates to the standards since that point in time are identified in brackets. When the manufacturer provides new components for the COTS items to the same device that satisfy updated standards, DISA will often purchase and install those components to accommodate growth, but will not replace existing components unless there is another reason to do so. As such, components will be operational within DISN that satisfy multiple versions of the standards. Testing will need to be undertaken using the standard release that applied to that component, where the revised standard cannot be satisfied by the original component.

NI-002930 [**Required**] ITU-T Recommendation G.691 (2006).

NI-002940 [**Required**] ITU-T Recommendation G.693 (2006).

NI-002950 [**Required**] ITU-T Recommendation G.707/Y1322 (2007).

NI-002960 [**Required**] ITU-T Recommendation G709/Y.1331.

NI-002970 [**Required**] ITU-T Recommendation G.783 (2006).

NI-002980 [**Required**] ITU-T Recommendation G.826 (2002).

NI-002990 [**Required**] ITU-T Recommendation G.831 (2000).

NI-003000 [**Required**] ITU-T Recommendation G.841 (1998).

NI-003010 [**Required**] ITU-T Recommendation G.842 (1997).

NI-003020 [**Required**] ITU-T Recommendation G.957 (2006).

NI-003030 [**Required**] ITU-T Recommendation M.2101 (2003).

NI-003040 [**Required**] ITU-T Recommendation G.7041/Y-1303 (2003) (2008).

NI-003050 [**Required**] ITU-T Recommendation G.7042/Y-1305 9 (2004) (2006).

NI-003060 [**Required**] ANSI T1.231-1993 (2003 [R2007]).

NI-003070 [**Required**] Telcordia Technologies GR-253-CORE, Issue 3, September 2000; (Issue 4, December 2005).

NI-003080 [**Required**] Telcordia Technologies GR-282-CORE, December 1997; (Issue 4, July 2006).

NI-003090 [**Required**] Telcordia Technologies GR-383-CORE, Issue 1, July 1997; (Issue 3, February 2006).

NI-003100 [**Required**] Telcordia Technologies GR-499-CORE, Issue 2, December 1998; (Issue 3, September 2004).

NI-003110 [**Required**] Telcordia Technologies GR-1230-CORE, Issue 4, December 1998.

NI-003120 [**Required**] Telcordia Technologies GR-1400-CORE, Issue 2, December 1999 (Issue 3, July 2006).

NI-003130 [**Required**] Telcordia Technologies GR-2996-CORE, Issue 1, January 1999.

NI-003140 [**Required**] Telcordia Technologies SR-3580, Issue 1, November 1995; (Issue 3, June 2007).

NI-003150 [**Required**] IEEE 802.3-2008, Section 5.

NI-003160 [**Optional**] IEEE 802.1Q-2003.

NI-003170 [**Optional**] IEEE 802.17-2004.

NI-003180 [**Required**] British Standards Institute BS EN 60950-1, August 6, 2006.

NI-003190 [**Required**] IEC 60950-1, 2006.

NI-003200 [**Required**] CFR FCC Part 15, Class A.

NI-003210 [**Required**] Network Equipment- Building System (NEBS), Level 3.

NI-003220 [**Required**] Underwriters Laboratories, Inc UL-1950, Standard for Safety, Information Technology Equipment Including Electrical Business Equipment, 1ed, 1989.

10.3.4 Access Grooming Function

Today, the AGF functional device is provided within the DISA-provided part of DISN by the MSPP or ODXC when used as an MSPP.

10.3.4.1 Description

The MSPP is an AGF functional device that receives low-speed circuits on multiple ports and multiplexes them via TDM into a high-speed circuit, and transmits it to one of its high-speed ports. The multiplexing is configured via multiple internal cross-connects between the low-speed ports and the high-speed port. The MSPP AGF functional device can connect circuits from any port to any other port within the bandwidth limits of the ports.

The MSPP AGF functional device can be configured with many different types of ports as follows:

- Concatenated SONET/SDH. For SONET, the port bandwidths are OC-3c, OC-12c, OC-48c, and OC192c. For SDH, the port bandwidths are STM-1c, STM-4c, and STM-16c.
- Unconcatenated SONET/SDH. For SONET, the port bandwidths are OC-3, OC-12, OC-48, and OC-192. For SDH, the port bandwidths are STM-1, STM-4, STM-16, and STM-64.
- Ethernet. Ethernet is a frame-based data communication technology for LAN. The data rate is 10 Mbps for Regular Ethernet, 100 Mbps for Fast Ethernet (FE), 1 Gbps for GbE.
- Digital Signal. DS1, DS3, E1 and E3. A different port, called a transmux, exists that will demultiplex the DS3 into 28 DS1s. The ports will also convert the format from a digital signal format into a SONET format. The DS1 becomes the VT1.5 and then E1 becomes the VT2.0. The DS3 becomes an STS-1. The AGF functional device can also be used to provide timing to DS1s.

10.3.4.2 AGF Functional Device SONET Interface

The MSPP shall meet the following AGF SONET interface requirements:

NI-003230 [**Required**] The OC-3/OC-3c optical interface shall conform to the standard SONET rates and formats documented in ANSI T1.105.

NI-003240 [**Required**] The OC-3/OC-3c optical interface shall conform to optical parameters for application category SR-1 per Telcordia Technologies GR-253-CORE, Sections 4.1 and 4.2, and Tables 4-1 through 4-11.

NI-003250 [**Required**] The OC-3/OC-3c optical interface shall conform to optical parameters for application category IR-1 per Telcordia Technologies GR-253-CORE, Sections 4.1 and 4.2, and Tables 4-1 through 4-11.

NI-003260 [**Required**] The OC-3/OC-3c optical interface shall conform to optical parameters for application category IR-2 per Telcordia Technologies, GR-253-CORE, Sections 4.1 and 4.2, and Tables 4-1 through 4-11.

NI-003270 [**Required**] The OC-3/OC-3c optical interface shall conform to optical parameters for application category LR-1 per Telcordia Technologies GR-253-CORE, Sections 4.1 and 4.2, and Tables 4-1 through 4-11.

NI-003280 [**Required**] The OC-3/OC-3c optical interface shall conform to optical parameters for application category LR-2 per Telcordia Technologies GR-253-CORE, Sections 4.1 and 4.2, and Tables 4-1 through 4-11.

NI-003290 [**Required**] The OC-3/OC-3c optical interface shall conform to optical parameters for application category LR-3 per Telcordia Technologies GR-253-CORE, Sections 4.1 and 4.2, and Tables 4-1 through 4-11.

NI-003300 [**Optional**] The OC-3/OC-3c interfaces shall be capable of having a multi-mode fiber (MMF) interface option for both transmit and receive using MMF as described in ITU-T Recommendation G.651 and ANSI 105.06-2002.

NI-003310 [**Required**] The OC-3/OC-3c interfaces shall be capable of using Single Mode Fiber (SMF) as described in ITU-T Recommendation G.652 and ANSI 105.06-2002.

NI-003320 [**Required**] The OC-12/OC-12c optical interface shall conform to the standard SONET rates and formats documented in ANSI T1.105.

NI-003330 [**Required**] The OC-12/OC-12c optical interface shall conform to optical parameters for application category SR-1 per Telcordia Technologies GR-253-CORE, Sections 4.1 and 4.2, and Tables 4-1 through 4-11.

NI-003340 [**Required**] The OC-12/OC-12c optical interface shall conform to optical parameters for application category IR-1 per Telcordia Technologies GR-253-CORE, Sections 4.1 and 4.2, and Tables 4-1 through 4-11.

NI-003350 [**Required**] The OC-12/OC-12c optical interface shall conform to optical parameters for application category IR-2 per Telcordia Technologies GR-253-CORE, Sections 4.1 and 4.2, and Tables 4-1 through 4-11.

NI-003360 [**Required**] The OC-12/OC-12c optical interface shall conform to optical parameters for application category LR-1 per Telcordia Technologies GR-253-CORE, Sections 4.1 and 4.2, and Tables 4-1 through 4-11.

NI-003370 [**Required**] The OC-12/OC-12c optical interface shall conform to optical parameters for application category LR-2 per Telcordia Technologies GR-253-CORE, Sections 4.1 and 4.2, and Tables 4-1 through 4-11.

NI-003380 [**Required**] The OC-12/OC-12c optical interface shall conform to optical parameters for application category LR-3 per Telcordia Technologies GR-253-CORE Sections 4.1 and 4.2, and Tables 4-1 through 4-11.

NI-003390 [**Optional**] The OC-12/OC-12c interfaces shall be capable of having an MMF interface option for both transmit and receive using MMF as described in ITU-T Recommendation G.651 and ANSI 105.06-2002.

NI-003400 [**Required**] The OC-12/OC-12c interfaces shall be capable of using SMF as described in ITU-T Recommendation G.652 and ANSI 105.06-2002.

NI-003410 [**Required**] The OC-48/OC-48c optical interface shall conform to the standard SONET rates and formats documented in ANSI T1.105.

NI-003420 [**Required**] The OC-48/OC-48c optical interface shall conform to optical parameters for application category SR-1 per Telcordia Technologies GR-253-CORE, Sections 4.1 and 4.2, and Tables 4-1 through 4-11.

NI-003430 [**Required**] The OC-48/OC-48c optical interface shall conform to optical parameters for application category IR-1 per Telcordia Technologies GR-253-CORE, Sections 4.1 and 4.2, and Tables 4-1 through 4-11.

NI-003440 [**Required**] The OC-48/OC-48c optical interface shall conform to optical parameters for application category IR-2 per Telcordia Technologies GR-253-CORE, Sections 4.1 and 4.2, and Tables 4-1 through 4-11.

NI-003450 [**Required**] The OC-48/OC-48c optical interface shall conform to optical parameters for application category LR-1 per Telcordia Technologies GR-253-CORE, Sections 4.1 and 4.2, and Tables 4-1 through 4-11.

NI-003460 [**Required**] The OC-48/OC-48c optical interface shall conform to optical parameters for application category LR-2 per Telcordia Technologies GR-253-CORE, Sections 4.1 and 4.2, and Tables 4-1 through 4-11.

NI-003470 [**Required**] The OC-48/OC-48c optical interface shall conform to optical parameters for application category LR-3 per Telcordia Technologies GR-253-CORE, Sections 4.1 and 4.2, and Tables 4-1 through 4-11.

NI-003480 [**Optional**] Software programmable Small Form-factor Pluggable (SFP) that supports OC-3/OC-12 optical interface shall conform to optical parameters for application category per Telcordia Technologies GR 253-CORE, Sections 4.1 and 4.2, and Tables 4-1 through 4-11.

NI-003490 [**Optional**] Programmable SFP that supports OC-3/OC-3c and OC-12/OC-12c optical interfaces shall be capable of having an MMF interface option for both transmit and receive using MMF as described in ITU-T Recommendation G.651 and ANSI 105.06-2002.

NI-003500 [**Optional**] Software programmable SFP that supports OC-3/OC-12/OC-48 and OC 3c/OC12c/OC-48c optical interface shall conform to optical parameters for application category per Telcordia Technologies GR-253-CORE, Sections 4.1 and 4.2, and Tables 4-1 through 4-11.

NI-003510 [**Required**] The OC-192 optical interface shall conform to the standard SONET rates and formats documented in ANSI T1.105.

NI-003520 [**Required**] The OC-192 optical interface shall conform to optical parameters for application category SR-1 per Telcordia Technologies GR-253-CORE, Sections 4.1 and 4.2, and Tables 4-1 through 4-11.

NI-003530 [**Required**] The OC-192 optical interface shall conform to optical parameters for application category IR-1 per Telcordia Technologies GR-253-CORE, Sections 4.1 and 4.2, and Tables 4-1 through 4-11.

NI-003540 [**Required**] The OC-192 optical interface shall conform to optical parameters for application category IR-2 per Telcordia Technologies GR-253-CORE, Sections 4.1 and 4.2, and Tables 4-1 through 4-11.

NI-003550 [**Required**] The OC-192 optical interface shall conform to optical parameters for application category LR-1 per Telcordia Technologies GR-253-CORE, Sections 4.1 and 4.2, and Tables 4-1 through 4-11.

NI-003560 [**Required**] The OC-192 optical interface shall conform to optical parameters for application category LR-2 per Telcordia Technologies GR-253-CORE, Sections 4.1 and 4.2, and Tables 4-1 through 4-11.

NI-003570 [**Required**] The OC-192 optical interface shall conform to optical parameters for application category lR-3 per Telcordia Technologies GR-253-CORE, Sections 4.1 and 4.2, and Tables 4-1 through 4-11.

NI-003580 [**Optional**] All SONET OC-N interfaces shall be software-provision to SDH STM-N.

NI-003590 [**Optional**] The software has to provide options for the OC-3 through OC-48 optical interfaces and the upgrade capability to the next higher optical rate by changing cards unless the optics is software programmable. If the optics is software programmable, then this capability must be allowed by changing the software setting to the next higher rate. Both procedures must preserve the customer data provisioned on the optical interface and move to the equivalent

bandwidth slot starting at the beginning STS. Example: OC-3 upgrade to OC-12, OC-12 to OC-48, and OC-48 to OC-192. Customer provisioned on OC-3 (STS-1 through 3) will occupy STS-1 through 3 on the OC-12 after the upgrade is completed.

10.3.4.3 AGF Functional Device SDH Interface

The MSPP shall meet the following SDH interface requirements:

NI-003600 [**Required**] The STM-1/STM-1c optical interface shall conform to optical parameters for application code I-1 per ITU–T Recommendation G.957, Table 2.

NI-003610 [**Required**] The STM-1/STM-1c optical interface shall conform to optical parameters for application code S-1.1 per ITU–T Recommendation G.957, Table 2.

NI-003620 [**Required**] The STM-1/STM-1c optical interface shall conform to optical parameters for application code S-1.2 per ITU–T Recommendation G.957, Table 2.

NI-003630 [**Required**] The STM-1/STM-1c optical interface shall conform to optical parameters for application code L-1.1 per ITU–T Recommendation G.957, Table 2.

NI-003640 [**Required**] The STM-1/STM-1c optical interface shall conform to optical parameters for application code L-1.2 per ITU–T Recommendation G.957, Table 2.

NI-003650 [**Required**] The STM-1/STM-1c optical interface shall conform to optical parameters for application code L-1.3 per ITU–T Recommendation G.957, Table 2.

NI-003660 [**Optional**] The STM-1 interfaces shall be capable of having an MMF interface option for both transmit and receive using MMF as described in ITU-T Recommendation G.651.

NI-003670 [**Required**] The STM-1/STM-1c interfaces shall be capable of using SMF as described in ITU-T Recommendation G.652.

NI-003680 [**Required**] The STM-4/STM-4c optical interface shall conform to optical parameters for application code I-4 per ITU–T Recommendation G.957, Table 3.

NI-003690 [**Required**] The STM-4/STM-4c optical interface shall conform to optical parameters for application code S-4.1 per ITU–T Recommendation G.957, Table 3.

NI-003700 [**Required**] The STM-4/STM-4c optical interface shall conform to optical parameters for application code S-4.2 per ITU–T Recommendation G.957, Table 3.

NI-003710 [**Required**] The STM-4/STM-4c optical interface shall conform to optical parameters for application code L-4.1 per ITU–T Recommendation G.957, Table 3.

NI-003720 [**Required**] The STM-4/STM-4c optical interface shall conform to optical parameters for application code L-4.2 per ITU–T Recommendation G.957, Table 3.

NI-003730 [**Required**] The STM-4/STM-4c optical interface shall conform to optical parameters for application code L-4.3 per ITU–T Recommendation G.957, Table 3.

NI-003740 [**Optional**] The STM-4/STM-4c interfaces shall be capable of having an MMF interface option for both transmit and receive using MMF as described in ITU-T Recommendation G.651.

NI-003750 [**Required**] The STM-4/STM-4c interfaces shall be capable of using SMF as described in ITU-T Recommendation G.652.

NI-003760 [**Required**] The STM-16/STM-16c optical interface shall conform to optical parameters for application code I-16 per ITU-T Recommendation G.957, Table 4.

NI-003770 [**Required**] The STM-16/STM-16c optical interface shall conform to optical parameters for application code S-16.1 per ITU-T Recommendation G.957, Table 4.

NI-003780 [**Required**] The STM-16/STM-16c optical interface shall conform to optical parameters for application code S-16.2 per ITU-T Recommendation G.957, Table 4.

NI-003790 [**Required**] The STM-16/STM-16c optical interface shall conform to optical parameters for application code L-16.1 per ITU-T Recommendation G.957, Table 4.

NI-003800 [**Required**] The STM-16/STM-16c optical interface shall conform to optical parameters for application code L-16.2 per ITU-T Recommendation G.957, Table 4.

NI-003810 [**Required**] The STM-16/STM-16c optical interface shall conform to optical parameters for application code L-16.3 per ITU-T Recommendation G.957, Table 4.

NI-003820 [**Optional**] Software programmable SFP that supports STM-1/STM-4 and STM-1c/STM-4c Optical interface shall conform to optical parameters for application Code L-16.2 per ITU T Recommendation G.957, Table 4.

NI-003830 [**Optional**] Programmable SFP that supports STM-1/STM-4 optical interfaces shall be capable of having an MMF interface option for both transmit and receive using MMF as described in ITU-T Recommendation G.651.

NI-003840 [**Optional**] Software programmable SFP that supports STM-1/STM-4/STM-16 optical interface shall conform to optical parameters for application code L-16.2 per ITU-T Recommendation G.957, Table 4.

NI-003850 [**Required**] The STM-64 Optical interface shall conform to ITU-T Recommendation G.691 optical interfaces for Single-Channel STM-64 systems.

NI-003860 [**Optional**] The STM-64 Optical interface shall conform to ITU-T Recommendation G.691.

NI-003870 [**Required**] The software has to provide options from the STM-1 through STM-16 optical interfaces and the upgrade capability to the next higher optical rate by changing cards

unless the optics is software programmable. If the optics is software programmable, then this capability must be allowed by changing the software setting to the next higher rate. Both procedures must preserve the customer data provisioned on the optical interface and move to the equivalent bandwidth slot starting at the beginning STM. Example: STM-1 upgrade to STM-4, STM-4 to STM-16, and STM-16 to STM-64. Customer provisioned on STM-1 (VC3-1 through VC3-3) will occupy STM-1 VC3-1 through 3 on the STM-4 after the upgrade is completed.

NI-003880 [**Required**] The AGF functional device shall be able to provision, monitor, and detect faults, and restore optical services in a standardized and automated fashion.

10.3.4.3.1 AGF Functional Device Lambda Interface

The MSPP shall meet the following requirements:

NI-003890 [**Optional**] The AGF functional device shall have Lambda interfaces at the 10-Gigabit rates. These shall be compatible with the transport requirements in Section 10.3.3, Transport Switch Function.

NI-003900 [**Required**] Lambda interfaces shall be compliant with the ITU-T Recommendation G.694.1 grid if an AGF functional device supports Lambda interfaces.

10.3.4.4 AGF Functional Device Electrical Interface

The MSPP shall meet the following electrical interface requirements:

NI-003910 [**Optional**] The AGF functional device shall support STS-1 (EC-1) electrical interfaces that comply with specifications and pulse masks as defined in Telcordia Technologies GR 253-CORE, Chapter 4.4 and ANSI T1.102.

NI-003920 [**Required**] The AGF functional device shall support DS1 electrical interfaces that comply with ANSI T1.102.

NI-003930 [**Optional**] The AGF functional device shall support DS1 pseudowire transport via gateway SFPs.

NI-003940 [**Required**] The AGF functional device shall support channelized and unchannelized DS1 Superframe (SF) format and Extended Superframe (ESF) format as specified in ANSI T1.403. The ability to read or write the ESF data link is required. The selection of format for any particular DS1 interface shall be user-selectable.

NI-003950 [**Required**] The AGF functional device shall support Alternate Mark Inversion (AMI) and Bipolar with Eight-Zero Substitution (B8ZS) line coding formats and unframed, D4, SF, and ESF framing format as specified in ANSI T1.403. The selection of framing format for any particular DS1 interface shall be user-selectable.

NI-003960 [**Required**] The AGF functional device shall support both in-band and out-band Facility Data Link (FDL) loop-up and loop-down codes as specified in ANSI T1.403.

NI-003970 [**Required**] The AGF functional device shall support FDL status messages and respond as specified in ANSI T1.403.

NI-003980 [**Required**] The AGF functional device shall support unframed DS1 electrical signals.

NI-003990 [**Required**] The electrical interface shall comply with ITU-T Recommendation G.703.

NI-004000 [**Required**] The AGF functional device shall support DS1 bit rate of 1.544 Mbps +/- 32 ppm as specified in ANSI T1.101.

NI-004010 [**Required**] The AGF functional device shall support DS1 100 ohms cable with maximum length of 655 feet as specified in ITU-T Recommendation G.703.

NI-004020 [**Required**] The AGF functional device shall support E1 electrical interfaces shall comply with ITU-T Recommendation G.711.

NI-004030 [**Required**] The AGF functional device shall support both channelized and unchannelized E1 as specified in ITU-T Recommendation G.711.

NI-004040 [**Required**] The E1 electrical interface format shall support both 30 and 31 channels when channelized with and without Cyclical Redundancy Check (CRC) as specified in ITU-T Recommendation G.711. The selection of format for any particular E1 interface shall be user-selectable.

NI-004050 [**Required**] The AGF functional device shall support E1 bit rate of 2.048 Mbps +/- 50 ppm as specified in ITU-T Recommendation G.703 and G.704.

NI-004060 [**Required**] The AGF functional device shall support DS3 electrical tributary interfaces that comply with ANSI T1.102-1993.

NI-004070 [**Required**] The AGF functional device DS3 interface shall support DS3 pulse shape that meets both ITU-T Recommendation G.703 and Telcordia Technologies GR-499-CORE.

NI-004080 [**Required**] The AGF functional device shall support channelized and unchannelized DS3 signals in either unframed, M13, or C-bit parity formats per ANSI T1.101 and T1.404. The selection of format for any particular DS3 interface shall be user-selectable.

NI-004090 [**Required**] The AGF functional device shall support DS3 C-bit far-end alarm and control signal to support alarm/status messages and loopback control on the DS3 and/or individual DS1 as specified in ANSI T1.101 and T1.404.

NI-004100 [**Required**] The AGF functional device shall support DS3 bit rate of 44.736 Mbps +/- 20 ppm as specified in ANSI T1.101.

NI-004110 [**Required**] The AGF functional device shall support E3 electrical tributary interfaces that comply with ITU-T Recommendation G.703.

NI-004120 [**Required**] The AGF functional device shall support channelized and unchannelized E3 signals using line coding of High Density Bipolar 3 Code (HDB-3).

NI-004130 [**Required**] The AGF functional device shall support E3 bit rate of 34.368 Mbps +/- 20 ppm as specified in ITU-T Recommendation G.703.

NI-004140 [**Required**] The AGF functional device shall be able to provision, monitor, and detect faults, and restore electrical (DS1, E1, DS3, E3) services in a standardized and automated fashion.

10.3.4.5 AGF Functional Device Ethernet Interface

The MSPP shall meet the following Ethernet requirements:

NI-004150 [**Required**] The AGF functional device shall provide interfaces for Ethernet, FE, and GbE services in conformance with IEEE 802.3 for Ethernet LAN interfaces.

NI-004160 [**Optional**] The AGF functional device shall provide interfaces for 10GbE Services in conformance with IEEE 802.3 for Ethernet LAN/WAN interfaces.

NI-004170 [**Required**] The Logical Link IWF shall terminate the MAC layer of Ethernet as described in Ethernet Standard IEEE 802.3.

NI-004180 [**Required**] Ethernet interfaces shall accommodate Ethernet packets greater than 4470 bytes.

NI-004190 [**Required**] Ethernet services shall support port-based and flow-based VLANs for multiple rates and customer interfaces as per IEEE 802.1Q.

NI-004200 [**Required**] The AGF functional device shall support transparent VLAN tagging for Ethernet on SONET/SDH service.

NI-004210 [**Required**] The AGF functional device shall not, by default, perform any Layer 3 IP routing.

NI-004220 [**Required**] The AGF functional device shall be able to provision, monitor, and detect faults, and restore Ethernet services in a standardized and automated fashion.

NI-004230 [**Required**] The AGF functional device shall selectively provide QoS/CoS for Ethernet services according to RFC 2474, DSCP.

NI-004240 [**Required**] Available Ethernet services shall include, Generic Framing Procedure (GFP) (ITU-T Recommendation G.7041/Y.1303), Hardware Link Capacity Adjustment Scheme (LCAS), and Virtual Concatenation (VCAT).

NI-004250 [**Required**] Ethernet and FE Services on SONET shall support GFP (ITU-T Recommendation G.7041/Y.1303), hardware LCAS, low order VCAT (VT1.5), high order (STS-1) VCAT, and Contiguous Concatenation (CCAT); STS-1 and STS-3c.

NI-004260 [**Required**] Ethernet and FE services on SDH shall support GFP (ITU-T Recommendation G.7041/Y.1303), hardware LCAS, low order VCAT (VC-12 and VC-3, and CCAT; VC-3 and VC-4.

NI-004270 [**Required**] GbE services on SDH shall support GFP (ITU-T Recommendation G.7041/Y.1303), hardware LCAS, low order VCAT (VC-3), high order (VC-4) VCAT, and CCAT; VC-3, VC-4, VC-4-3, and VC-4-16.

NI-004280 [**Required**] Ten GbE services on SDH shall support GFP (ITU-T Recommendation G.7041/Y.1303), hardware LCAS, high order (VC-4) VCAT, and CCAT; VC-3, VC-4, VC-4-3, and VC-4-16, and VC-4-64.

NI-004290 [**Required**] The AGF functional device shall selectively provide point-to-point Ethernet services with dedicated non-shared bandwidth without queuing or buffering Ethernet frames.

NI-004300 [**Required**] Ethernet and FE interfaces shall be auto-sensing/auto-detecting and auto-configuring between incoming Ethernet and FE signals.

10.3.4.6 AGF Functional Device Cross-Connect

NI-004310 The MSPP shall provide the following cross-connect requirements:

NI-004320 [**Required**] The AGF functional device shall cross connect with the granularity of STS-1 and VT1.5 on a SONET AGF functional device.

NI-004330 [**Required**] The STS-1 (high order) cross-connect fabric shall be capable of supporting at least 40 G of cross connects at the STS-1/STM-0 level.

NI-004340 [**Required**] The VT1.5 (low order) cross-connect fabric shall be scalable and capable of supporting at least 10 Gbps of traffic at the VC-11/VC-12 level.

NI-004350 [**Optional**] The AGF functional device shall have an Ethernet switch fabrics via agnostic fabric or separate from its STS-1 or VT1.5 TDM fabric.

NI-004360 [**Required**] The AGF functional device shall perform Time Slot Interchange (TSI) and Time Slot Assignment (TSA) cross connect between DS1 interfaces and channelized DS3 interfaces into a SONET VT1.5 formatted within the STS containers.

NI-004370 [**Required**] The AGF functional device shall support structured Administrative Unit-4 (AU-4) mapping for SDH applications using the ITU multiplexing structure in ITU-T Recommendation G.707.

NI-004380 [**Required**] The AGF functional device shall be able to map T1, E1, T3, and E3 signals into an AU-4 mapping structure as per ITU-T G.707.

NI-004390 [**Required**] The AGF functional device shall support VC-11, VC-12, VC-3, and VC-4 cross-connect capability for SDH AU-4-based system.

NI-004400 [**Required**] The AGF functional device shall support SDH/SONET container gateway functionalities (i.e., VC-3 to STS-1 and VC-11 to VT1.5).

NI-004410 [**Optional**] The AGF functional device shall have the ability to retime signals from either VT1.5 or DS1 formats, as well as pass timing through the matrix directly to provide timing up to Stratum 1 via DS1 ports.

NI-004420 [**Required**] The AGF functional device cross-connects and interfaces shall be compatible with network-side STS or Lambda cross-connects at the DISN switch or the DISN Transport Element.

NI-004430 [**Required**] The AGF functional device cross-connects and interfaces at the AGF functional device shall be transparent to all protection switching at the DISN switch or the DISN Transport Element.

NI-004440 [**Required**] The AGF functional device shall support SONET provisioning of CCAT formats; OC-3c, OC-12c, and OC-48c.

NI-004450 [**Required**] The AGF functional device shall support SDH provisioning of CCAT formats; VC-4-3c, VC-4-16c, and VC-4-64c.

10.3.4.7 AGF Functional Device Interface Performance

The MSPP shall meet the following interface performance requirements:

NI-004460 [**Required**] The AGF functional device shall meet the jitter criteria for SONET systems in Telcordia Technologies GR-253-CORE, Section 5.6.

NI-004470 [**Required**] The AGF functional device shall meet the jitter criteria for SDH systems according to ITU-T Recommendation G.825 and ITU-T G.732.

NI-004480 [**Required**] The AGF functional device shall meet the interface jitter criteria specified for User Network Interface (UNI) interfaces for ITU-T OTN.

NI-004490 [**Required**] The jitter tolerance measured at the OC-N interface on the AGF functional device shall meet Figure A.1 input jitter tolerance specification documented in ANSI T1.105.03.

NI-004500 [**Required**] The jitter tolerance measured at the DS3 interface on the AGF functional device shall be at least 5 Unit Interval peak-to-peak (UIpp) between 10 Hertz (Hz) and 2.3 x 10^3 Hz, and at least 0.1 UIpp between 60 x 10^3 and 200 x 10^3 Hz as per Figure 7-1 in GR 499.

NI-004510 [**Required**] The jitter transfer measured between an input DS3 interface and the corresponding output DS3 interface on an AGF functional device (with its OC-12 or OC 3 signal looped-back) shall be less than the jitter transfer mask shown in Figure 7-4 of GR 499.

NI-004520 [**Required**] The jitter generation measured at the OC-N interface on the AGF functional device shall be less than 0.01 UIrms, when measured using a high-pass filter with 12-kHz cut-off frequency per ANSI T1.105.03, Section A.3.3.

NI-004530 [**Required**] The jitter generation because of DS3/STS-1 payload mapping for the DS3 interface on the AGF functional device shall be less than 0.4 UIpp, without pointer adjustments as per ANSI T1.105.03, Section 6.1.2.1.

NI-004540 [**Required**] The jitter generation because of DS3/STS-1 payload mapping for the DS3 interface on the AGF functional device shall be less than A1 equals A0 plus .3 UIpp for a single pointer adjustment as shown in Table 2 of ANSI T1.105.03-1994.

NI-004550 [**Required**] The jitter generation because of DS3/STS-1 payload mapping for the DS3 interface on the AGF functional device shall be less than 1.3 UIpp for pointer adjustment bursts as shown in Table 3 of ANSI T1.105.03.

NI-004560 [**Required**] The jitter generation because of DS3/STS-1 payload mapping for the DS3 interface on the AGF functional device shall be less than 1.2 UIpp for phase transient pointer adjustment bursts as shown in Table 4 of ANSI T1.105.03.

NI-004570 [**Required**] The jitter generation because of DS3/STS-1 payload mapping for the DS3 interface on the AGF functional device shall be less than 1.3 UIpp for periodic pointer adjustments as shown in Table 6 of ANSI T1.105.03-1994.

NI-004580 [**Required**] The jitter generation because of DS3/STS-1 payload mapping for the DS3 interface on the AGF functional device shall be less than 5 UIpp between 10 Hz and 500 Hz, and at least 0.1 UIpp between $8x10^3$ and $40x10^3$ Hz per Figure 7-1 of Telcordia Technologies GR-499-CORE.

NI-004590 [**Required**] The jitter transfer measured between an input DS1 interface and the corresponding output DS1 interface on the AGF functional device (with its OC-12 or OC-3 signal looped back) shall be less than the jitter transfer mask shown in Figure 7-4 of Telcordia Technologies GR 499-CORE.

NI-004600 [**Required**] The jitter generation because of DS1/VT-1.5 payload mapping without pointer adjustments for the DS1 interface on the AGF functional device shall be less than 0.7 UIpp per ANSI T1.105.03s, Section 6.1.1.1.

NI-004610 [**Required**] The jitter generation because of DS1/VT1.5 payload mapping and a single pointer adjustment for the DS1 interface on the AGF functional device shall meet the single VT pointer adjustment Maximum Time Interval Error (MTIE) mask shown on Figure 8 of the ANSI T1X1.3/94-001R5 supplement to ANSI T1.105.03.

NI-004620 [**Required**] The jitter generation because of DS1/VT1.5 payload mapping and periodic pointer adjustments for the DS1 interface on the AGF functional device shall meet the periodic VT pointer adjustment MTIE mask shown on Figure 10 of the ANSI T1X1.3/94-001R5 supplement to ANSI T1.105.03.

NI-004630 [**Required**] The maximum delay for a full STS passed through the AGF functional device (OC-N to OC-N), or for an STS add/drop shall not exceed 25 microseconds (μs) as per Telcordia Technologies TR-496, (R) [3-45].

NI-004640 [**Required**] The maximum delay for a floating VT passed through a DISN Access element (OC-N to OC-N), or for a floating VT add/drop (OC-N to low-speed or low-speed to OC N) shall not exceed 50 μs as per Telcordia Technologies, TR-496, (R) [3 46].

10.3.4.8 AGF Functional Device Equipment Redundancy

The MSPP shall meet the following redundancy requirements:

NI-004650 [**Required**] No single failure in the switch fabric shall affect service. The AGF functional device shall meet Telcordia Technologies GR-2996-CORE requirements for fabric availability.

NI-004660 [**Required**] The interface cards shall be capable of switching between the working and protection switch fabric in an errorless manner for manual operation, and in a hitless manner for automated operation. No bits shall be lost or corrupted with errorless switching. Bit errors are allowed with hitless switching. However, hitless switching shall not cause downstream reframing to occur.

NI-004670 [**Required**] A Plesiochronous Digital Hierarchy (PDH) (DS1, DS3, E1, E3) card shall support a 1:1 configuration.

NI-004680 [**Optional**] A PDH (DS1, DS3, E1, E3) card should support a 1:N configuration.

NI-004690 [**Required**] The AGF functional device shall support redundant processor and cross-connect matrix working in an active/standby mode.

NI-004700 [**Required**] The AGF functional device shall support redundant power supply and electrical feeds.

10.3.4.9 AGF Functional Device General Protection

The MSPP shall meet the following protection requirements:

NI-004710 [**Required**] It shall be possible to provision any SONET port for 1+1 APS, 1:N APS; 1:N OP, 2-Fiber UPSR per Telcordia Technologies GR-1400-CORE, or 2/4-Fiber BLSR per Telcordia Technologies GR-1230-CORE.

NI-004720 [**Required**] It shall be possible to provision any SDH port for 1+1 APS, 0:1 APS, 1:N APS, 1+1 2/4-Fiber Unidirectional Ring, or 2-Fiber MS Shared Protection Ring per ITU-T Recommendation G.841.

NI-004730 [**Required**] When the AGF functional device participates in point-to-point UPSR or BLSR protection, switching shall take place in 50 ms. These protection mechanisms shall be definable and selectable from the EMS, and shall offer the selection of revertive and non-revertive restoration mechanisms.

NI-004740 [**Required**] When the AGF functional device participates in point-to-point UPSR or BLSR protection and the selection of revertive restoration mechanisms shall have a revertive timer that is software programmable in a 30-second increment from 0 to 5 minutes, at a minimum.

NI-004750 [**Required**] The service restoration for a protection switch shall be automatic and accomplished without human or central management system intervention.

NI-004760 [**Required**] The protection switching mechanism shall be independent among separately managed network domains. A protection switch in one separately managed network domain shall not propagate or relay to another separately managed network domain.

NI-004770 [**Required**] The maximum detection time to determine if a signal's BER threshold is exceeded shall comply with Telcordia Technologies GR-253-CORE and ITU-T Recommendation G.783.

NI-004780 [**Required**] Once a decision is made to switch, the terminal circuit pack switching shall take place within 50 ms, as described in Telcordia Technologies GR-253-CORE and ITU-T Recommendation G.783.

NI-004790 [**Required**] Catastrophic failures on a user-definable Excessive BER (EBER) condition shall be detected by an equipment-protected circuit pack in a terminal within 10 ms as described in Telcordia Technologies GR-253-CORE and ITU-T Recommendation G.783.

NI-004800 [**Required**] When equipped, the AGF functional device shall be compliant with types and characteristics of SDH network protection architectures as defined in ITU-T G.841.

NI-004810 [**Required**] When equipped, the AGF functional device shall be compliant with interworking of SDH network protection architectures as defined in ITU-T Recommendation G.842.

10.3.4.10 AGF Functional Device Interoperability

The MSPP shall meet the following interoperability requirements:

NI-004820 [**Required**] The AGF functional device user interfaces, software, firmware, and hardware shall be fully compatible and interoperable with and without protection mechanisms of the OTS muxponder; OTS ROADM; ODXC; M13; Standard Terminal Interface (STI); Defense

Switched Network (DSN) Multifunction Switch (MFS); encryption devices; and DISN Provider (P), Provider Edge (PE), Aggregation Routers (ARs).

NI-004830 [**Required**] The AGF functional device cross-connects and interfaces shall be compatible with network-side STS, STM, or Lambda cross-connects at the OTS muxponder, OTS ROADM, and ODXC.

NI-004840 [**Required**] The AGF functional device cross-connects and interfaces at the AGF functional device shall be compatible with all protection switching at OTS muxponder, OTS ROADM, ODXC, M13, STI, DSN MFS, encryption devices, and DISN P, PE, and ARs.

10.3.4.11 AGF Functional Device Fault Management

The MSPP shall meet the following fault management requirements:

NI-004850 [**Required**] The AGF functional device shall send the appropriate AIS and RDI to adjacent systems, the EMS, and/or the higher level management system after detecting signal failure or degraded conditions for a specified alarm or indication activation time, as described in ANSI T1.231, Tables 2, 6, and 11.

NI-004860 [**Required**] The AGF functional device shall remove the appropriate AIS and RDI after the source system has cleared the signal failure or degraded condition for a specified alarm or indication activation time, as described in ANSI T1.231, Tables 2, 6, and 11.

NI-004870 [**Required**] Alarms shall indicate circuit-level or signal alarms, as well as alarms in the AGF functional device itself, such as Span Failure, LOS, Path Switch Complete/Fail, Laser Degradation, Card Failure, and Card Mismatch.

NI-004880 [**Required**] Standard SONET alarms shall be supported by the system, including LOS, LOP, LOF, Rx AIS, RDI, and RFI.

NI-004890 [**Required**] The AGF functional device shall indicate SONET timing synchronization failures. The AGF functional device shall give an alarm showing the inability to establish a PLL. The AGF functional device shall have the ability to monitor the BITS incoming references (BITS-A and BITS-B). The AGF functional device shall give an alarm when there is any timing change, e.g., a switch from BITS-A to BITS-B.

NI-004900 [**Required**] Each NE shall detect, report, and clear the following signal failure events or conditions: LOS, LOF, LOP, SEF, AIS, and OOF, according to ANSI T1.231.

NI-004910 [**Required**] The AGF functional device shall provide the following DS3 alarms and report them to the EMS: LOS and AIS (or blue alarm). Definitions are the same as with DS1. The AGF functional device shall be able to transmit and receive the Far-End Out of Frame (FEOOF) alarm for those AGF functional devices that transmit them. In addition, the AGF functional device shall be able to transmit and receive Far-End Alarm and Control (FEAC) signals. The FEAC option allows the AGF functional device to display far-end alarm and status

information via the FEAC channel and to transmit FEAC messages from the near end to the far end.

NI-004920 [**Required**] The AGF functional device shall provide the following SONET VT alarms and report them to the EMS: include signal label mismatch, receive unequipped, and Rx AIS. Signal label mismatch tells whether the VT payload is locked or floating. Receive unequipped indicates that the far-end SONET port has not been provisioned.

NI-004930 [**Required**] The AGF functional device shall provide the following DS1 alarms and report them to the EMS: AIS or yellow alarm, LOS, Remote Alarm Indication (RAI)/yellow alarm, and excess zeroes. Alarm Indication Signal is transmitted as a result of a received LOS. The RAI or yellow alarm is transmitted upstream to indicate a red alarm or LOS downstream. Alarms shall indicate which physical port is receiving or transmitting the alarm. The yellow or RAI alarm is for ESF circuits only. Excess zeroes alarm only applies to D4/Superframe circuits.

NI-004940 [**Required**] The AGF functional device shall have LEDs for minor, major, and critical alarms and the LED must be set and cleared when a alarm of the defined category is present or cleared as defined by Telcordia Technologies GR.253-CORE.

NI-004950 [**Required**] The AGF functional device shall provide alarm status with at least the following minimum information: reference number, date and time of occurrence, node name, card type/slot, severity (i.e., minor, major, critical, informational), and alarm status (set, clear, and transient).

10.3.4.12 AGF Functional Device Performance Monitoring

The MSPP shall meet the following performance monitoring requirements:

NI-004960 [**Required**] The AGF functional device shall provide a performance monitoring capability of all the supported interfaces (i.e., PDH, SONET, SDH) in accordance with Telcordia Technologies GR-253-CORE, and ITU-T Recommendation G.829.

NI-004970 [**Required**] The PDH performance monitoring shall provide ES, Severally SES, Unavailable Seconds, BP or CV, LOS, and AIS in accordance with Telcordia Technologies GR-820-CORE and ITU-T Recommendations G.826.

NI-004980 [**Required**] The SONET performance monitoring shall provide ES, SES, unavailable seconds, CV, LOS, AIS, and pointer adjustments in accordance with Telcordia Technologies GR-499-CORE.

NI-004990 [**Required**] The SDH performance monitoring shall provide ES, SES, unavailable seconds, CV, LOS, AIS, and pointer adjustments in accordance with ITU-T G.829.

NI-005000 [**Required**] The Ethernet performance monitoring shall provide Link availability time, various pack sizes, undersize packets, jumbo frames, frame alignment errors, frame check sequence errors, fragmentation, and CRC alignment errors in accordance with IEEE 802.3.

NI-005010 [**Required**] The optical card performance monitoring shall provide receive power, transmit power, bias current, low power threshold, and high power threshold in accordance with Telcordia Technologies GR-253-CORE.

NI-005020 [**Required**] All interfaces shall provide alarm thresholds for error rates that are determine to be degraded (10E-6) and failed (10E-3) and declare alarms based on the error rates to the user via the alarm in accordance with Telcordia Technologies GR-253-CORE and ITU-T Recommendation G.829.

10.3.4.13 AGF Functional Device

The MSPP shall meet the following functional requirements:

NI-005030 [**Required**] The AGF functional device shall perform hair-pinning and ADM functions in accordance with Telcordia Technologies GR-496-CORE.

NI-005040 [**Required**] The AGF functional device shall perform drop ADM functions in accordance with Telcordia Technologies GR-496-CORE.

NI-005050 [**Required**] The AGF functional device shall perform continued ADM functions in accordance with Telcordia Technologies GR-496-CORE.

NI-005060 [**Optional**] The AGF functional device shall perform drop and continue ADM functions in accordance with Telcordia Technologies GR-496-CORE.

NI-005070 [**Required**] The AGF functional device shall provide the ability to hub or nest lower DISN Access elements in a linear or ring configuration from user-side interfaces.

NI-005080 [**Optional**] The AGF functional device shall not use external connections for ring interconnection. Where multiple rings can be supported by a single shelf, connectivity between rings shall be accomplished via the switch matrix. No external connection between tributary interfaces shall be used to cross connect rings in the same bay.

NI-005090 [**Required**] The AGF functional device shall be protocol-transparent to incoming bit streams. Except for internetworking functions associated with Ethernet services within the AGF functional device, the AGF functional device shall not perform any user protocol conversions.

NI-005100 [**Required**] The AGF functional device shall not impart any errors onto the connections during cross-connects, grooming, or multiplexing.

NI-005110 [**Required**] The AGF functional device shall perform hair-pinning cross-connects without affecting the line capacity rate of the AGF functional device.

NI-005120 [**Required**] The AGF functional device shall send the appropriate AIS and RDI to adjacent AGF functional devices, the EMS, and/or higher level management systems after detecting signal failure or degraded conditions for a specified alarm or indication activation time per ANSI T1.231, Tables 2, 6 and 11.

NI-005130 [**Required**] The AGF functional device shall remove appropriate AIS and RDI after another AGF functional device has cleared the signal failure or degraded conditions for a specified alarm or indication activation time per ANSI T1.231, Tables 2, 6, and 11.

NI-005140 [**Optional**] The AGF functional device shall have internal local and remote terminal loopback capability per Telcordia Technologies GR-253-CORE, (R) 6-380.

NI-005150 [**Required**] The AGF functional device shall have a local and remote service loopback capability as per Telcordia Technologies GR-253-CORE, (R) 6-389.

NI-005160 [**Required**] The AGF functional device with DS1/E1 line terminations shall provide both DS1/E1 terminal and service loopback capabilities as per Telcordia Technologies GR 253 CORE, (O) 6-397.

NI-005170 [**Required**] The AGF functional device with DS3 line terminations shall provide both DS3 terminal and service loopback capabilities per Telcordia Technologies GR-253-CORE, (O) 6-397.

NI-005180 [**Optional**] The AGF functional device should support BER Testing using standard test patterns: PRBS15, PRBS20, PRBS23, QRSS, and ATL1s0s.

10.3.4.14 AGF Functional Device EMS

NI-005190 [**Required**] The AGF functional device EMS shall report PHY (Layer 1) statistics. Further, it shall report errors. It shall report all QoS parameters defined for the RPR as described in IEEE 802.17.

NI-005200 [**Required**] The AGF functional device EMS shall be able to track frame errors, P-Bit parity errors, C-Bit parity errors, and FEBE.

NI-005210 [**Required**] The AGF functional device EMS shall be able to provision the AGF functional device on all interfaces (i.e., PDH/SONET/SDH/Ethernet) and be able to provision a circuit using the different types of cross-connects (VT1.5, VC-11, VC-12, VC-3, VC-4, STS-1, STM-1, STS-3c, STM-4, STS-12c, STM-16, STS-48c, STM-64, and STS-192c).

NI-005220 [**Required**] The AGF functional device EMS shall be able to build protection topologies APS 1+1, UPSR, and BLSR.

NI-005230 [**Required**] The AGF functional device EMS shall be able to provision card parameters required for interoperability to interconnecting carrier systems; and interface framing format, and line type, line build out.

NI-005240 [**Required**] The AGF functional device EMS shall be able to provision alarms profiles according to network requirements (i.e., minor, major, critical, none service affecting, and none reporting).

NI-005250 [**Required**] The AGF functional device EMS shall be able to review and retrieve alarm and administration logs.

NI-005260 [**Required**] The AGF functional device EMS shall be able to set the alarm threshold on any interface (i.e., SD and SF).

NI-005270 [**Required**] The AGF functional device EMS shall be able to provision all administrated and security screens based on password level (i.e., network IP address, NE name, user accounts, and radius server).

10.3.4.15 Physical Design

NI-005280 [**Required**] All MSPP elements shall meet the EMC/EMI requirements defined in FCC Part 15 Class A.

NI-005290 [**Required**] All MSPP elements shall meet the EMC/EMI requirements defined in Telcordia Technologies GR-1089-CORE.

NI-005300 [**Required**] All MSPP elements shall meet the EMC/EMI requirements defined in ETSI EN 50082.

NI-005310 [**Required**] All MSPP elements shall meet the EMC/EMI requirements defined in ETSI EN 55022.

NI-005320 [**Required**] All MSPP elements shall meet the EMC/EMI requirements defined in ETSI EN 300-386.

NI-005330 [**Required**] All MSPP elements shall be designed to operate continuously in the following environment ranges without degradation. Temperature: 0 to +50°C, Humidity: 5 to 95 percent relative humidity, without condensation.

NI-005340 [**Required**] All MSPP elements shall be designed to be fully operational after transportation and/or storage in the following environment ranges: Temperature: -40 to +70°C, Humidity: 5 to 95 percent relative humidity, without condensation.

NI-005350 [**Required**] All MSPP elements shall be designed to operate continuously in the following environment range without degradation. Altitude: -100 to 15,000 ft AMSL.

NI-005360 [**Required**] All MSPP elements shall be designed to be fully operational after transportation and/or storage in the following environment range: Transport Altitude: -100 ft to +40,000 ft AMSL.

NI-005370 [**Required**] All MSPP elements shall adhere to NEBS Level 3 compliance standards for acceptable voltage ranges, EMI, and ESD safety, and shall be operable using standard 48V dc power as well as having redundant isolated power input feeds. For certain sites, an alternative ac/dc rectifier may need to be supplied to power the system and shall be able to switch 110/220V with redundant isolated power modules.

NI-005380 [**Required**] All MSPP elements shall be fully operational throughout the battery voltage range of -41.5 to -56 VDC.

NI-005390 [**Required**] All MSPP elements shall not be damaged and shall recover to normal performance following application of the following maximum transient voltages for the durations given (nominal voltage 48 VDC): 75 VP-P for 1 ms, 60 VP-P for 500 ms.

NI-005400 [**Required**] All MSPP elements shall be fully NEBS, Level 3 compliant.

NI-005410 [**Required**] All MSPP elements shall be designed to operate continuously in the following environment ranges without degradation. Temperature: 0 to +50°C, Humidity: 5 to 95 percent relative humidity, without condensation.

NI-005420 [**Required**] All MSPP elements shall be designed to be fully operational after transportation and/or storage in the following environment ranges: Temperature: -40 to +70°C, Humidity: 5 to 95 percent relative humidity, without condensation.

NI-005430 [**Required**] All MSPP elements shall be designed to operate continuously in the following environment range without degradation. Altitude: -100 to 15,000 ft AMSL.

NI-005440 [**Required**] All MSPP elements shall be designed to be fully operational after transportation and/or storage in the following environment range: Transport Altitude: -100 ft to +40,000 ft AMSL.

NI-005450 [**Required**] All MSPP elements shall adhere to NEBS level 3 compliance standards for acceptable voltage ranges, EMI, and ESD safety, and shall be operable using standard 48V dc power as well as having redundant isolated power input feeds. For certain sites, an alternative ac/dc rectifier may need to be supplied to power the system and shall be able to switch 110/220V with redundant isolated power modules.

NI-005460 [**Required**] All MSPP elements shall be fully operational throughout the battery voltage range of: -41.5 to -56 VDC.

NI-005470 [**Required**] All MSPP equipment shall have been tested and registered as compliant to the following electrical safety standards: UL-1950, EN60950, and IEC 60950.

10.3.4.16 AGF Functional Device Standards Compliance

The standards in effect when the equipment was first acquired are listed. Updates to the standards since that point in time are identified in brackets. When the manufacturer provides new components for the COTS items to the same device that satisfy updated standards, DISA will often purchase and install those components to accommodate growth, but will not replace existing components unless there is another reason to do so. As such, components will be operational within DISN that satisfy multiple versions of the standards. Testing will need to be undertaken using the standard release that applied to that component, where the revised standard cannot be satisfied by the original component. MSPPs shall meet the following standards:

NI-005480 [**Required**] ITU-T Recommendation G.651.1 (2007).

NI-005490 [**Required**] ITU-T Recommendation G.652 (10/2000) (Revised in 2005).

NI-005500 [**Required**] ITU-T Recommendation 694.1 (2002).

NI-005510 [**Required**] ITU-T Recommendation G.703 (2001).

NI-005520 [**Required**] ITU-T Recommendation G.707/Y.1322 (2007).

NI-005530 [**Required**] ITU-T Recommendation G.709/Y.1331.

NI-005540 [**Required**] ITU-T Recommendation G.711 (1988).

NI-005550 [**Required**] ITU-T Recommendation G.732 (1988).

NI-005560 [**Required**] ITU-T Recommendation G.783 (2006).

NI-005570 [**Required**] ITU-T Recommendation G.825 (2000).

NI-005580 [**Required**] ITU-T Recommendation G.829.

NI-005590 [**Required**] ITU-T Recommendation G.841 (1998).

NI-005600 [**Required**] ITU-T Recommendation G.842 (1997).

NI-005610 [**Required**] ITU-T Recommendation G.872 (2001).

NI-005620 [**Required**] ITU-T Recommendation G.957 (2006).

NI-005630 [**Required**] ITU-T Recommendation G.7041/Y-1303 (2003) (Revised in 2008).

NI-005640 [**Required**] ANSI T1.101.

NI-005650 [**Required**] ANSI T1.102-1999.

NI-005660 [**Required**] ANSI T1.105.1-2000.

NI-005670 [**Required**] ANSI T1.105.03-1994 (Revised 2003 (R2008)).

NI-005680 [**Required**] ANSI T1.105.06-2002 (R2007).

NI-005690 [**Required**] ANSI T1.107-2002 (R2006).

NI-005700 [**Required**] ANSI T1.231-1993 (Revised 2003 (R2007)).

NI-005710 [**Required**] ANSI T1.403-1999 (R2007).

NI-005720 [**Required**] ANSI T1.404-2002 (R2006).

NI-005730 [**Required**] Telcordia Technologies GR-253-CORE, Issue 3, September 2000 (Issue 5, October 2009).

NI-005740 [**Required**] Telcordia Technologies GR-496-CORE, Issue 1, December 1998, (Issue 2, August 2007).

NI-005750 [**Required**] Telcordia Technologies GR-499-CORE, Issue 2, December 1998 (Issue 3, September 2004).

NI-005760 [**Required**] Telcordia Technologies GR-820-CORE, Issue 2, December 1997.

NI-005770 [**Required**] IEEE 802.3-2008.

NI-005780 [**Required**] IEEE 802.1Q-2003.

NI-005790 [**Optional**] IEEE 802.17-2004, IEEE standard for information technology-telecommunications and information exchange between systems-local and metropolitan area networks-specific requirements-part 17: resilient packet ring (RPR) access method and physical layer specifications.

NI-005800 [**Required**] X3-230. ANSI FC-SB-3 and International Committee for Information Technology Standards (INCITS) 230:1994 [R2004].

NI-005810 [**Required**] British Standards Institute BS EN 60950-1 August 6, 2006.

NI-005820 [**Required**] IEC 60950-1, 2006.

NI-005830 [**Required**] CFR FCC Part 15, Class A.

NI-005840 [**Required**] Network Equipment - Building System (NEBS), Level 3.

NI-005850 [**Required**] Underwriters Laboratories, Inc. UL-1950, First Edition 1989.

10.3.5 M13 Multiplexer

10.3.5.1 Description

The M13 Multiplexer (Mux) functionally multiplexes DS1s into a DS3.

10.3.5.2 M13 Mux Electrical Interface

NI-005860 [**Required**] The M13 Mux shall support DS1 electrical interfaces that comply with ANSI T1.102.

NI-005870 [**Required**] The M13 Mux shall support channelized and unchannelized DS1 Superframe (SF) format and ESF format as specified in ANSI T1.403. The ability to read/write the ESF data link is required. The selection of format for any particular DS1 interface shall be user-selectable.

NI-005880 [**Required**] The M13 Mux shall support AMI and B8ZS framing format as specified in ANSI T1.403. The selection of framing format for any particular DS1 interface shall be user-selectable.

NI-005890 [**Required**] The M13 Mux shall support both in-band and out-band (FDL) loop-up and loop-down codes as specified in ANSI T1.403.

NI-005900 [**Required**] The M13 Mux shall support FDL status messages and respond according as specified in ANSI T1.403.

NI-005910 [**Required**] The M13 Mux shall support unframed DS1 electrical signals.

NI-005920 [**Required**] The M13 Mux shall support electrical interfaces that shall comply with ITU-T Recommendation G.703.

NI-005930 [**Required**] The M13 Mux shall support DS1 bit rate of 1.544 Mbps +/- 32 ppm as specified in ANSI T1.101.

NI-005940 [**Required**] The M13 Mux shall support DS1 100 ohms cable with maximum length of 655 feet as specified in ITU-T Recommendation G.703.

NI-005950 [**Required**] The M13 Mux shall support DS3 electrical tributary interfaces that comply with ANSI T1.102.

NI-005960 [**Required**] The M13 Mux DS3 interface shall support DS3 pulse shape that meets both ITU-T G.703 and Telcordia Technologies GR-499-CORE. Older Promina® equipment will not work correctly on just meeting the pulse shape of Telcordia Technologies GR-499-CORE. The interface can be software selectable to support both pulse shapes.

NI-005970 [**Required**] The M13 Mux shall support channelized DS3 signals in either M13 or C-bit parity formats per ANSI T1.107 and T1.404. The selection of format for any particular DS3 interface shall be user selectable.

NI-005980 [**Required**] The M13 Mux shall support DS3 C-bit far-end alarm and control signal to support alarm/status messages and loopback control on the DS3 and/or individual DS1 as specified in ANSI T1.107 and ANSI T1.404.

NI-005990 [**Required**] The M13 Mux shall support DS3 bit rate of 44.736 Mbps +/- 20 ppm as specified in ANSI T1.101.

NI-006000 [**Required**] The M13 Mux shall be able to provision, monitor, and detect faults, and restore electrical (DS1, E1, DS3) services in a standardized and automated fashion.

NI-006010 [**Required**] The M13 Mux shall be able to multiplex 28 DS1s into a single DS3.

10.3.5.3 M13 Mux Interface Performance

The M13 Mux shall meet the following interface requirements:

NI-006020 [**Required**] The jitter tolerance measured at the DS3 interface on the M13 shall be at least 5 UIpp between 10 Hz and 2.3 x 103 Hz, and at least 0.1 UIpp between 60 x 10^3 and 200 x 10^3 Hz as per Figure 7-1 in Telcordia Technologies TR-499.

NI-006030 [**Required**] The jitter transfer measured between an input DS1 interface and the corresponding output DS1 interface on the M13 (with its DS3 signal looped back) shall be less than the jitter transfer mask shown in Figure 7-4 of Telcordia Technologies GR-499.

NI-006040 [**Required**] The jitter generation for the DS1 interface on the M13 shall be less than 0.7 UIpp as per ANSI T1.105.03s, Section 6.1.1.1.

10.3.5.4 M13 Mux Equipment Redundancy

NI-006050 [**Required**] The M13 Mux shall support a redundant processor in an active/standby mode.

NI-006060 [**Required**] The M13 Mux shall support redundant power supply/electrical feeds.

10.3.5.5 M13 Mux Fault Management

NI-006070 [**Required**] The M13 Mux shall send the appropriate AIS and RDI to adjacent systems, the EMS, and/or the higher level management system after detecting signal failure or degraded conditions for a specified alarm or indication activation time, as described in ANSI T1.231, Tables 2, 6, and 11.

NI-006080 [**Required**] The M13 Mux shall remove the appropriate AIS and RDI after the source system has cleared the signal failure or degraded condition for a specified alarm or indication activation time, as described in ANSI T1.231, Tables 2, 6, and 11.

NI-006090 [**Required**] The M13 Mux shall support Alarms that indicate circuit-level or signal alarms, as well as alarms in the M13 itself, such as LOS, AIS, LOF, and RDI.

NI-006100 [**Required**] The M13 Mux shall provide the following DS3 alarms and report them to the EMS: LOS and AIS (or blue alarm). Definitions are the same as with DS1. The M13 shall be able to transmit and receive the FEOOF alarm for those network elements (NEs) that transmit them. In addition, the M13 shall be able to transmit and receive FEAC signals. The FEAC option allows the M13 to display far-end alarm and status information via the FEAC channel and to transmit FEAC messages from the near end to the far end.

NI-006110 [**Required**] The M13 Mux shall provide the following DS1 alarms and report them to the EMS: AIS or yellow alarm, LOS, RAI/yellow alarm, and excess zeroes. Alarm Indication Signal is transmitted as a result of a received LOS. The RAI or yellow alarm is transmitted upstream to indicate a red alarm or LOS downstream. Alarms shall indicate which physical port is receiving or transmitting the alarm. The yellow or RAI alarm is for ESF circuits only. The excess zeroes alarm only applies to D4/Superframe circuits.

NI-006120 [**Required**] The M13 Mux shall have LEDs for minor, major, and critical alarms, and the LED must be set and cleared when an alarm of the defined category is present or cleared, as defined by Telcordia Technologies GR-253-CORE.

NI-006130 [**Required**] The M13 Mux shall provide alarm status with at least the following minimum information: reference number, date and time of occurrence, node name, card type/slot, severity (i.e., minor, major, critical, and informational), and alarm status (i.e., set, clear, and transient).

10.3.5.6 M13 Mux Performance Monitoring

NI-006140 [**Required**] The M13 Mux shall provide a performance monitoring capability on the DS1 and DS3 interfaces in accordance with Telcordia Technologies GR-820-CORE.

NI-006150 [**Required**] The M13 Mux shall support DS1 and DS3 performance monitoring that provides ES, SES, Unavailable Seconds, BP or CV, LOS, and AIS in accordance with Telcordia Technologies GR-499-CORE and GR-820-CORE.

NI-006160 [**Required**] All M13 Mux interfaces shall provide alarm thresholds for error rates that are determined to be degraded (10E-6) and failed (10E-3) and declare alarms based on the error rates to the user via the alarm in accordance with Telcordia Technologies GR-820-CORE.

10.3.5.7 M13 MUX Alarm

NI-006170 [**Required**] The M13 Mux shall send the appropriate AIS and RDI to adjacent Network Encyrption System (NES), the EMS, and/or higher level management systems after detecting signal failure or degraded conditions for a specified alarm or indication activation time as per ANSI T1.231, Tables 2, 6, and 11.

NI-006180 [**Required**] The M13 Mux shall remove appropriate AIS and RDI after another NE has cleared the signal failure or degraded conditions for a specified alarm or indication activation time as per ANSI T1.231, Tables 2, 6, and 11.

NI-006190 [**Required**] The M13 Mux shall have a DS1 and DS3 loopback capability per Telcordia Technologies GR-253-CORE, (R) 6-397.

NI-006200 [**Desired**] The M13 Mux should support BER testing using standard test patterns; PRBS15, PRBS20, PRBS23, QRSS, and ATL1s0s.

10.3.5.8 M13 EMS

All EMS requirements are contained in Section 15.

10.3.5.9 M13 Mux Physical Design

NI-006210 [**Required**] All M13 Mux elements shall meet the EMC/EMI requirements defined in FCC Part 15 Class A.

NI-006220 [**Required**] All M13 Mux elements shall meet the EMC/EMI requirements defined in Telcordia Technologies GR-1089-CORE.

NI-006230 [**Required**] All M13 Mux elements shall meet the EMC/EMI requirements defined in ETSI EN 50082.

NI-006240 [**Required**] All M13 Mux elements shall meet the EMC/EMI requirements defined in ETSI EN 55022.

NI-006250 [**Required**] All M13 Mux elements shall meet the EMC/EMI requirements defined in ETSI EN 300-386.

NI-006260 [**Required**] All M13 Mux elements shall be designed to operate continuously in the following environment ranges without degradation. Temperature: 0 to +50°C, Humidity: 5 to 95 percent relative humidity, without condensation.

NI-006270 [**Required**] All M13 Mux elements shall be designed to be fully operational after transportation and/or storage in the following environment ranges: Temperature: -40 to +70°C, Humidity: 5 to 95 percent relative humidity, without condensation.

NI-006280 [**Required**] All M13 Mux elements shall be designed to operate continuously in the following environment range without degradation: Altitude: -100 to 15,000 ft AMSL.

NI-006290 [**Required**] All M13 Mux elements shall be designed to be fully operational after transportation and/or storage in the following environment range: Transport Altitude: -100 ft to +40,000 ft AMSL.

NI-006300 [**Required**] All M13 Mux elements shall adhere to NEBS Level 3 compliance standards for acceptable voltage ranges, EMI, and ESD safety, and shall be operable using standard 48V dc power as well as having redundant isolated power input feeds. For certain sites, an alternative ac/dc rectifier may need to be supplied to power the system and shall be able to switch 110/220V with redundant isolated power modules.

NI-006310 [**Required**] All M13 Mux elements shall be fully operational throughout the battery voltage range of -41.5 to -56 VDC.

NI-006320 [**Required**] All M13 Mux elements shall not be damaged and shall recover to normal performance following application of the following maximum transient voltages for the durations given (nominal voltage 48 VDC): 75 VP-P for 1 ms, 60 VP-P for 500 ms.

NI-006330 [**Required**] All M13 Mux elements shall be fully NEBS, Level 3 compliant.

NI-006340 [**Required**] All M13 Mux elements shall be designed to operate continuously in the following environment ranges without degradation. Temperature: 0 to +50°C, Humidity: 5 to 95 percent relative humidity, without condensation.

NI-006350 [**Required**] All M13 Mux elements shall be designed to be fully operational after transportation and/or storage in the following environment ranges: Temperature: -40 to +70°C, Humidity: 5 to 95 percent relative humidity, without condensation.

NI-006360 [**Required**] All M13 Mux elements shall be designed to operate continuously in the following environment range without degradation. Altitude: -100 to 15,000 ft AMSL.

NI-006370 [**Required**] All M13 Mux elements shall be designed to be fully operational after transportation and/or storage in the following environment range: Transport Altitude: -100 ft to +40,000 ft AMSL.

NI-006380 [**Required**] All M13 Mux elements shall adhere to NEBS Level 3 compliance standards for acceptable voltage ranges, EMI, and ESD safety, and shall be operable using standard 48V dc power as well as having redundant isolated power input feeds. For certain sites, an alternative ac/dc rectifier may need to be supplied to power the system and shall be able to switch 110/220V with redundant isolated power modules.

NI-006390 [**Required**] All M13 Mux elements shall be fully operational throughout the battery voltage range of: -41.5 to -56 VDC.

NI-006400 [**Required**] All M13 Mux equipment shall have been tested and registered as compliant to the following electrical safety standards: UL-1950, EN60950, IEC 60950, and C22-2 No. 950.

10.3.5.10 M13 Mux Standards Compliance

The standards in effect when the equipment was first acquired are listed. Updates to the standards since that point in time are identified in brackets. When the manufacturer provides new components for the COTS items to the same device that satisfy updated standards, DISA will often purchase and install those components to accommodate growth, but will not replace existing components unless there is another reason to do so. As such, components will be operational within DISN that satisfy multiple versions of the standards. Testing will need to be undertaken using the standard release that applied to that component, where the revised standard cannot be satisfied by the original component. The M13 Mux shall meet the following standards:

NI-006410 [**Required**] ITU-T Recommendation G.703 (2001).

NI-006420 [**Required**] ITU-T Recommendation G.711 (1988).

NI-006430 [**Required**] ANSI T1.102-1999.

NI-006440 [**Required**] ANSI T1.105.03-1994 (Revised 2003 (R2008)).

NI-006450 [**Required**] ANSI T1.107-2002 (R2006).

NI-006460 [**Required**] ANSI T1.231-1993 (Revised 2003 (R2007)).

NI-006470 [**Required**] ANSI T1.403-1999 (R2007).

NI-006480 [**Required**] ANSI T1.404-2002 (R2006).

NI-006490 [**Required**] Telcordia Technologies GR-253-CORE, Issue 3, September 2000 (Issue 4, December 2005).

NI-006500 [**Required**] Telcordia Technologies GR-499-CORE, Issue 2, December 1998 (Issue 3, September 2004).

NI-006510 [**Required**] Telcordia Technologies GR-820-CORE, Issue 2, December 1997.

NI-006520 [**Required**] ETSI EN-300-386.

NI-006530 [**Required**] British Standards Institute BS EN 60950-1, August 6, 2006.

NI-006540 [**Required**] IEC 60950-1, 2006.

NI-006550 [**Required**] CFR FCC Part 15, Class A.

NI-006560 [**Required**] Network Equipment GR-637 - Building System (NEBS), Level 3.

NI-006570 [**Required**] Underwriters Laboratories, Inc. UL-1950, First Edition 1989.

10.3.6 Serial TDM Multiplexer

10.3.6.1 Description

The serial TDM Mux multiplexes user serial synchronous and asynchronous data interfaces and 2-wire and 4-wire analog into one or more aggregated higher bandwidth network interface trunks. These services are currently provided by DISA within the DISN using the Promina nodes and D4 channel banks but they may be offered by a similar IP-based device in the future. The network interface trunks supporting these services may be provided via DS1, DS3, E1, E3, Ethernet, FE, GbE or serial data transport as required.

The data transport services offer fixed data rates, fixed end-to-end delay. Data services are offered via the following interfaces:

- RS-232.
- RS-422/449.
- RS-530.
- V.35.
- Conditioned Diphase.

For analog voice users, the serial TDM multiplexer supports foreign exchange (FX) signaling for extending DSN connectivity to analog stations. The TDM multiplexer includes echo cancellation to provide acceptable echo QoS to voice users. The analog services also support fax and modem bypass. Some of the voice services are:

- FX, office and station unit, with ground start, loop start, automatic ringdown.
- 2-wire and 4-wire Ear and Mouth (E&M) signaling.

10.3.6.2 Serial TDM Mux Network Interface

NI-006580 [**Required**] The serial TDM Mux shall support DS1 electrical interfaces that comply with ANSI T1.102.

NI-006590 [**Required**] The serial TDM Mux shall support channelized and unchannelized DS1 SF format and ESF format as specified in ANSI T1.403. The ability to read or write the ESF data link is required. The selection of format for any particular DS1 interface shall be user selectable.

NI-006600 [**Required**] The serial TDM Mux shall support AMI and B8ZS framing format as specified in ANSI T1.403. The selection of framing format for any particular DS1 interface shall be user selectable.

NI-006610 [**Required**] The serial TDM Mux shall support both in-band and out-band (FDL) loop-up and loop-down codes as specified in ANSI T1.403.

NI-006620 [**Required**] The serial TDM Mux shall support FDL status messages and respond as specified in ANSI T1.403.

NI-006630 [**Required**] The serial TDM Mux shall support unframed DS1 electrical signals.

NI-006640 [**Required**] The electrical interface shall comply with ITU-T Recommendation G.703.

NI-006650 [**Required**] The serial TDM Mux shall support DS1 bit rate of 1.544 Mbps +/- 32 ppm, as specified in ANSI T1.101.

NI-006660 [**Required**] The serial TDM Mux shall support DS1 100 ohms cable with maximum length of 655 feet, as specified in ITU-T Recommendation G.703.

NI-006670 [**Required**] The serial TDM Mux shall support DS3 electrical tributary interfaces that comply with ANSI T1.102-1993.

NI-006680 [**Required**] The jitter generation for the DS1 interface on the TDM multiplexer shall be less than 0.7 UIpp per ANSI T1.105.03s, Section 6.1.1.1.

NI-006690 [**Required**] Each alarm state shall be reported to the EMS.

NI-006700 [**Required**] The serial TDM Mux DS3 interface shall support DS3 pulse shape that meets both ITU-T Recommendation G.703 and Telcordia Technologies GR-499-CORE. Older Promina equipment will not work correctly on just meeting the pulse shape of Telcordia Technologies GR-499-CORE. The interface can be software selectable to support both pulse shapes.

NI-006710 [**Required**] The serial TDM Mux shall support channelized DS3 signals in either M13 or C-bit parity formats per ANSI T1.107 and T1.404. The selection of format for any particular DS3 interface shall be user selectable.

NI-006720 [**Required**] The serial TDM Mux shall support DS3 C-bit far-end alarm and control signal to support alarm/status messages and loopback control on the DS3 and/or individual DS1 as specified in ANSI T1.107 and ANSI T1.404.

NI-006730 [**Required**] The serial TDM Mux shall support DS3 bit rate of 44.736 Mbps +/- 20 ppm as specified in ANSI T1.101.

NI-006740 [**Required**] The serial TDM Mux shall be able to provision, monitor, and detect faults, and restore electrical (DS1, E1, DS3) services in a standardized and automated fashion.

NI-006750 [**Optional**] The serial TDM Mux shall support STS-1 (EC-1) electrical interfaces that comply with specifications and pulse masks as defined in Telcordia Technologies GR-253-CORE Chapter 4.4, and ANSI T1.102.

NI-006760 [**Required**] The serial TDM Mux shall support E3 electrical tributary interfaces that comply with ITU-T Recommendation G.703.

NI-006770 [**Required**] The serial TDM Mux shall support channelized and unchannelized E3 signals using line coding of HDB-3.

NI-006780 [**Required**] The serial TDM Mux shall support E3 bit rate of 34.368 Mbps +/- 20 ppm as specified in ITU-T Recommendation G.703.

NI-006790 [**Required**] The serial TDM Mux shall provide and support the MIL-STD 188c-200 Conditioned Diphase interface at the data rates specified below.

NI-006800 [**Required**] The serial TDM Mux shall provide interfaces for Ethernet and FE services in conformance with IEEE 802.3 for Ethernet LAN interfaces.

NI-006810 [**Required**] The serial TDM Mux shall provide interfaces for Ethernet, FE, and GbE Services in conformance with IEEE 802.3 for Ethernet LAN interfaces.

NI-006820 [**Required**] The serial TDM Mux shall not, by default, perform any Layer 3 IP routing.

NI-006830 [**Required**] The serial TDM Mux shall be able to provision, monitor, and detect faults, and restore Ethernet services in a standardized and automated fashion.

NI-006840 [**Required**] The serial TDM Mux shall selectively provide QoS/CoS for Ethernet Services according to IEEE 802.1Q.

NI-006850 [**Optional**] Available Ethernet services shall include RPR (IEEE 802.17b), GFP (ITU-T Recommendation G.7041/Y.1303), Hardware LCAS, and VCAT.

NI-006860 [**Required**] Ethernet and FE services on SONET shall support GFP (ITU-T Recommendation G.7041/Y.1303), hardware LCAS, low order VCAT (VT1.5), high order (STS-1) VCAT, and CCAT; STS-1 and STS-3c.

NI-006870 [**Required**] The serial TDM Mux shall selectively provide point-to-point Ethernet services with dedicated non-shared bandwidth without queuing or buffering Ethernet frames.

10.3.6.3 Serial TDM Multiplexer Interface

The serial TDM Mux shall support the following interface requirements. The serial TDM Mux shall minimally support a serial 'data' user side interface. The network interfaces shall minimally be either an Ethernet/IP or DS1 interface.

Analog interfaces (optional) shall meet:

NI-006880 [**Required**] An analog interface shall be able to support switched service close-end loop start signaling per Telcordia Technologies TR-NWT-000335, Paragraph 4.2.

NI-006890 [**Required**] An analog interface shall be able to support switched service open-ended loop start signaling per Telcordia Technologies TR-NWT-000335, Paragraph 4.2.

NI-006900 [**Required**] An analog interface shall be able to support switched service close-end ground start signaling per Telcordia Technologies TR-NWT-000335, Paragraph 4.3.

NI-006910 [**Required**] An analog interface shall be able to support switched service open-end ground start signaling per Telcordia Technologies TR-NWT-000335, Paragraph 4.3.

NI-006920 [**Required**] An analog interface shall be able to support switched service 2-wire E&M signaling per Telcordia Technologies TR-NWT-000335, Paragraph 4.4.

NI-006930 [**Required**] An analog interface shall be able to support switched service 4-wire E&M signaling per Telcordia Technologies TR-NWT-000335, Paragraph 4.4.

NI-006940 [**Required**] An analog interface shall be able to support switched service SF signaling per Telcordia Technologies TR-NWT-000335, Paragraph 4.7.

NI-006950 [**Required**] An analog interface shall be able to support special access voice grade 1 (VG1) service per Telcordia Technologies TR-NWT-000335, Paragraph 5.3.1.

NI-006960 [**Required**] An analog interface shall be able to support special access voice grade 2 (VG2) service per Telcordia Technologies TR-NWT-000335, Paragraph 5.3.2.

NI-006970 [**Required**] An analog interface shall be able to support special access voice grade 3 (VG3) service per Telcordia Technologies TR-NWT-000335, Paragraph 5.3.3.

NI-006980 [**Required**] An analog interface shall be able to support special access voice grade 4 (VG4) service per Telcordia Technologies TR-NWT-000335, Paragraph 5.3.4.

NI-006990 [**Required**] An analog interface shall be able to support special access voice grade 5 (VG5) service per TR-NWT-000335, Paragraph 5.3.5.

NI-007000 [**Required**] An analog interface shall be able to support special access voice grade 6 (VG6) service per Telcordia Technologies TR-NWT-000335, Paragraph 5.3.6.

Serial data interface (required) shall meet:

NI-007010 [**Required**] An data interface shall support RS-232 up to 19.2 Kbps using an EIA/TIA-232-F interface. Both Data Communication Equipment (DCE) and data terminal equipment (DTE) connections shall be supported.

NI-007020 [**Required**] An data interface shall support up to 6 Mbps using an RS-422/RS-449 interface. Both DCE and DTE connections shall be supported.

NI-007030 [**Required**] An data interface shall support up to 2 Mbps per second using an RS-530 interface. Both DCE and DTE connections shall be supported.

NI-007040 [**Required**] An data interface shall support up to 6 Mbps per second using a conditioned diphase interface. Both DCE and DTE connections shall be supported.

NI-007050 [**Required**] A data interface shall support up to 64 kbps using a V.35 interface. Both DCE and DTE connections shall be supported.

DS1 Network interface (optional) shall meet:

NI-007060 [**Required**] The DS1 requirement in Section 10.3.6.3 shall apply for user interfaces as well as the network interface.

NI-007070 [**Required**] The DS1 user side interfaces shall support fractional T1 services of n x 64 up to at least 768 kbps.

NI-007080 [**Required**] The serial TDM Mux shall be able to assign DS0s into any slot within a DS1 to create inverse multiplexer function.

NI-007090 [**Required**] For the user-side interfaces, the serial TDM Mux shall be able to clock data rates selectable from 1 bps to 6 mbps.

NI-007100 [**Required**] For the user-side interfaces, the serial TDM Mux shall be able to clock and transport data at rates selectable among the following bps rates:

200	3,600	12,800	32,000	76,800	168,000	384,000	1,024,000
400	4,800	14,400	38,400	86,400	192,000	448,000	1,184,000
800	6,400	16,000	48,000	96,000	224,000	512,000	1,344,000
1,200	7,200	16,800	56,000	112,000	230,400	672,000	1,536,000
1,800	8,000	19,200	57,600	115,200	256,000	768,000	1,544,000
2,400	9,600	24,000	64,000	128,000	288,000	772,000	2,048,000
3,200	12,000	28,800	72,000	144,000	336,000	896,000	

IP network interfaces shall meet IP interface requirements specified in Section 11.2.3.

10.3.6.4 Serial TDM Mux Equipment Redundancy

NI-007110 [**Required**] The serial TDM Mux shall support redundant processor in an active/standby mode with standby diagnostics status indicated locally and via the EMS.

NI-007120 [**Required**] The serial TDM Mux shall support redundant power supply and indicate their individual locally and via the EMS. Each supply shall be capable of carrying the entire load and shall have separate electrical feeds.

10.3.6.5 Serial TDM Mux Fault Management

NI-007130 [**Required**] The serial TDM Mux shall send the appropriate AIS and RDI to adjacent systems, the EMS, and/or the higher level management system after detecting signal failure or degraded conditions for a specified alarm or indication activation time, as described in ANSI T1.231, Tables 2, 6, and 11.

NI-007140 [**Required**] The serial TDM Mux shall remove the appropriate AIS and RDI after the source system has cleared the signal failure or degraded condition for a specified alarm or indication activation time, as described in ANSI T1.231, Tables 2, 6, and 11.

NI-007150 [**Required**] Alarms shall indicate circuit-level or signal alarms, as well as alarms in the serial TDM Mux itself, such as LOS, AIS, LOF, and RDI.

NI-007160 [**Required**] The serial TDM Mux shall provide the following DS1 alarms and report them to the EMS: AIS or yellow alarm, LOS, RAI/yellow alarm, and excess zeroes. Alarm Indication Signal is transmitted as a result of a received LOS. The RAI or yellow alarm is transmitted upstream to indicate a red alarm or LOS downstream. Alarms shall indicate which physical port is receiving or transmitting the alarm. The yellow or RAI alarm is for ESF circuits only. An excess zeroes alarm only applies to D4/super frame circuits.

NI-007170 [**Required**] The serial TDM Mux shall have LEDs for minor, major, and critical alarms, and the LED must be set and cleared when an alarm of the defined category is present or cleared, as defined by Telcordia Technologies GR-253-CORE.

NI-007180 [**Required**] The serial TDM Mux shall provide alarm status with at least the following minimum information: reference number, date and time of occurrence, node name, card type/slot, severity (i.e., minor, major, critical, and informational), alarm status (i.e., set, clear, and transient).

NI-007190 [**Required**] All interfaces shall provide alarm thresholds for error rates that are determined to be degraded (10E-6) and failed (10E-3) and declare alarms based on the error rates to the user via the alarm in accordance with Telcordia Technologies GR-820-CORE.

10.3.6.6 Serial TDM Mux Performance Monitoring

NI-007200 [**Required**] The serial TDM Mux shall provide a performance monitoring capability on all the interfaces in accordance with Telcordia Technologies GR-820-CORE.

NI-007210 [**Required**] The DS1 performance monitoring shall provide ES, SES, unavailable seconds, BP or CV, LOS, and AIS in accordance with Telcordia Technologies GR-499-CORE and GR-820-CORE.

10.3.6.7 Serial TDM Mux Network Element

NI-007220 [**Required**] The serial TDM Mux shall send the appropriate AIS and RDI to adjacent NEs, the EMS, and/or higher level management systems after detecting signal failure or degraded conditions for a specified alarm or indication activation time as per ANSI T1.231, Tables 2, 6 and 11.

NI-007230 [**Required**] The serial TDM Mux shall remove appropriate AIS and RDI after another NE has cleared the signal failure or degraded conditions for a specified alarm or indication activation time per ANSI T1.231, Tables 2, 6, and 11.

NI-007240 [**Required**] The serial TDM Mux shall have a DS1 loopback capability per Telcordia Technologies GR-253-CORE, (R) 6-397.

10.3.6.8 Serial TDM Mux EMS

EMS requirements are contained in Section 15.

10.3.6.9 Serial TDM Mux Physical Design

NI-007250 [**Required**] All serial TDM Mux shall meet the EMC/EMI requirements defined in FCC Part 15 Class A.

NI-007260 [**Required**] All serial TDM Mux shall meet the EMC/EMI requirements defined in Telcordia Technologies GR-1089-CORE.

NI-007270 [**Required**] All serial TDM Mux shall meet the EMC/EMI requirements defined in ETSI EN 50082.

NI-007280 [**Required**] All serial TDM Mux shall meet the EMC/EMI requirements defined in ETSI EN 55022.

NI-007290 [**Required**] All serial TDM Mux shall meet the EMC/EMI requirements defined in ETSI EN 300-386.

NI-007300 [**Required**] All serial TDM Mux shall be designed to operate continuously in the following environment ranges without degradation: Temperature: 0 to +50°C, Humidity: 5 to 95 percent relative humidity, without condensation.

NI-007310 [**Required**] All serial TDM Mux shall be designed to be fully operational after transportation and/or storage in the following environment ranges: Temperature: -40 to +70°C, Humidity: 5 to 95 percent relative humidity, without condensation.

NI-007320 [**Required**] All serial TDM Mux shall be designed to operate continuously in the following environment range without degradation: Altitude: -100 to 15,000 ft AMSL.

NI-007330 [**Required**] All serial TDM Mux shall be designed to be fully operational after transportation and/or storage in the following environment range: Transport Altitude: -100 ft to +40,000 ft AMSL.

NI-007340 [**Required**] All serial TDM Mux shall adhere to NEBS Level 3 compliance standards for acceptable voltage ranges, EMI, and ESD safety, and shall be operable using standard 48V dc power as well as having redundant isolated power input feeds. For certain sites, an alternative ac/dc rectifier may need to be supplied to power the system and shall be able to switch 110/220V with redundant isolated power modules.

NI-007350 [**Required**] All serial TDM Mux shall be fully operational throughout the battery voltage range of -41.5 to -56 VDC.

NI-007360 [**Required**] All serial TDM Mux shall not be damaged and recover to normal performance following application of the following maximum transient voltages for the durations given (nominal voltage 48 VDC): 75 VP-P for 1 ms, 60VP-P for 500 ms.

NI-007370 [**Required**] All serial TDM Mux shall be fully NEBS, Level 3 compliant.

NI-007380 [**Required**] All serial TDM Mux shall be designed to operate continuously in the following environment ranges without degradation. Temperature: 0 to +50°C, Humidity: 5 to 95 percent relative humidity, without condensation.

NI-007390 [**Required**] All serial TDM Mux shall be designed to be fully operational after transportation and/or storage in the following environment ranges: Temperature: -40 to +70°C, Humidity: 5 to 95 percent relative humidity, without condensation.

NI-007400 [**Required**] All serial TDM Mux shall be designed to operate continuously in the following environment range without degradation. Altitude: -100 to 15,000 ft AMSL.

NI-007410 [**Required**] All serial TDM Mux shall be designed to be fully operational after transportation and/or storage in the following environment range: Transport Altitude: -100 ft to +40,000 ft AMSL.

NI-007420 [**Required**] All serial TDM Mux shall adhere to NEBS level 3 compliance standards for acceptable voltage ranges, EMI, and ESD safety, and shall be operable using standard 48V dc power as well as having redundant isolated power input feeds. For certain sites, an alternative ac/dc rectifier may need to be supplied to power the system and shall be able to switch 110/220V with redundant isolated power modules.

NI-007430 [**Required**] All serial TDM Mux shall be fully operational throughout the battery voltage range of: -41.5 to -56 VDC.

NI-007440 [**Required**] All equipment shall have been tested and register as compliant to the following electrical safety standards: UL-1950, EN60950, and IEC 60950.

10.3.6.10 Serial TDM Mux Standards Compliance

The standards in effect when the equipment was first acquired are listed. Updates to the standards since that point in time are identified in brackets. When the manufacturer provides new components for the COTS items to the same device that satisfy updated standards, DISA will often purchase and install those components to accommodate growth, but will not replace existing components unless there is another reason to do so. As such, components will be operational within DISN that satisfies multiple versions of the standards. Testing will need to be undertaken using the standard release that applied to that component, where the revised standard cannot be satisfied by the original component.

NI-007450 [**Required**] ITU-T Recommendation G.703 (2001).

NI-007460 [**Required**] ITU-T Recommendation G.711 (1988).

NI-007470 [**Required**] ANSI T1.102-1999.

NI-007480 [**Required**] ANSI T1.105.03-1994 [Revised 2003 (R2008)].

NI-007490 [**Required**] ANSI T1.107-2002 (R2006), Digital Hierarchy – Formats Specifications.

NI-007500 [**Required**] ANSI T1.231-1993 [Revised 2003 (R2007)].

NI-007510 [**Required**] ANSI T1.403-1999 (R2007).

NI-007520 [**Required**] ANSI T1.404-2002 (R2006).

NI-007530 [**Required**] Telcordia Technologies GR-253-CORE, Issue 3, September 2000 (Issue 4, December 2005).

NI-007540 [**Required**] Telcordia Technologies GR-499-CORE, Issue 2, December 1998 (Issue 3, September 2004).

NI-007550 [**Required**] Telcordia Technologies GR-820-CORE.

NI-007560 [**Required**] EIA/TIA-232-E (January 1991) (superseded by TIA-232-F).

NI-007570 [**Required**] TIA-422-B (May 1994) (ANSI/TIA/EIA-422-B-1994) (R2000) (R2005).

NI-007580 [**Required**] EIA-449 (January 2000).

NI-007590 [**Required**] TIA-530-A (June 1992) (ANSI/TIA/EIA-530-A-92) (R98) (R2003).

NI-007600 [**Required**] ETSI EN-300-386.

NI-007610 [**Required**] British Standards Institute, August 6, 2006 BS EN 60950-1.

NI-007620 [**Required**] IEC 60950-1, 2006.

NI-007630 [**Required**] CFR FCC Part 15, Class A.

NI-007640 [**Required**] Network Equipment - Building System (NEBS), Level 3.

NI-007650 [**Required**] Underwriters Laboratories, Inc. UL-1950, First Edition, 1989.

10.3.7 Serial to IP (STI)

NI-007660 [**Required: STI**] Serial to IP (STI) technologies which feed into DCA equipment have these requirements, based on replacing the TDM equipment described in Section 10.3.6 and meeting the customer technology standards of 10.3.6 while providing an IP output interface:

a. (Trunk/Output side only) Fast Ethernet (IEEE 802.3u Carrier Sense Multiple Access with Collision Detection CSMA-CD) Ethernet 10/100 Mbps.

b. T1 Channelized/Clear 1.536 Mps.

c. European Basic Multplex Rate (E1) Channelized/Clear 2.048 Mps.

d. ISDN PRI 23B + D channels.

e. (Optional) E3 Clear 34.368 Mps.

f. (Optional) T3 Clear 44.736 Mps.

g. Electronic Industries Alliance (EIA)-530 Serial – up to 12.288 Mbps (Optional) 16.384Mbps.

h. EIA 530A.

i. RS-232 (Synchronous 1.2 to 64 Kbps).

j. RS-422 (Synchronous 9.6 kbps to 8192 Mbps).

k. RS-530 (Synchronous 9.6 kbps to 8192 Mbps).

l. RS-232 (Asynchronous 75 bps to 19.2 Kbps).

m. RS-422 Up to 2.048 Mps.

n. V.35 (Synchronous).

o. Conditioned Diphase (16-2048 kbps).

p. IETF RFC-based encapsulation methods, SAToP (optional CESoPSN).

q. ITU Voice Compression G.711, G.728, G.729, Idle Suppression, and Echo cancelling.

10.3.8 DISN Converged Access (DCA)

NI-007670 [**Required: DCA**] DCA Layer 2 Switching Specification Requirements:

a. ATM Pseudowire Transport.

b. Ethernet Pseudowire.

c. MPLS RSVP-TE Point-to-multipoint LSPs.

d. MPLS fast reroute (FRR).

e. VPLS signaled vai BGP and RSVP.

NI-007680 [**Required: DCA**] DCA shall satisfy the following Interface Interworking Requirements:

a. ATM To Ethernet Interworking.

b. HDLC to Ethernet Interworking.

c. PPP to Ethernet Interworking.

d. HDLC Interworking to VLAN Ethernet.

e. PDH/SDH/SONET to Ethernet Interworking.

NI-007690 [**Required: DCA**] DCA shall satisfy the following L2 Aggregation Requirements:

a. ATM VC Aggregation.

b. ATM VP Aggregation – PVP rewrite path only.

c. ATM VP/VC Aggregation – rewrite path and channelize.

d. Ethernet Aggregation (no customer tags).

e. Ethernet Aggregation [802.1Q Tag Stacking (push, pop, swap) and aggregate traffic onto a single interface with an additional VLAN tag (QinQ for P-to-P VPN mixed customer tags)].

NI-007700 [**Required: DCA**] DCA shall support PDH circuit Emulation (CEM), DS1, (Optionally DS3).

NI-007710 [**Required: DCA**] DCA shall the following CoS/QoS requirements:

a. Traffic prioritization with a minimum eight logical queues (two are low latency).

b. Traffic policing on ingress (all interfaces) and egress shaping use or ignore DSCP either ignore the customer 802.1p bits, or prioritize traffic based on the 802.1p bits.

NI-007720 [**Required: DCA**] DCA shall support DISN Core specific – channelized SONET (for MSAA coolated w/MSPP site).

10.4 TIMING AND SYNCHRONIZATION

10.4.1 Description

Figure 10.4-1, DISN Primary Site T&S, depicts the timing flow of a DISN primary site with T&S systems consisting of collocated BITS and MSPPs (NE) with equipment currently used in the DISN. This configuration is considered to be the "baseline" for DISN primary sites.

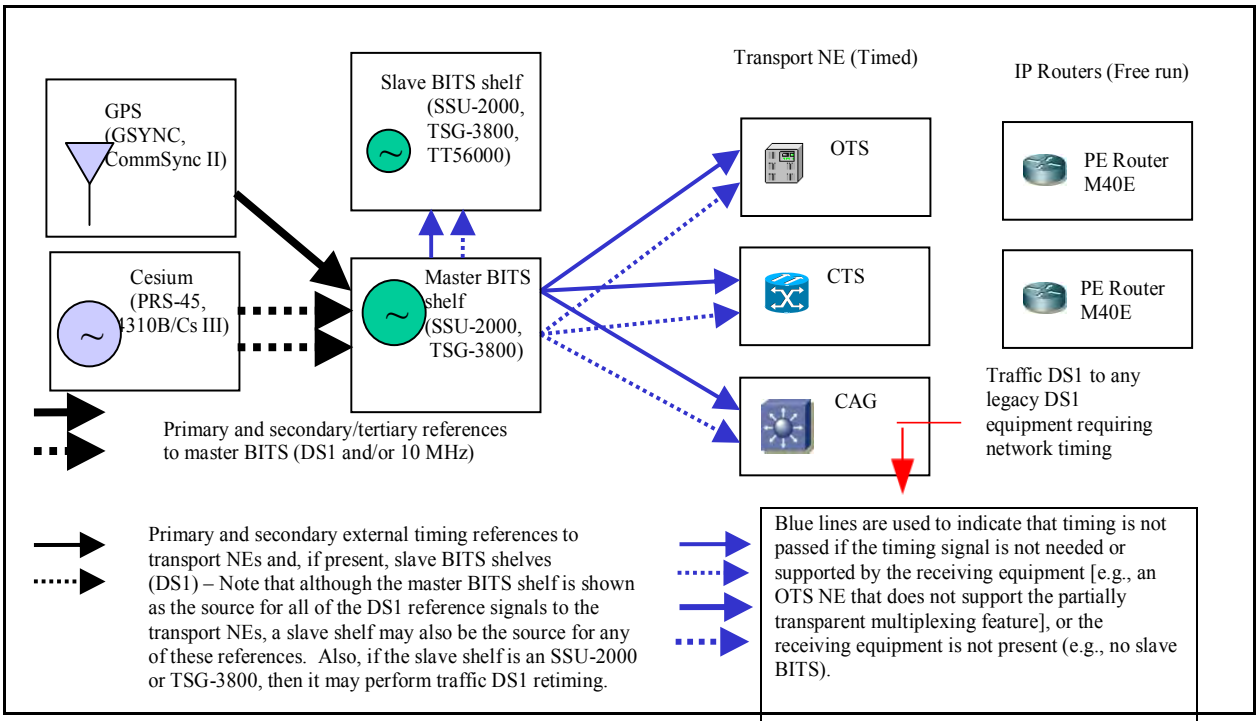


Figure 10.4-1. DISN Primary Site T&S

The BITS configuration includes a master BITS shelf and a slave BITS shelf. The BITS receives primary and secondary reference timing from a Cesium source or a Global Positioning System (GPS) source. The BITS provides redundant timing to the NEs of OTS, TSF, and CAG. The PE routers timing is free run. A secondary node does not use BITS, but instead derives timing via a line interface from a SONET CAG that is being timed from an upstream BITS. The following requirements apply to a primary site with BITS and suite of OTS, TSF, CAG, and routers.

10.4.2 Requirements

This section specifies the requirements (both Required and Optional) identified for the following:

- T&S system.
- BITS.
- General NI Requirements.
- OTS T&S Requirements.
- ODXC Timing Requirements.
- MSPP T&S Requirements.
- DISN Router T&S Requirements.

10.4.2.1 Timing and Synchronization System

The T&S system consists of the combination of the BITS and the UC NISP. This subsection specifies the requirements for the combined T&S system.

NI-007730 [**Required**] The T&S system shall conform to the Telcordia Technologies GR-1244-CORE and GR-253-CORE requirements for network timing and synchronization.

NI-007740 [**Required**] The T&S system shall conform to the Telcordia Technologies GR-1110 requirements for network T&S.

NI-007750 [**Required**] The T&S system shall provide for the external, line, loop, internal, and through timing modes as defined in Telcordia Technologies GR-253-CORE, Section 5.4.

NI-007760 [**Required**] For the T&S system neither manual nor autonomous protection switching of clock reference sources or clock units, including manual removal of the active clock unit, shall cause any error on any traffic signal.

NI-007770 [**Required**] The T&S system shall provide synchronization status messages (SSMs) and shall conform to the timing message generation, validation, and reaction characteristics in accordance with Telcordia Technologies GR-253-CORE, Section 5.4 to preclude and detect timing loops within the SONET network.

NI-007780 [**Required**] The T&S system shall be able to provide a selectable timing option, which will generate timing on DS1s across the DISN to users connected to other DISN Access elements.

NI-007790 [**Required**] The T&S system shall be capable of meeting or exceeding the wander and transient specifications defined in Telcordia Technologies GR-1244-CORE.

NI-007800 [**Required**] The T&S physical interface for the external timing references shall be DS1 or E1, terminated and transformer-coupled, and compliant with ANSI T1.101 or ITU-T Recommendation G.703 and G.704, respectively.

NI-007810 [**Optional**] If retiming of DS1 is required, the T&S system shall provide for equipment that retimes DS1 signals (e.g., external slip buffers, or NEs that support the bit-synchronous digital signal 12 (DS12) to VT1.5 payload mapping as a non-proprietary feature).

NI-007820 [**Desired**] The T&S system should provide for the capability for a Time of Day (TOD) timestamp accuracy of +/- 10 ms. (Such capability may be a reference GPS, a Network Time Protocol (NTP) server, and sufficient NTP clients.)

NI-007830 [**Desired**] The DS1 transmitters of the T&S system should provide for user-provisionable line buildout (LBO) in a convenient range, such as 0-133, 134-266, 267-399, 400-532, and 533-655.

10.4.2.2 Building Integrated Timing Supply

This section specifies the requirements for the BITS including the reference clock and timing distribution system.

NI-007840 [**Desired**] The BITS system shall consist of two sets of duplicated clock hardware (i.e., four-fold clock redundancy) that can independently provide system timing. Each set shall consist of two physically separate clock systems. The clock system shall be implemented so that any clock failure, including a loss of a single clock shelf, shall not result in any traffic outage.

NI-007850 [**Required**] The BITS shall be compliant with ITU-T Recommendation G.811.

NI-007860 [**Required**] The BITS shall be capable of providing a clock signal formatted as electrical D-1 75 or 120 ohms according to ANSI T1.101.

NI-007870 [**Required**] The BITS shall be capable of providing a clock signal formatted as electrical E1 75 or 120 ohms according to ITU-T Recommendation G.732.

10.4.2.3 General NI

This section specifies the general requirements for all network infrastructure products (NISPs) that support TDM interfaces.

NI-007880 [**Required**] The NISP shall be capable of slaving each interface to a specific timing source, such as BITS, internal Stratum 3E Clock, or the timing recovered from any selected port.

NI-007890 [**Required**] The NISP shall support errorless transitions between external timing and internal timing. An event is errorless if no SES is incurred by the event.

NI-007900 [**Required**] The NISPs shall provide appropriate alarms and proper responses when the frequencies of the incoming signals differ in magnitude from their nominal frequency by more than 20 parts ppm.

NI-007910 [**Required**] The NISP shall provide for the external timing mode as defined in Telcordia Technologies GR-253-CORE, Issue 3, September 2000, Section 5.4.

a. The NISP shall be capable of receiving a BITS clock signal formatted as an electrical T1, AMI formatted ESF with SSM.

b. The NISP shall be capable of receiving a BITS clock signal formatted as an electrical E1 75 or 120 ohms according to ITU-T Recommendation G.732.

c. The NISP shall be capable of receiving two (i.e., primary and secondary) external BITS sources. It shall be capable of switching between the primary and secondary source, and the switch shall not cause any errors to be imparted on data traffic.

d. The NISPs shall be capable of accepting two (i.e., primary and secondary) external timing sources from a BITS system that is traceable to a Stratum 1 primary reference source, as defined Telcordia Technologies in GR-436-CORE and GR-253-CORE, Sections 5.4, and ANSI T1.101-1999.

NI-007920 [**Required**] The NISP shall support the Line timing mode as defined in Telcordia Technologies GR-253-CORE, Section 5.4.

a. The NISP shall be capable of accepting its timing reference via a line interface from a SONET MSPP that is being timed from an upstream BITS as defined in Telcordia Technologies GR-253-CORE, Section 5.4.

b. The NISPs shall be capable of accepting its timing reference via a line interface from an SDH MSPP that is being timed from an upstream BITS.

NI-007930 [**Required**] The NISP shall support the loop timing mode as defined in Telcordia Technologies GR-253-CORE, Section 5.4.

NI-007940 [**Required**] The NISP shall support the internal timing mode as defined in Telcordia Technologies GR-253-CORE, Section 5.4.

a. The NISP internal clock shall conform to Telcordia Technologies GR-253-CORE standards for Stratum 3E and higher sources.

b. The NISP internal clock shall conform to Telcordia Technologies GR-253-CORE standards for SONET Minimum Clock (SMC) applications for Stratum 3 and higher

sources as per GR-253-CORE, Section 5.4, for free run accuracy, holdover, pull-in/hold in, wander, jitter, phase transients, input tolerance, and transition from self-timing to normal timing modes.

c. The NISPs shall provide an error-free transition (i.e., no payload errors) between external and internal timing.

NI-007950 [**Required**] The NISP shall support the Through timing mode as defined in Telcordia Technologies GR-253-CORE, Section 5.4.

NI-007960 [**Optional**] If the NISP terminates the SONET line layer (e.g., performs STS pointer processing) the system shall support derived DS1 features.

10.4.2.4 Optical Transport System

This section specifies the specific requirements for the following modes of operation of the OTS for line system functions that require timing:

- Regeneration: In this mode of operation, the OTS NEs are able to provide efficient transparent transport of various client signals for one wavelength to another. This configuration is considered to be the "baseline" for a DISN primary site.
- OTN/Proprietary Wrapping: In this mode of operation, the OTS adds additional overhead bits or bytes to individual client signals to support functions, such as FEC and protection switching at the optical layer, as part of the fully transparent multiplexing mode.
- Partially Transparent Multiplexing: In mode of operation the OTS NEs that support this multiplexing function typically use proprietary methods to transfer as much of the information contained in the section and line overheads of the incoming client signals as possible through to the outgoing client signals at the far end.

NI-007970 [**Optional**] If the OTS uses regeneration line system function, the T&S system shall provide for the following:

a. Through timing mode as defined in Telcordia Technologies TR-917 and GR-253-CORE, Issue 3, September 2000, Section 5.6.

b. Internal timing mode as defined in Telcordia Technologies TR-917.

NOTE: loop, line, and external timing are not applicable to the regeneration function.

NI-007980 [**Optional**] If the T&S system shall provide for the following:

a. Through timing mode as defined in ITU-T Recommendation G.8251.

b. Internal timing mode as defined in ITU-T Recommendation G.8251.

NI-007990 [**Optional**] The T&S system shall provide for the following:

a. External timing mode as defined in Telcordia Technologies GR-253-CORE, Section 5.4.

b. Line timing mode as defined in Telcordia Technologies GR-253-CORE, Section 5.4.

c. Internal ST3 timing mode as defined in Telcordia Technologies GR-253-CORE, Section 5.4.

d. 27.4 SONET SSM as defined in Telcordia Technologies GR-253-CORE, Section 5.4.

e. Derived DS1 as defined in Telcordia Technologies GR-253-CORE, Section 5.4.

10.4.2.5 ODXC Timing

This section specifies the specific requirements for the following modes of operation of the TSF functional device transport switching (TS) for Line System functions that require timing:

- SONET Line and Path Termination: In this mode of operation, the NE adjusts the STS pointers and terminates the SONET line layer (which, in turn, implies that the SONET section layer has been terminated. This mode of operation is considered the "baseline" for a DISN primary site.
- SONET Regeneration: In this mode of operation, the TSF device supports a Regeneration function in addition to its (normal) SONET Line Termination function.

NI-008000 [**Optional**] If the TSF device uses SONET line and path termination, the T&S system shall provide the following:

a. External timing mode as defined in Telcordia Technologies GR-253-CORE, Section 5.4.

b. Line timing mode as defined in Telcordia Technologies GR-253-CORE, Section 5.4.

c. Internal timing as defined in Telcordia Technologies GR-253-CORE, Section 5.4.

d. Derived DS1 as defined in Telcordia Technologies GR-253-CORE, Section 5.4.

e. SONET SSM as defined in Telcordia Technologies GR-253-CORE, Section 5.4.

NI-008010 [**Optional**] If the TSF device uses SONET regeneration, the T&S system shall provide for the following:

a. Through timing mode as defined in Telcordia Technologies GR-253-CORE, Section 5.6, and Telcordia Technologies TR-917.

b. Internal timing as defined in Telcordia Technologies TR-917.

10.4.2.6 MSPP Timing

This section specifies the specific requirements for the following mode of operation of the MSPP:

- SONET Line and Path Termination: This mode of operation is considered to be the "baseline" for a DISN primary site.

NI-008020 [**Optional**] If the MSPP functional device uses SONET line and path termination, the T&S system shall provide the following:

a. External timing mode as defined in Telcordia Technologies GR-253-CORE, Section 5.4.

b. Line timing mode as defined in Telcordia Technologies GR-253-CORE, Section 5.4.

c. Internal ST3 timing mode as defined in Telcordia Technologies GR-253-CORE, Section 5.4.

d. Derived DS1 as defined in Telcordia Technologies GR-253-CORE, Section 5.4.

NI-008030 [**Optional**] If a DS1 circuit requires retiming, the CAG functional device shall support DS1 retiming per channel and the retiming requirement shall comply with the synchronization-related criteria in ANSI T1.101, and the electrical interface criteria in ANSI T1.102 and Telcordia Technologies GR-499-CORE.

10.4.2.7 Router

This section specifies the specific requirements for the following modes of operations of the IP Routers:

- SONET Line and Path Termination: This mode of operation requires only internal timing. It is consider the "baseline" for a DISN primary site.
- DS1 Circuit Emulation Service (CES): For this mode of operation, the IP routers transport DS1 CES traffic.

NI-008040 [**Optional**] If the IP router uses SONET line and path termination mode of operation, T&S system shall provide for internal SMC timing mode as defined in Telcordia Technologies GR-253-CORE, Section 5.4.

NI-008050 [**Optional**] If the IP Router transport DS1 CES, the T&S system shall provide for the following:

a. External timing mode as defined in Telcordia Technologies GR-253-CORE, Section 5.4.

b. Line timing mode as defined in Telcordia Technologies GR-253-CORE, Section 5.4.

c. Internal SMC timing mode as defined in Telcordia Technologies GR-253-CORE, Section 5.4.

d. Derived DS1 as defined in Telcordia Technologies GR-253-CORE, Section 5.4.

10.4.2.8 T&S Standards Compliance

The standards in effect when the equipment was first acquired are listed. Updates to the standards since that point in time are identified in brackets. When the manufacturer provides new components for the COTS items to the same device that satisfy updated standards, DISA will often purchase and install those components to accommodate growth, but will not replace

existing components unless there is another reason to do so. As such, components will be operational within DISN that satisfy multiple versions of the standards. Testing will need to be undertaken using the standard release that applied to that component, where the revised standard cannot be satisfied by the original component.

NI-008060 [**Required**] ITU-T Recommendation G.703 (2001).

NI-008070 [**Required**] ITU-T Recommendation G.704 (1998).

NI-008080 [**Required**] ITU-T Recommendation G.732 (1988).

NI-008090 [**Required**] ITU-T Recommendation G.811 (1997).

NI-008100 [**Required**] ITU-T Recommendation G.8251 (2001).

NI-008110 [**Required**] ANSI T1.101.

NI-008120 [**Required**] Telcordia Technologies GR-253-CORE, Issue 3, September 2000 (Issue 4, December 2005).

NI-008130 [**Required**] Telcordia Technologies TR-917, December 1990.

NI-008140 [**Required**] Telcordia Technologies GR-1244-CORE, Issue 2, December 2000 (Issue 5, May 2005).

10.5 PLANNING TOOLS

To aid in the design and implementation of the network, planning tools are required that model and cost-out the features of the equipment. For optical network design and implementation, an optical layer planning tool shall be provided that can model the OTS system over all anticipated DISN scenarios. Likewise, a TSF/CAG network planning tool shall be available that models the TSF switching and/or CAG aggregation.

10.5.1 OTS Planning Tool

NI-008150 [**Required**] A COTS OTS planning tool shall be available.

NI-008160 [**Required**] The OTS software planning tool shall be able to run on a standard PC.

NI-008170 [**Required**] The OTS planning tool shall enable the user to enter all fiber and other user-settable parameters via Excel® spreadsheet input.

NI-008180 [**Required**] If the OTS planning tool offers a user friendly Graphical User Interface (GUI) with menu-driven commands, it shall also enable the network designer to enter all the parameters into a spreadsheet.

NI-008190 [Required] The OTS planning tool shall provide performance outputs on a per wavelength level for Q and OSNR.

NI-008200 [**Required**] The OTS planning tool shall enable variations in the following inputs for design purposes:

a. Total span loss.

b. Length per span.

c. Chromatic dispersion.

d. Chromatic dispersion slope.

e. PMD.

f. Fiber type.

g. Per channel optical power (transport-side).

h. Per channel bit rate.

i. Per channel protocol.

j. Per channel format.

k. Alien wavelength parameters:

(1) Minimum optical input power (client-side).

(2) Maximum optical input power (client-side).

(3) Minimum extinction ratio.

(4) Maximum extinction ratio.

(5) Minimum receiver power.

(6) Maximum receiver power.

NI-008210 [**Required**] The OTS planning tool shall enable the network engineer to input user-settable parameters to create additional default fiber types. This shall include, but not be limited to, settings for:

a. Fiber-type/vintage.

b. Optical attenuation.

c. Chromatic dispersion.

d. Chromatic dispersion slope.

e. PMD.

f. Effective area.

NI-008220 [**Required**] The OTS planning tool shall enable a single span to consist of up to three types of different fibers for a mixed-fiber implementation analysis.

NI-008230 [**Required**] The OTS planning tool shall provide the option to set all optical channels to the same user-settable default values in the same amount of steps as a single optical channel setting.

NI-008240 [**Required**] If dispersion compensation modules are an option with the OTS, then the OTS planning tool shall provide both options: (1) the tool optimizes the choice and placement of the dispersion compensation modules, and (2) the network engineer chooses and places the dispersion compensation modules.

NI-008250 [**Required**] The OTS planning tool shall be capable of simulating and verifying all OTS capabilities, including, but not limited to, all OLA, ROADM, and terminal options.

NI-008260 [**Required**] The OTS planning tool shall address risk reduction and deployment design cost effectiveness before procurement, deployment, and service turn-up.

NI-008270 [**Required**] The OTS planning tool shall characterize the vendor's equipment in the following categories:

a. All optical transport.

b. OEO functionality.

c. Alien wavelength transport capability.

NI-008280 [**Required**] The OTS planning tool shall have graphical views.

NI-008290 [**Required**] The OTS planning tool shall provide a topology view of the optical network.

NI-008300 [**Required**] If the OTS offers automatic optical protection switching, the OTS planning tool shall provide optical protection analysis.

NI-008310 [**Required**] The OTS planning tool shall provide mean time between failures (MTBF) and availability of the equipment.

NI-008320 [**Required**] The OTS planning tool shall provide amplifier and optical regeneration system placement analysis.

NI-008330 [**Required**] The OTS planning tool shall provide optimal cost solution analysis.

NI-008340 [**Required**] The OTS planning tool shall provide simulation through "what if" scenarios. This includes the ability to reset optical channel population distributions and other parameters one at a time and not needing to input an entire reload of data manually every time one parameter needs to be changed.

NI-008350 [**Required**] The OTS planning tool shall provide user-constraint settings for analysis.

NI-008360 [**Required**] The OTS planning tool shall provide automated failure (link and node) scenarios for analysis.

NI-008370 [**Required**] The OTS planning tool shall provide results through printable performance reports, and bill of materials on a per node and network basis with equipment breakdown.

NI-008380 [**Required**] The OTS planning tool shall include documentation that includes the following:

a. A functional overview on the operation of the tool.

b. The simulation engine used.

c. Instructions for the network designer to facilitate tool usage.

d. The acceptable performance levels (e.g., OSNR, Q) generated by the tool that are needed for 10^(-15) BER transmissions.

e. All limitations and capabilities/trade-off scenarios supported by the tool.

10.5.2 Network Layer Planning Tool

NI-008390 [**Required**] The network planning tool shall be able to run on a standard PC.

NI-008400 [**Required**] The network planning tool shall be capable of wavelength designations, if ITU grid optics is an option, to provide alien wavelength input to OTS planning tool.

NI-008410 [**Required**] The network planning tool shall be capable of digital switching and grooming simulation, analysis, and design.

NI-008420 [**Required**] The network planning tool shall enable the user to enter all digital signal demands and other user-settable parameters via an Excel spreadsheet input.

NI-008430 [**Required**] The network planning tool shall support emulation of the equipment link state and routing algorithms.

NI-008440 [**Required**] The network planning tool shall support user constraints supported by the equipment.

NI-008450 [**Required**] The network planning tool shall support protection and restoration features supported by the equipment.

NI-008460 [**Required**] The network planning tool shall support MTBF and availability calculations and analysis.

NI-008470 [**Required**] The network planning tool shall support optimal cost solution modeling.

NI-008480 [**Required**] The network planning tool shall support simulation through “what if” scenarios. The vendor shall list all trade-off scenarios that the network planning tool supports.

NI-008490 [**Required**] The network planning tool shall support printable node, link, and connection reports, including the generation of a bill of materials.

NI-008500 [**Required**] The network planning tool shall support automated failure (link and node) scenarios.

NI-008510 [**Required**] The network planning tool shall have graphical views for all "what if" scenarios.

NI-008520 [**Required**] If the network planning tool includes a user friendly GUI with menu-driven user interfaces, then it shall also enable the network designer to enter all the parameters into a spreadsheet.

NI-008530 [**Required**] The network planning tool shall support a topology view of the network.

NI-008540 [**Required**] The network planning tool shall support traffic engineering.

NI-008550 [**Required**] The network planning tool shall support traffic variation analysis.

10.6 DISN ROUTER

The DISN uses a variety of makes and models of routers. The integration of these routers into the DISN architecture is dependent on capabilities, such as backplane capacity and available interfaces. It is customary to assign names to such routers to depict their placement in the architecture. Examples would be P routers and PE routers. Typically, the higher backplane routers, which also support high bandwidth but low port density interfaces, are used in the core of the DISN. However, as technologies evolve, no specific make or model of router should be limited to a particular place in the architecture.

10.6.1 Interface

The interface requirements specified in the following paragraphs will be implemented on all DISN routers as appropriate for specific DISN infrastructure and customer requirements. All IPv6 implementations shall be capable of legacy support of IPv4.

10.6.1.1 Packet over SONET Interface

DISN Routers shall support:

NI-008560 [**Required**] The OC-3c/STM-1 Packet Over SONET (POS) interfaces.

NI-008570 [**Required**] The OC-3c/STM-1 POS interfaces shall be configurable to support either SONET or SDH framing.

NI-008580 [**Required**] The OC-3c/STM-1 POS interfaces shall conform to ANSI T1.105-2001.

NI-008590 [**Required**] The OC-3c/STM-1 POS interfaces shall conform to Telcordia Technologies GR-253-CORE, Issue 4, December 2005, Sections 3, 4, and 5.

NI-008600 [**Required**] The OC-3c/STM-1 POS interfaces shall conform to ITU-T Recommendation G.707 and ITU-T Recommendation G.957.

NI-008610 [**Required**] The OC-3c/STM-1 POS interfaces shall provide the standard SONET STS-1, STS-N, and STS-Nc frame structures defined in ANSI T1.105-2001.

NI-008620 [**Required**] The OC-3c/STM-1 POS interfaces shall provide the standard SDH AU-3, AU-4, and AU-4-Xc frame structures defined in ITU-T Recommendation G.707.

NI-008630 [**Required**] The definition, generation, and function of the OC-3c/STM-1 POS interface SONET overhead and pointer processing shall follow standards defined in ANSI T1.105 2001.

NI-008640 [**Required**] The definition, generation, and function of the OC-3c/STM-1 SDH interface SDH overhead and pointer processing shall follow standards defined in ITU-T Recommendation G.707.

NI-008650 [**Required**] The OC-3c/STM-1 POS interfaces shall ignore the value contained in unused bits/bytes.

NI-008660 [**Required**] The OC-3c/STM-1 POS interfaces shall support point-to-point frame relay encapsulation for link layer framing of packets as defined by RFC 2427.

NI-008670 [**Required**] The OC-3c/STM-1 POS interfaces shall support Point-to-Point Protocol (PPP) for link layer framing of packets as defined by RFCs 1662 and 2615.

NI-008680 [**Required**] The OC-3c/STM-1 POS interfaces shall support High-Level Data Link Control (HDLC) for link layer framing of packets.

NI-008690 [**Required**] The OC-3c/STM-1 POS interfaces shall allow separate Maximum Transmission Unit (MTU) sizes for unlabeled network layer packets and labeled MPLS packets.

NI-008700 [**Required**] The OC-3c/STM-1 POS interfaces shall support an MTU size of at least 4470 bytes.

NI-008710 [**Required**] The OC-3c/STM-1 POS interfaces shall support appropriate in-band routing and control protocols, such as Intermediate System to Intermediate System (IS-IS), Resource Reservation Protocol (RSVP), and Border Gateway Protocol (BGP).

NI-008720 [**Required**] The OC-3c/STM-1 POS interfaces shall support the transport of IPv6 packets.

NI-008730 [**Required**] The OC-3c/STM-1 POS interfaces shall clock transmitted data based on an internal source clock.

NI-008740 [**Required**] The OC-3c/STM-1 POS interfaces shall clock transmitted data based on an external source clock recovered from the received line.

NI-008750 [**Required**] OC-12c/STM-4 POS interfaces.

NI-008760 [**Required**] The OC-12c/STM-4 POS interfaces shall be configurable to support either SONET or SDH framing.

NI-008770 [**Required**] The OC-12c/STM-4 POS interfaces shall conform to ANSI T1.105-2001.

NI-008780 [**Required**] The OC-12c/STM-4 POS interfaces shall conform to Telcordia Technologies GR-253-CORE, Issue 4, December 2005, Sections 3, 4, and 5.

NI-008790 [**Required**] The OC-12c/STM-4 POS interfaces shall conform to ITU-T Recommendation G.707, and Recommendation G.957.

NI-008800 [**Required**] The OC-12c/STM-4 POS interfaces shall provide the standard SONET STS-1, STS-N, and STS-Nc frame structures defined in ANSI T1.105-2001.

NI-008810 [**Required**] The OC-12c/STM-4 POS interfaces shall provide the standard SDH AU-3, AU-4, and AU-4-Xc frame structures defined in ITU-T Recommendation G.707.

NI-008820 [**Required**] The definition, generation, and function of the OC-12c/STM-4 POS interface SONET overhead and pointer processing shall follow standards defined in ANSI T1.105-2001.

NI-008830 [**Required**] The definition, generation, and function of the OC-12c/STM-4 POS interface SDH overhead and pointer processing shall follow standards defined in ITU-T G.707.

NI-008840 [**Required**] The OC-12c/STM-4 POS interfaces shall ignore the value contained in unused bits/bytes.

NI-008850 [**Required**] The OC-12c/STM-4 POS interfaces shall support point-to-point frame relay encapsulation for link layer framing of packets as defined by RFC 2427.

NI-008860 [**Required**] The OC-12c/STM-4 POS interfaces shall support PPP for link layer framing of packets as defined by RFCs 1662 and 2615.

NI-008870 [**Required**] The OC-12c/STM-4 POS interfaces shall support HDLC for link layer framing of packets.

NI-008880 [**Required**] The OC-12c/STM-4 POS interfaces shall allow separate MTU sizes for unlabeled network layer packets and labeled MPLS packets.

NI-008890 [**Required**] The OC-12c/STM-4 POS interfaces shall support an MTU size of at least 4470 bytes.

NI-008900 [**Required**] The OC-12c/STM-4 POS interfaces shall support appropriate in-band routing and control protocols, such as IS-IS, RSVP, and internal BGP.

NI-008910 [**Required**] The OC-12c/STM-4 POS interfaces shall support the transport of IPv6 packets.

NI-008920 [**Required**] The OC-12c/STM-4 POS interfaces shall clock transmitted data based on an internal source clock.

NI-008930 [**Required**] The OC-12c/STM-4 POS interfaces shall clock transmitted data based on an external source clock recovered from the received line.

NI-008940 [**Required**] The OC-48c/ STM-16 POS interfaces.

NI-008950 [**Required**] The OC-48c/STM-16 POS interfaces shall be configurable to support either SONET or SDH framing.

NI-008960 [**Required**] The OC-48c/STM-16 POS interfaces shall conform to ANSI T1.105-2001.

NI-008970 [**Required**] The OC-48c/STM-16 POS interfaces shall conform to Telcordia Technologies GR-253-CORE Sections 3, 4, and 5.

NI-008980 [**Required**] The OC-48c/STM-16 POS interfaces shall conform to ITU-T Recommendations G.707 and G.957.

NI-008990 [**Required**] The OC-48c/STM-16 POS interfaces shall provide the standard SONET STS-1, STS-N, and STS-Nc frame structures defined in ANSI T1.105-2001.

NI-009000 [**Required**] The OC-48c/STM-16 POS interfaces shall provide the standard SDH AU-3, AU-4, and AU-4-Xc frame structures defined in ITU-T Recommendation G.707.

NI-009010 [**Required**] The definition, generation, and function of the OC-48c/STM-16 POS interface SONET overhead and pointer processing shall follow standards defined in ANSI T1.105-2001.

NI-009020 [**Required**] The definition, generation, and function of the OC-48c/STM-16 POS interface SDH overhead and pointer processing shall follow standards defined in ITU-T Recommendation G.707.

NI-009030 [**Required**] The OC-48c/STM-16 POS interfaces shall ignore the value contained in unused bits/bytes.

NI-009040 [**Required**] The OC-48c/STM-16 POS interfaces shall support point-to-point frame relay encapsulation for link layer framing of packets as defined by RFC 2427.

NI-009050 [**Required**] The OC-48c/STM-16 POS interfaces shall support PPP for link layer framing of packets as defined by RFCs 1662 and 2615.

NI-009060 [**Required**] The OC-48c/STM-16 POS interfaces shall support HDLC for link layer framing of packets.

NI-009070 [**Required**] The OC-48c/STM-16 POS interfaces shall allow separate MTU sizes for unlabeled network layer packets and labeled MPLS packets.

NI-009080 [**Required**] The OC-48c/STM-16 POS interfaces shall support an MTU size of at least 4470 bytes.

NI-009090 [**Required**] The OC-48c/STM-16 POS interfaces shall support appropriate in-band routing and control protocols, such as IS-IS, RSVP, and BGP.

NI-009100 [**Required**] The OC-48c/STM-16 POS interfaces shall support the transport of IPv6 packets.

NI-009110 [**Required**] The OC-48c/STM-16 POS interfaces shall clock transmitted data based on an internal source clock.

NI-009120 [**Required**] The OC-48c/STM-16 POS interfaces shall clock transmitted data based on an external source clock recovered from the received line.

NI-009130 [**Required**] OC-192c/STM-64 POS interfaces.

NI-009140 [**Required**] The OC-192c/STM-64 POS interfaces shall be configurable to support either SONET or SDH framing.

NI-009150 [**Required**] The OC-192c/STM-64 POS interfaces shall conform to ANSI T1.105-2001.

NI-009160 [**Required**] The OC-192c/STM-64 POS interfaces shall conform to Telcordia Technologies GR-253-CORE, Issue 4, December 2005, Sections 3, 4, and 5.

NI-009170 [**Required**] The OC-192c/STM-64 interfaces shall conform to ITU-T Recommendation G.691.

NI-009180 [**Required**] The OC-192c/STM-64 POS interfaces shall provide the standard SONET STS-1, STS-N, and STS-Nc frame structures defined in ANSI T1.105-2001.

NI-009190 [**Required**] The OC-192c/STM-64 POS interfaces shall provide the standard SDH AU-3, AU-4, and AU-4-Xc frame structures defined in ITU-T Recommendation G.707.

NI-009200 [**Required**] The definition, generation, and function of the OC-192c/STM-64 POS interface SONET overhead and pointer processing shall follow standards defined in ANSI T1.105-2001.

NI-009210 [**Required**] The definition, generation, and function of the OC-192c/STM-64 POS interface SDH overhead and pointer processing shall follow standards defined in ITU-T Recommendation G.707.

NI-009220 [**Required**] The OC-192c/STM-64 POS interfaces shall ignore the value contained in unused bits/bytes.

NI-009230 [**Required**] The OC-192c/STM-64 POS interfaces shall support point-to-point frame relay encapsulation for link layer framing of packets as defined by RFC 2427.

NI-009240 [**Required**] The OC-192c/STM-64 POS interfaces shall support PPP for link layer framing of packets as defined by RFCs 1662 and 2615.

NI-009250 [**Required**] The OC-192c/STM-64 POS interfaces shall support HDLC for link layer framing of packets.

NI-009260 [**Required**] The OC-192c/STM-64 POS interfaces shall allow separate MTU sizes for unlabeled network layer packets and labeled MPLS packets.

NI-009270 [**Required**] The OC-192c/STM-64 POS interfaces shall support an MTU size of at least 4470 bytes.

NI-009280 [**Required**] The OC-192c/STM-64 POS interfaces shall support appropriate in-band routing and control protocols, such as IS-IS, RSVP, and BGP.

NI-009290 [**Required**] The OC-192c/STM-64 POS interfaces shall support the transport of IPv6 packets.

NI-009300 [**Required**] The OC-192c/STM-64 POS interfaces shall support VSR optics as defined by the Optical Internetworking Forum (OIF).

NI-009310 [**Required**] The OC-192c/STM-64 POS interfaces shall clock transmitted data based on an internal source clock.

NI-009320 [**Required**] The OC-192c/STM-64 POS interfaces shall clock transmitted data based on an external source clock recovered from the received line.

NI-009330 [**Optional**] The NE shall support OC-768c/STM-256 POS interfaces.

10.6.1.2 ATM Interface

DISN Routers may optionally support ATM interfaces. For certification, the ATM interfaces must meet the following requirements:

NI-009340 [**Required**] The router shall support OC-12c/STM-4 ATM interfaces.

NI-009350 [**Required**] The OC-12c/STM-4 ATM interfaces shall be configurable to support either SONET or SDH framing.

NI-009360 [**Required**] The OC-12c/STM-4 ATM interfaces shall conform to ANSI T1.105-2001.

NI-009370 [**Required**] The OC-12c/STM-4 ATM interfaces shall conform to Telcordia Technologies GR-253-CORE, issue 4, December 2005, Sections 3, 4, and 5.

NI-009380 [**Required**] The OC-12c/STM-4 ATM interfaces shall conform to ITU-T Recommendations G.707 and G.957.

NI-009390 [**Required**] The OC-12c/STM-4 ATM interfaces shall provide the standard SONET STS-1, STS-N, and STS-Nc frame structures defined in ANSI T1.105-2001.

NI-009400 [**Required**] The OC-12c/STM-4 ATM interfaces shall provide the standard SDH AU-3, AU-4, and AU-4-Xc frame structures defined in ITU-T Recommendation G.707.

NI-009410 [**Required**] The definition, generation, and function of the OC-12c/STM-4 ATM interface SONET overhead and pointer processing shall follow standards defined in ANSI T1.105 2001.

NI-009420 [**Required**] The definition, generation, and function of the OC-12c/STM-4 ATM interface SDH overhead and pointer processing shall follow standards defined in ITU-T Recommendation G.707.

NI-009430 [**Required**] The OC-12c/STM-4 ATM interfaces shall ignore the value contained in unused bits/bytes.

NI-009440 [**Required**] The OC-12c/STM-4 ATM interfaces shall provide segmentation and reassembly (SAR) of IP packets for transport over ATM Adaptation Layer 5 (AAL5) as defined by RFC 2684.

NI-009450 [**Required**] The OC-12c/STM-4 ATM interfaces shall support the ATM Forum UNI.

NI-009460 [**Required**] The OC-12c/STM-4 ATM interfaces shall support the ATM Forum UNI 4.1.

NI-009470 [**Required**] The OC-12c/STM-4 ATM interfaces shall support the ATM Forum Integrated Local Management Interface (ILMI).

NI-009480 [**Required**] The OC-12c/STM-4 ATM interfaces shall support F5 O&AM.

NI-009490 [**Required**] The OC-12c/STM-4 ATM interfaces shall allow separate MTU sizes for unlabeled network layer packets and labeled MPLS packets.

NI-009500 [**Required**] The OC-12c/STM-4 ATM interfaces shall support appropriate in-band routing and control protocols, such as IS-IS, RSVP, and BGP.

NI-009510 [**Required**] The OC-12c/STM-4 ATM interfaces shall support the transport of IPv6 packets.

NI-009520 [**Required**] The OC-12c/STM-4 ATM interfaces shall clock transmitted data based on an internal source clock.

NI-009530 [**Required**] The OC-12c/STM-4 ATM interfaces shall clock transmitted data based on an external source clock recovered from the received line.

NI-009540 [**Required**] The NE shall support OC-48c/STM-16 ATM interfaces.

NI-009550 [**Required**] The OC-48c/STM-16 ATM interfaces shall be configurable to support either SONET or SDH framing.

NI-009560 [**Required**] The OC-48c/STM-16 ATM interfaces shall conform to ANSI T1.105-2001.

NI-009570 [**Required**] The OC-48c/STM-16 ATM interfaces shall conform to Telcordia Technologies GR-253-CORE, Issue 4, December 2005, Sections 3, 4, and 5.

NI-009580 [**Required**] The OC-48c/STM-16 ATM interfaces shall conform to ITU-T Recommendations G.707 and G.957.

NI-009590 [**Required**] The OC-48c/STM-16 ATM interfaces shall provide the standard SONET STS-1, STS-N, and STS-Nc frame structures defined in ANSI T1.105-2001.

NI-009600 [**Required**] The OC-48c/STM-16 ATM interfaces shall provide the standard SDH AU-3, AU-4, and AU-4-Xc frame structures defined in ITU-T Recommendation G.707.

NI-009610 [**Required**] The definition, generation, and function of the OC-48c/STM-16 ATM interface SONET overhead and pointer processing shall follow standards defined in ANSI T1.105-2001.

NI-009620 [**Required**] The definition, generation, and function of the OC-48c/STM-16 ATM interface SDH overhead and pointer processing shall follow standards defined in ITU-T Recommendation G.707.

NI-009630 [**Required**] The OC-48c/STM-16 ATM interfaces shall ignore the value contained in unused bits/bytes.

NI-009640 [**Required**] The OC-48c/STM-16 ATM interfaces shall provide SAR of IP packets for transport over AAL5 as defined by RFC 2684.

NI-009650 [**Required**] The OC-48c/STM-16 ATM interfaces shall support the ATM Forum UNI.

NI-009660 [**Required**] The OC-48c/STM-16 ATM interfaces shall support the ATM Forum UNI 4.1.

NI-009670 [**Required**] The OC-48c/STM-16 ATM interfaces shall support the ATM Forum ILMI.

NI-009680 [**Required**] The OC-48c/STM-16 ATM interfaces shall support F5 O&AM.

NI-009690 [**Required**] The OC-48c/STM-16 ATM interfaces shall allow separate MTU sizes for unlabeled network layer packets and labeled MPLS packets.

NI-009700 [**Required**] The OC-48c/STM-16 ATM interfaces shall support appropriate in-band routing and control protocols, such as IS-IS, RSVP, and BGP.

NI-009710 [**Required**] The OC-48c/STM-16 ATM interfaces shall support the transport of IPv6 packets.

NI-009720 [**Required**] The OC-48c/STM-16 ATM interfaces shall clock transmitted data based on an internal source clock.

NI-009730 [**Required**] The OC-48c/STM-16 ATM interfaces shall clock transmitted data based on an external source clock recovered from the received line.

NI-009740 [**Required**] OC-192c/STM-64 ATM interfaces.

NI-009750 [**Required**] The OC-192c/STM-64 ATM interfaces shall be configurable to support either SONET or SDH framing.

NI-009760 [**Required**] The OC-192c/STM-64 ATM interfaces shall conform to ANSI T1.105-2001.

NI-009770 [**Required**] The OC-192c/STM-64 ATM interfaces shall conform to Telcordia Technologies GR-253-CORE, Issue 4, December 2005, Sections 3, 4, and 5.

NI-009780 [**Required**] The OC-192c/STM-64 ATM interfaces shall conform to ITU-T Recommendation G.691.

NI-009790 [**Required**] The OC-192c/STM-64 ATM interfaces shall provide the standard SONET STS-1, STS-N, and STS-Nc frame structures defined in ANSI T1.105-2001.

NI-009800 [**Required**] The OC-192c/STM-64 ATM interfaces shall provide the standard SDH AU-3, AU-4, and AU-4-Xc frame structures defined in ITU-T Recommendation G.707.

NI-009810 [**Required**] The definition, generation, and function of the OC-192c/STM-64 ATM interface SONET overhead and pointer processing shall follow standards defined in ANSI T1.105-2001.

NI-009820 [**Required**] The definition, generation, and function of the OC-192c/STM-64 ATM interface SDH overhead and pointer processing shall follow standards defined in ITU-T Recommendation G.707.

NI-009830 [**Required**] The OC-192c/STM-64 ATM interfaces shall ignore the value contained in unused bits/bytes.

NI-009840 [**Required**] The OC-192c/STM-64 ATM interfaces shall provide SAR of IP packets for transport over AAL5 defined by RFC 2684.

NI-009850 [**Required**] The OC-192c/STM-64 ATM interfaces shall support the ATM Forum UNI.

NI-009860 [**Required**] The OC-192c/STM-64 ATM interfaces shall support the ATM Forum UNI 4.1.

NI-009870 [**Required**] The OC-192c/STM-64 ATM interfaces shall support the ATM Forum ILMI.

NI-009880 [**Required**] The OC-192c/STM-64 ATM interfaces shall support F5 O&AM.

NI-009890 [**Required**] The OC-192c/STM-64 ATM interfaces shall allow separate MTU sizes for unlabeled network layer packets and labeled MPLS packets.

NI-009900 [**Required**] The OC-192c/STM-64 ATM interfaces shall support appropriate in-band routing and control protocols, such as IS-IS, RSVP, and BGP.

NI-009910 [**Required**] The OC-192c/STM-64 ATM interfaces shall support the transport of IPv6 packets.

NI-009920 [**Required**] The OC-192c/STM-64 ATM interfaces shall support VSR optics as defined by the OIF.

NI-009930 [**Required**] The OC-192c/STM-64 ATM interfaces shall clock transmitted data based on internal source clock.

NI-009940 [**Required**] The OC-192c/STM-64 ATM interfaces shall clock transmitted data based on external source clock recovered from the received line.

10.6.1.3 Ethernet Interface

The DISN Router shall support:

NI-009950 [**Required**] GbE interfaces.

NI-009960 [**Required**] GbE interfaces shall comply with IEEE 802.3-2002.

NI-009970 [**Required**] GbE interfaces shall allow separate MTU sizes for unlabeled network layer packets and labeled MPLS packets.

NI-009980 [**Required**] GbE interfaces shall support an MTU size of at least 4470 bytes.

NI-009990 [**Required**] GbE interfaces shall support modular, interchangeable optics for SR applications over standard MMF optic cable and extended reach applications over standard single-mode fiber optic cable.

NI-010000 [**Required**] GbE interfaces shall support appropriate in-band routing and control protocols, such as IS-IS, RSVP, and BGP.

NI-010010 [**Required**] 10GbE interfaces.

NI-010020 [**Required**] The 10GbE interfaces shall comply with IEEE 802.3ae-2002.

NI-010030 [**Required**] The 10GbE interfaces shall support VLAN and priority tagging, as defined by IEEE 802.1Q-1998.

NI-010040 [**Required**] The 10GbE interfaces shall allow separate MTU sizes for unlabeled network layer packets and labeled MPLS packets.

NI-010050 [**Required**] The 10GbE interfaces shall support an MTU size of at least 4470 bytes.

NI-010060 [**Required**] The 10GbE interfaces shall support appropriate in-band routing and control protocols. These will include IS-IS, RSVP, Protocol Independent Multicast (PIM), Open Shortest Path Fiber (OSPF), Multi-Protocol Border Gateway Protocol (MPBGP) and Border Gateway Protocol 4 (BGP4).

NI-010070 [**Required**] The 10GbE interfaces shall support the transport of IPv6 packets.

10.6.1.4 Packet Ring

The DISN Router may optionally support 802.17 RPR. To be certified, the Router must support the following packet ring requirements:

NI-010080 [**Required**] IEEE 802.17 RPR Working Group.

NI-010090 [**Required**] OC-12c/STM-4 packet ring interfaces.

NI-010100 [**Required**] OC-48c/STM-16 packet ring interfaces.

NI-010110 [**Required**] OC-192c/STM-64 packet ring interfaces.

10.6.2 IPv6

The IPv6 requirements for routers can be found in Section 5, IPv6.

10.6.3 Performance

DISN Routers shall support the following:

NI-010120 [**Required**] The switch fabric shall be non-blocking while operating at maximum full-duplex rate and bandwidth in a fully loaded chassis.

NI-010130 [**Required**] Interfaces shall forward at maximum rate for all packet sizes, including 40-byte IPv4 packets, while offering simultaneous services to include Access Control List (ACL) filtering, policy routing, and packet marking.

NI-010140 [**Required**] Neither internal nor external control plane signaling shall be interrupted by fully loaded data forwarding.

NI-010150 [**Required**] Packet loss within the DISN Router, for reasons other than congestion, lack of route, or external corruption, shall be less than 0.1 percent under full load.

NI-010160 [**Required**] 10,000 multicast groups with a minimum of 150,000 forwarding cache entries.

NI-010170 [**Required**] QoS-aware multicast over Differentiated Services (DiffServ) IAW RFC 3754. The router may optionally support the Internet Engineering Task Force (IETF) draft-bianchi-qos-multicast-over-diffserv.

NI-010180 [**Optional**] 40 Gbps interfaces without chassis replacement, including POS, Ethernet, and ITU-T Recommendation G.709.

10.6.3.1 IS-IS

The DISN Router shall support IS-IS IAW the following requirements:

NI-010190 [**Required**] The router shall implement the Integrated Intermediate System to Intermediate System (IS-IS) Routing Protocol as specified in RFCs 1195, 5302, 5304, and 5405.

NI-010200 [**Required**] The router shall be able to authenticate IS-IS routing updates using the HMAC-MD5 algorithm, as specified in RFC 5304.

NI-010210 [**Required**] The router shall support the IS-IS extensions for traffic engineering as specified in RFC 5305.

NI-010220 [**Required**] The router shall support the extended Intermediate System (IS) reachability Type-Length-Value (TLV) 22 with sub-TLV18: default metric traffic engineering, as specified in RFC 5305.

NI-010230 [**Required**] The router shall support the extended IP reachability TLV 135 with the up/down bit as specified in RFC 5305.

NI-010240 [**Required**] The router shall support the Traffic Engineering NE ID TLV 134 as specified in RFC 5305.

NI-010250 [**Required**] The router shall support the IS-IS extended IS reachability TLV 22 with sub-TLV 3: administrative group as defined in RFC 5305.

NI-010260 [**Required**] The router shall support the IS-IS Extended IS reachability TLV 22 with sub-TLV 6: IPv4 Interface Address as specified in RFC 5305.

NI-010270 [**Required**] The router shall support the IS-IS extended IS reachability TLV 22 with sub-TLV 8: IPv4 neighbor address as specified in RFC 5305.

NI-010280 [**Required**] The router shall support the IS-IS extended IS reachability TLV 22 with sub-TLV 9: IPv4 Maximum Link Bandwidth as specified in RFC 5305.

NI-010290 [**Required**] The router shall support the IS-IS Extended IS reachability TLV 22 with sub-TLV 10: Reservable Link Bandwidth as specified in RFC 5305.

NI-010300 [**Required**] The router shall support the IS-IS extended IS reachability TLV 22 with sub-TLV, 11: Unreserved Bandwidth (eight values for priorities 0 through 7) as specified in RFC 5305.

NI-010310 [**Required**] The router shall be compatible with known IS-IS TLV code points as defined in RFC 3359 (i.e. the NE should only use the code points specified in the RFC for the purpose specified in RFC 3359).

NI-010320 [**Required**] The router shall be able to restart the IS-IS routing process and initiate database synchronization without cycling adjacencies through a down state, as described in RFC 5306.

NI-010330 [**Required**] The router shall be able to treat an Ethernet interface that is directly connected to a neighboring NE as a point-to-point circuit with regard to IS-IS routing as specified in RFC 5309.

NI-010340 [**Required**] The router shall be able to reduce the flooding of redundant Link State Protocol Data Unit (LSPs) in IS-IS topologies as specified in RFC 2973.

NI-010350 [**Required**] The router shall be able to dynamically exchange IS-IS hostnames as specified in RFC 5301.

NI-010360 [**Required**] The router shall be able to eliminate IS-IS reliance on reliable protocols at the link layer for point-to-point links as specified in RFC 5303.

NI-010370 [**Required**] The router shall be able to support two new TLVs, a reachability TLV, and an interface address TLV, to distribute the necessary IPv6 information throughout a routing domain, as specified in RFC 5308.

NI-010380 [**Required**] The router shall be able to support three new TLVs and two new sub-TLVs of the extended IS reachability TLV, that allow a constrained shortest path first (CSPF) algorithm to calculate traffic-engineered routes using IPv6 addresses, as specified in RFC 6119.

NI-010390 [**Required**] The router shall recognize IS-IS TLVs defined for Generalized MPLS (GMPLS) traffic-engineering links as specified in the RFC 5307.

NI-010400 [**Required**] The router shall act as an IS-IS Level 1 NE.

NI-010410 [**Required**] The router shall act as an IS-IS Level 2 NE.

NI-010420 [**Required**] The router shall act as an IS-IS Level 1/Level 2 NE.

NI-010430 [**Required**] The router shall be able to perform incremental shortest path first (SPF) calculations, rather than a full calculation, after minor changes in the network topology.

NI-010440 [**Required**] The router shall begin to forward packets on the new route within 50 ms of receiving an LSP that causes the NE to change the SPF route.

NI-010450 [**Required**] The router shall be able to apply filter/access lists to the control plane including route policy to control IS-IS route leaking.

NI-010460 [**Required**] The router shall be able to maintain a minimum of 1,000 prefixes in the IS-IS database.

NI-010470 [**Optional**] The router shall be able to maintain a minimum of 10,000 prefixes in the IS-IS database.

NI-010480 [**Required**] The router shall support a minimum of 10 IS-IS neighbors (adjacencies).

NI-010490 [**Optional**] The router shall support a minimum of 50 IS-IS neighbors (adjacencies).

NI-010500 [**Optional**] The router shall support traffic load distribution over at least four equal-cost nearest-neighbor links between NE while maintaining per-flow packet sequence order.

NI-010510 [**Optional**] The router shall support multiple independent instances of IS-IS to offer alternate topologies for different services.

10.6.4 OSPF

The DISN Router shall support OSPF IAW the following requirements:

NI-010520 [**Required**] The router shall support the OSPF Link State Protocol as defined by RFC 2328.

NI-010530 [**Required**] The router shall support OSPF for IPv6 as defined in RFC 5340.

10.6.5 BGP

The DISN Router shall support BGP IAW the following requirements:

NI-010540 [**Required**] The router shall support the BGP4, as specified in RFCs 4271 and 1772 for the exchange of network reachability information with external networks External BGP (eBGP) and the distribution of external network reachability with internal neighbors Internal BGP (iBGP).

NI-010550 [**Required**] The router shall support the MP-BGP Sub-Address Family Identifier (SAFI) for multicast addresses as specified in RFC 4760.

NI-010560 [**Required**] The router shall support MP-BGP SAFI for global unicast IPv6 addresses as specified in RFC 4760.

NI-010570 [**Required**] The router shall support MP-BGP SAFI for MPLS Layer 3 VPN-IPv4 as specified in RFCs 4364 and RFC 4760.

NI-010580 [**Required**] The implementation of the BGP-4/MP-BGP protocol on the Provider router shall interoperate with the implementation of the BGP-4/MP-BGP protocol on the PE router.

NI-010590 [**Required**] The router shall be able to authenticate BGP routing information using an MD5 signature as specified in RFC ~~5925~~2385.

NI-010600 [**Required**] The router shall be able to reduce routing oscillations by dampening updates associated with unstable routes as specified in RFC 2439.

NI-010610 [**Required**] Enhancements to the BGP-4 protocol to mitigate against the persistent BGP route oscillations introduced in particular configurations that use route reflection or confederation in conjunction with the MULTI_EXIT_DISC attribute as documented in RFC 3345.

NI-010620 [**Required**] The router shall be able to tag routes on ingress and egress for common group identification and administration using the Communities attribute as specified in RFC 1997.

NI-010630 [**Required**] The router shall support the Extended Community attribute that extends the range of the Community attribute and adds a Type field for structure of the community space as specified in the RFC 4360.

NI-010640 [**Required**] The router shall be able to distribute an MPLS label with a route in the same update message as specified in RFC 3107.

NI-010650 [**Required**] The router shall be able to act as a BGP route reflector as specified in RFC 4456.

NI-010660 [**Required**] The router shall be able to act as an MP-BGP route reflector.

NI-010670 [**Required**] The router shall be able to participate as a BGP router within a confederation of autonomous systems that is represented as a single autonomous system to BGP peers external to the confederation as specified in RFC 5065.

NI-010680 [**Required**] The router shall be able to negotiate capabilities with a BGP neighbor by sending and receiving the optional Capabilities parameter as specified in RFC 5492.

NI-010690 [**Required**] The router shall be able to request and respond to requests for re-advertisement of the BGP neighbor outbound routing information base (Adj-RIB-Out) as specified in RFC 2918.

NI-010700 [**Required**] The router shall be able to restart the BGP routing process and initiate database synchronization with neighbors while preserving a forwarding state as specified in RFC 4724.

NI-010710 [**Required**] The router shall be able to apply policy to affect route acceptance and forwarding based on prefix.

NI-010720 [**Required**] The router shall be able to apply policy to affect route acceptance and forwarding based on a community string.

NI-010730 [**Required**] The router shall be able to apply policy to affect route acceptance and forwarding based on address family.

NI-010740 [**Required**] The router shall be able to apply policy to affect route acceptance and forwarding based on an Autonomous System (AS) path.

NI-010750 [**Required**] The router shall be able to apply policy to affect route acceptance and forwarding based on a BGP next-hop.

NI-010760 [**Required**] The router shall be able to apply policy to affect route acceptance and forwarding based on multi-exit discriminator.

NI-010770 [**Required**] The router shall be able to apply policy to affect route acceptance and forwarding based on a local preference.

NI-010780 [**Required**] The router shall be able to perform eBGP multihop to allow two non-directly connected peers to exchange eBGP.

NI-010790 [**Required**] The router shall support the BGP Time To Live (TTL) security hack as specified in IETF draft-gill-btsh-02.

NI-010800 [**Required**] The router shall be able to logically group neighbors with similar policy attributes to avoid Routing Information Base (RIB) duplication.

NI-010810 [**Required**] The router shall support multiple configurable NE IDs Router ID (RID) and corresponding routable source address, (e.g., multiple loopback interfaces each with a unique address or single loopback with multiple addresses, to separate and uniquely identify each unicast, multicast, and VPN address family supported.

NI-010820 [**Required**] The router shall stabilize its BGP routing table without requiring intervention or assistance after a full system or routing restart.

NI-010830 [**Required**] The router shall support a minimum of 200,000 best path BGP entries that are unique from each other in a prefix or subnet.

NI-010840 [**Optional**] The router shall support a minimum of 400,000 best path BGP entries that are unique from each other in prefix or subnet in addition to 600,000 routes that provide alternate paths to those prefixes or subnets.

NI-010850 [**Required**] The router shall support 100 distinct internal neighbors that are not logically grouped to optimize memory or update processing.

NI-010860 [**Optional**] The router shall support 200 distinct internal neighbors that are not logically grouped to optimize memory or update processing.

NI-010870 [**Required**] The router shall support 100 distinct external neighbors that are not logically grouped to optimize memory or update processing.

NI-010880 [**Optional**] The router shall support 200 distinct external neighbors that are not logically grouped to optimize memory or update processing.

10.6.6 MPLS

The DISN Router shall support MPLS IAW the following requirements:

NI-010890 [**Required**] The router shall act as an MPLS Label Switching Router (LSR) by forwarding inbound labeled packets based on the contents of the packet MPLS header and performing label swapping (inbound packet label pop and outbound packet label push) as defined in RFC 3031.

NI-010900 [**Required**] The router shall act as an MPLS Label Edge Router (LER) by pushing a label onto packets when at the Label Switched Path (LSP) ingress and popping a label off packets when at the LSP egress.

NI-010910 [**Required**] The router shall possess encoding capabilities to produce a valid MPLS-labeled packet from a given label stack and a network layer packet as defined by RFC 3032, Section 2.1.

NI-010920 [**Optional**] The router shall support label stacks consisting of at least three labels.

NI-010930 [**Optional**] The router shall support load sharing between multiple LSPs with the same ingress and egress LERs.

10.6.7 RSVP

The DISN Router shall support RSVP as follows:

NI-010940 [**Required**] The router shall use extensions to RSVP to establish MPLS LSP and enable constraint-based routing traffic engineering as defined by RFC 3209.

NI-010950 [**Required**] The router shall authenticate the integrity of RSVP requests for MPLS LSPs as defined by RFC 2747 and updated by RFC 3097.

NI-010960 [**Required**] The router shall support the Summary Refresh Message to reduce the processing overhead requirements of RSVP refresh messages as defined by RFC 2961.

NI-010970 [**Required**] The router shall support the Bundle Message to reduce the processing overhead requirements of RSVP refresh messages as defined by RFC 2961.

NI-010980 [**Required**] The router shall be able to dynamically signal and enforce different bandwidth constraints for different classes of traffic that are transported over separately routed constraint-based LSPs as defined by RFC 4124.

NI-010990 [**Required**] The router shall support Forwarding Adjacencies (FAs) and hierarchal or nested label switched paths as described in RFC 4206.

NI-011000 [**Required**] The router shall support extensions to RSVP for Generalized MPLS (GMPLS) as specified in RFC 4201.

NI-011010 [**Required**] The router shall support protocols for requesting and accepting resources from other physical and link layer NEs and signaling GMPLS traffic-engineered links between nodes as defined by RFC 4204 and OIF UNI 1.0.

NI-011020 [**Required**] The router shall support the bundling of multiple component links into a single logical traffic-engineered bundled link as specified in RFC 4201.

NI-011030 [**Required**] The router shall be able to repair an RSVP-Traffic Engineering (RSVP-TE) LSP locally, within 50 ms of downstream link or node failure by rerouting the LSP traffic around the failure using both the one-to-one backup and the facility backup methods as specified in RFCs 4090 and 5462.

NI-011040 [**Required**] The router acting as an ingress MPLS label edge NE shall reroute data traffic to a secondary presignaled LSP in less than 20 ms upon indication of the primary LSP failure.

NI-011050 [**Required**] The router shall support 10,000 bidirectional traffic-engineered LSPs acting as an intermediate LSR.

NI-011060 [**Required**] The router shall be able to originate 500 traffic-engineered LSPs and terminate the same number.

10.6.8 LDP

The DISN Router shall support LDP as follows:

NI-011070 [**Required**] The router shall support the Label Distribution Protocol (LDP) for MPLS downstream-unsolicited label distribution as defined by RFC 5036.

10.6.9 DiffServ

The DISN Router shall support DiffServ as follows:

NI-011080 [**Required**] The router shall support DiffServ in accordance with RFCs 2474 and 3140 as updated by 3168, 3260.

NI-011090 [**Required**] The router shall support the DiffServ Expedited Forwarding (EF) Per-Hop Behavior (PHB) and code point assignment as defined by RFC 3246.

NI-011100 [**Required**] The router shall support the DiffServ Assured Forwarding (AF) PHB classes and code point assignments as defined by RFC 2597 as updated by 3260.

NI-011110 [**Required**] The router shall support DiffServ over MPLS by mapping the Differentiated Services Code Point (DSCP) of packets received into MPLS EXP-Inferred LSPs (E-LSP) as defined by RFC 3270 as updated by 5462.

NI-011120 [**Required**] The router shall support DiffServ over MPLS by mapping DSCP code points of packets received into Label-Only-Inferred LSPs (L-LSPs) as defined by RFC 3270 as updated by 5462.

NI-011130 [**Optional**] The router shall support the 16-bit encoding mechanism for the identification of DiffServ PHB in protocol messages, including both code points defined by standards action and code points not defined by standards action, as specified in RFC 3140.

10.6.10 INTSERV

NI-011140 [**Required**] The router shall support Integrated Services (INTSERV) using RSVP for user-signaled per-flow QoS requirements and for reservation of resources as defined by RFCs 2205 and 2210.

NI-011150 [**Required**] The router shall provide Intserv Controlled Load service, which offers a customer service with a low average delay with limited packet loss as defined by RFC 2211.

NI-011160 [**Required**] The router shall provide Intserv Guaranteed service, which offers customers a precisely bounded maximum delay with no packet loss as defined by RFC 2212.

NI-011170 [**Required**] The router shall support preemption priority policy for signaled policy-based admission protocols used to establish MPLS LSPs as an alternate preemption mechanism to DiffServ as defined by RFC 3181. In particular, RSVP will be supported.

10.6.11 Congestion Control

NI-011180 [**Required**] The router shall provide congestion control based on the EXP field in the MPLS header for E-LSP packets. The router shall provide congestion control based on the MPLS label for L-LSP packets.

NI-011190 [**Required**] The router shall provide congestion control based on the DSCP for IPv4 packets.

NI-011200 [**Required**] The router shall provide congestion control based on the Traffic Class field for IPv6 packets.

10.6.12 Queuing

NI-011210 [**Required**] The router shall queue packets based on the EXP field in the MPLS header for E-LSP packets. The router shall provide queue packets based on the MPLS label for L-LSP packets.

NI-011220 [**Required**] The router shall queue packets based on the DSCP for IPv4 packets.

NI-011230 [**Required**] The router shall queue packets based on the Traffic Class field for IPv6 packets.

NI-011240 [**Required**] The router shall support QoS/CoS on all interfaces and sub-interfaces.

NI-011250 [**Required**] The router shall support Hierarchical QoS.

NI-011260 [**Required**] The router shall support minimum of 2 low-latency queues.

NI-011270 [**Required**] The router shall support any combination of CoS/QoS/EXP translations/mapping/imposing.

10.6.13 Multicast

NI-011280 [**Required**] The router shall support Protocol Independent Multicast-Sparse Mode (PIM-SM) as defined by RFCs 4601.

NI-011290 [**Required**] The router shall support the bootstrap NE Bootstrap Router (BSR) mechanism for PIM-SM as defined by RFC 5059.

NI-011300 [**Required**] The router shall be capable of performing the Rendezvous Point (RP) function for PIM-SM.

NI-011310 [**Required**] The router shall support multiple RPs in a single domain for load sharing and redundancy as defined by RFC 3446.

NI-011320 [**Required**] The router shall enhance interdomain multicast via Multicast Source Discovery Protocol (MSDP) as defined by RFC 3618.

NI-011330 [**Required**] The router shall support the Generic Routing Encapsulation (GRE) Tunneling Protocol as defined by RFC 2784 for the transport of multicast traffic.

NI-011340 [**Required**] The router shall be able to perform a reverse path forwarding (RPF) check on a GRE tunnel interface.

NI-011350 [**Required**] The router shall support Source-Specific Multicast (SSM) and its assigned address range as defined by RFC 4607.

NI-011360 [**Optional**] The router shall support the Border Gateway Multicast Protocol (BGMP) as defined by RFC 3913.

NI-011370 [**Required**] The router shall provide multicast routing for native IPv6 packets.

NI-011380 [**Required**] The router shall support the Internet Group Management Protocol, version 3 (IGMPv3) for IPv4 multicast management and multicast group membership reporting to neighboring multicast routers as defined by IETF RFC 3376.

NI-011390 [**Required**] The router shall support Multicast Listener Discovery (MLD) version 2 for IPv6 multicast routers to discover the presence of multicast listeners as defined by IETF RFC 4604.

NI-011400 [**Required**]The router shall support standards based Next Gen multicast features using point to multipoint LSPs.

10.6.14 Equipment Redundancy

NI-011410 [**Required**] The router shall support at least one redundant component for every N component that is required for full operation (1:N redundancy protection) for all service affecting components.

NI-011420 [**Required**] The router shall support redundant switch fabric elements and schedulers, System control processors, System clocks, Power supplies, and Cooling systems.

NI-011430 [**Required**] The router shall recover to its pre-failure forwarding performance level within 50 ms after the failure of a single component.

10.6.15 Management

NI-011440 [**Required**] The router shall support the Internet Group Management Protocol, Version 3 (IGMPv3) for IPv4 multicast management and multicast group membership reporting to neighboring multicast NE as defined by RFC 3376 and 4604.

NI-011450 [**Required**] The router shall support Multicast Listener Discovery (MLD), Version 2 for IPv6 multicast NEs to discover the presence of multicast listeners as defined by RFC 4604.

NI-011460 [**Required**] The router shall support administratively scoped addresses (239/8) and multicast administrative boundaries as described in RFC 2365.

10.7 INTERNET PROTOCOL TRANSPORT – PROVIDER EDGE (IPT-PE)

The Internet Protocol Transport – Provider Edge (IPT-PE) is a new PE layer being added to DISN IP network. It will support advanced MPLS Services. Initially, it will be implemented to support a variety of transport services such as Carrier Ethernet (VPLS, EVPL) and Carrier's Carrier (Labeled service). Layer 3 MPLS VPNs may be added in the future. IPT-PEs will use high-end modern Ethernet-dense routers supporting interfaces speeds of up to 100 Gig and

advanced Quality of Service. In addition to supporting new advanced MPLS services, the IPT-PE will replace the existing C-PE routers.

10.7.1 IPT-PE Availability

NI-011470 [**Required: IPT-PE**] The router hardware platform shall have an inherent availability of at least 99.999% (assuming a 4-hour mean-time-to-repair).

NI-011480 [**Required: IPT-PE**] The router line cards shall each have an inherent availability of at least 99.994% (assuming a 4-hour mean-time-to-repair).

10.7.2 IPT-PE Component Redundancy

NI-011490 [**Required: IPT-PE**] The router shall support at least one redundant unit for every N units that are required for full operation (1:N redundancy protection) for all critical components including but not limited to the following:

- System control processors.
- Switch fabric elements and schedulers.
- System clocks.
- Power supplies.
- Cooling systems.

10.7.3 IPT-PE Interface Specifications – Large Node

NI-011500 [**Required: IPT-PE**] The router shall support a minimum of 16, OC-12c/STM-4 POS ports. (The minimum number of ports that the router can support assuming only that type of interface is installed.)

NI-011510 [**Required: IPT-PE**] The router shall support a minimum of 16, OC-48c/STM-16 POS ports. (The minimum number of ports that the router can support assuming only that type of interface is installed.)

NI-011520 [**Required: IPT-PE**] The router shall support a minimum of 8, OC-192c/STM-64 POS ports. (The minimum number of ports that the router can support assuming only that type of interface is installed.)

NI-011530 [**Required: IPT-PE**] The router shall support a minimum of 200, 1Gbps Ethernet ports. (The minimum number of ports that the router can support assuming only that type of interface is installed.)

NI-011540 [**Required: IPT-PE**] The router shall support a minimum of 80, 10 Gbps Ethernet ports. (The minimum number of ports that the router can support assuming only that type of interface is installed.)

NI-011550 [**Required: IPT-PE**] The router shall support a minimum of 10, 100 Gbps Ethernet ports. (The minimum number of ports that the router can support assuming only that type of interface is installed.)

10.7.4 IPT-PE Interface Specifications – Other

NI-011560 [**Required: IPT-PE**] The router shall support at least 1.8 Tbps inbound and 1.8 Tbps outbound simultaneously (full-duplex), 3.6 Tbps aggregate, through the chassis switch-fabric/backplane.

NI-011570 [**Required: IPT-PE**] The router shall support wave-division multiplexing (WDM) interfaces.

NI-011580 [**Required: IPT-PE**] The router shall support ITU Optical Transport Network (OTN) framed interfaces as defined by ITU-T G.709/Y.1331, Interfaces for the Optical Transport Network (OTN).

10.7.5 IPT-PE Routing Specifications

NI-011590 [**Required: IPT-PE**] The router shall implement the Integrated IS-IS routing protocol as specified in IETF RFCs 1195, 5302, and 5304.

NI-011600 [**Required: IPT-PE**] The router shall support the IS-IS Extensions for Traffic Engineering as specified in IETF RFC 5305.

NI-011610 [**Required: IPT-PE**] The router shall support the Border Gateway Protocol, Version 4 as specified in IETF RFCs 4271 and 1772 for the exchange of network reachability information with external networks (EBGP) and the distribution of external network reachability with internal neighbors (IBGP).

NI-011620 [**Required: IPT-PE**] The router shall support the Multi-Protocol BGP (MP-BGP) Sub-Address Family Identifier (SAFI) for multicast addresses as specified in IETF RFC 4760.

NI-011630 [**Required: IPT-PE**] The router shall support MP-BGP SAFI for global unicast IPv6 Addresses as specified in IETF RFC 4760.

NI-011640 [**Required: IPT-PE**] The router shall support MP-BGP SAFI for MPLS Layer 3 VPN-IPv4 as specified in IETF RFCs 4760, and 4364.

NI-011650 [**Required: IPT-PE**] The router shall support a minimum of 500,000 best path BGP entries for IPv4 and 300,000 for IPv6 that are unique from each other in prefix/subnet.

NI-011660 [**Required: IPT-PE**] The router shall support a minimum of 650,000 best path BGP entries for IPv4 and 350,000 for IPv6 that are unique from each other in prefix/subnet in addition to 1,000,000 routes that provide alternate paths to those prefixes/subnets.

NI-011670 [**Required: IPT-PE**] The router shall support the Open Shortest Path First (OSPF) link state protocol as defined by IETF RFC 2328.

NI-011680 [**Required: IPT-PE**] The router shall support OSPF for IPv6 as defined by IETF RFC 5340.

NI-011690 [**Required: IPT-PE**] The router shall act as an MPLS Label Switching Router (LSR) by forwarding inbound labeled packets based on the contents of the packet MPLS header and performing label swapping (inbound packet label pop and outbound packet label push) as defined in IETF RFC 3031.

NI-011700 [**Required: IPT-PE**] The router shall support label stacks consisting of at least three labels.

NI-011710 [**Required: IPT-PE**] The router shall support label stacks consisting of five labels.

NI-011720 [**Required: IPT-PE**] The router shall support Forwarding Adjacencies (FA) and hierarchal or nested label switched paths as described in IETF draft-ietf-mpls-lsp-hierarchy.

NI-011730 [**Required: IPT-PE**] The router shall support extensions to RSVP for Generalized MPLS (GMPLS) as specified in IETF draft-ietf-mpls-bundle.

NI-011740 [**Required: IPT-PE**] The router shall support 10,000 bi-directional traffic engineered LSPs acting as an intermediate LSR.

NI-011750 [**Required: IPT-PE**] The router shall be able to originate 1000 traffic engineered LSPs and terminate the same number.

NI-011760 [**Required: IPT-PE**] The router shall be able to originate 2000 traffic engineered LSPs and terminate the same number.

NI-011770 [**Required: IPT-PE**] The router shall support the Label Distribution Protocol (LDP) for MPLS downstream-unsolicited label distribution as defined by IETF RFC 5036.

10.7.6 IPT-PE QoS Specifications

NI-011780 [**Required: IPT-PE**] The router shall support Differentiated Services (Diffserv) in accordance with IETF RFCs 2474 and 3140.

NI-011790 [**Required: IPT-PE**] The router shall support the Diffserv Expedited Forwarding (EF) per-hop-behavior and codepoint assignment as defined by IETF RFC 3246.

NI-011800 [**Required: IPT-PE**] The router shall support the Diffserv Assured Forwarding (AF) per-hop-behavior classes and codepoint assignments as defined by IETF RFC 2597.

NI-011810 [**Required: IPT-PE**] The router shall support Differentiated Services (Diffserv) over MPLS by mapping the Diffserv code points of packets received into MPLS EXP-Inferred LSPs (E-LSP) as defined by IETF RFC 3270.

NI-011820 [**Required: IPT-PE**] The router shall support Differentiated Services (Diffserv) over MPLS by mapping DiffServ code points of packets received into Label-Only-Inferred LSPs (L-LSPs) as defined by IETF RFC 3270.

NI-011830 [**Required: IPT-PE**] The router shall provide congestion control based on the EXP field in the MPLS header for E-LSP packets.

NI-011840 [**Required: IPT-PE**] The router shall provide congestion control based on the MPLS label for L-LSP packets.

NI-011850 [**Required: IPT-PE**] The router shall provide congestion control based on the DSCP for IPv4 packets.

NI-011860 [**Required: IPT-PE**] The router shall provide congestion control based on the Traffic Class field for IPv6 packets.

NI-011870 [**Required: IPT-PE**] The router shall queue packets based on the EXP field in the MPLS header for E-LSP packets.

NI-011880 [**Required: IPT-PE**] The router shall queue packets based on the MPLS label for L-LSP packets.

NI-011890 [**Required: IPT-PE**] The router shall queue packets based on the DSCP for IPv4 packets.

NI-011900 [**Required: IPT-PE**] The router shall queue packets based on the Traffic Class field for IPv6 packets.

NI-011910 [**Required: IPT-PE**] Router shall support QoS/CoS on all interfaces and sub-interfaces.

NI-011920 [**Required: IPT-PE**] Router shall support Hierarchichal QoS.

NI-011930 [**Required: IPT-PE**] Router shall support minimum of 2 low-latency queues.

NI-011940 [**Required: IPT-PE**] Router shall support any combination of CoS/QoS/EXP translations/mapping/imposing.

10.7.7 IPT-PE Advanced Services Specifications

10.7.7.1 VPLS

NI-011950 [**Required: IPT-PE**] Router shall support standards based VPLS as stated in RFC 4761 - Using BGP for Auto-Discovery and Signaling.

NI-011960 [**Required: IPT-PE**] Router shall support classification based on DSCP for Layer 2 MPLS services (Pseuowire, VPLS) with no or minimal performance hit.

NI-011970 [**Required: IPT-PE**] Router shall support Jumbo Frame 9000 byte MTU for interfaces in a VPLS.

NI-011980 [**Required: IPT-PE**] Router shall support 802.1ag - connectivity fault management.

NI-011990 [**Required: IPT-PE**] Router shall support 802.3ah - Link Layer OAM.

10.7.7.2 L3 VPN

NI-012000 [**Required: IPT-PE**] Router shall support standards based L3VPN as stated in RFC 4364 - BGP/MPLS IP Virtual Private Networks (VPNs).

NI-012010 [**Required: IPT-PE**] Router shall support 1000 VRFs with minimum of 1000 routes per VRF.

10.7.7.3 Carrier's Carrier

NI-012020 [**Required: IPT-PE**] Router shall support BGP labeled unicast as defined in RFC 3107.

10.7.7.4 Other Specifications

NI-012030 [**Required: IPT-PE**] Router shall support Distributed implementation of Multi-hop BFD with sub-second (or close to it) hellos – BFD should be done in Hardware on in software on Jacket/Line Card to support quick hellos.

NI-012040 [**Required: IPT-PE**] The router shall support BFD for LSPs.

NI-012050 [**Required: IPT-PE**] The router shall support BFD for GRE tunnels.

10.7.8 IPT-PE Multicast Specifications

NI-012060 [**Required: IPT-PE**] The router shall support Protocol Independent Multicast-Sparse Mode (PIM-SM) as defined by IETF RFC 4601.

NI-012070 [**Required: IPT-PE**] The router shall provide multicast routing for native IPv6 packets.

NI-012080 [**Required: IPT-PE**] The router shall support the Internet Group Management Protocol, version 3 (IGMPv3) for IPv4 multicast management and multicast group membership reporting to neighboring multicast routers as defined by IETF RFCs 3376 and 4604.

NI-012090 [**Required: IPT-PE**] The router shall support Multicast Listener Discovery (MLD) version 2 for IPv6 multicast routers to discover the presence of multicast listeners as defined by IETF RFC 4604.

NI-012100 [**Required: IPT-PE**] The router shall support standards based Next Gen multicast features using point to multipoint LSPs.

SECTION 11
NETWORK ELEMENTS

11.1 INTRODUCTION

This section specifies the requirements that must be met by the Defense Information Systems Network (DISN) Fixed network element (F-NE) and Deployed network element (D-NE) devices.

11.1.1 Applicability

This requirement applies to all network elements (NEs) procured or leased for installation in the DISN. This section is not applicable to those NEs that are covered explicitly in other sections of the Unified Capabilities Requirements (UCR). Figure 11.1-1, Network Element Diagram, illustrates how an NE can operate as a standalone device or integrated into the transmission interfaces of switches or other network devices.

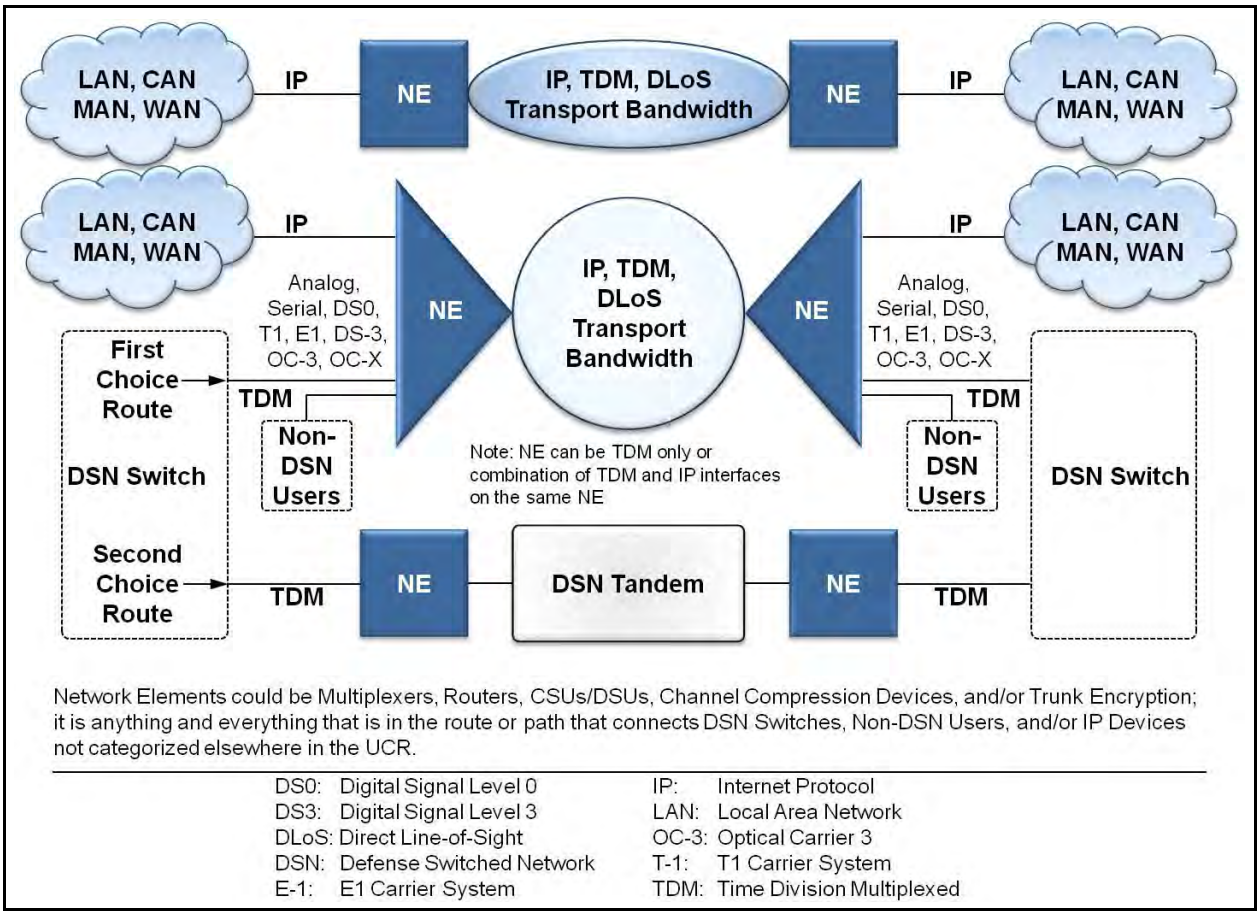


Figure 11.1-1. Network Element Diagram

An NE is any component of a network through which the Defense Switched Network (DSN) bearer and signaling traffic transits. This may include either Time Division Multiplexing (TDM) or Internet Protocol (IP) bearer and signaling traffic, or both. The transport between NEs may be

TDM, IP, or Direct Line of Sight (DLoS). 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) depending on its deployment. It can interconnect the Session Controller (SC).

11.2 DSN F-NE GENERIC

This section describes the requirements that must be met by DSN F NE devices. The F-NE is referred to as NEs throughout Section 11.2 and its subparagraphs.

11.2.1 General

As a minimum, the requirements in this section include the features and capabilities considered necessary for a particular switch type to support the Department of Defense (DoD) warfighter mission. In addition to the compliance requirements of the main body of this UCR, all NEs are to be compliant with the following requirements and conditions.

The following are NE general requirements and conditions:

NE-000010 [**Required**] The introduction of an NE(s) shall not cause the end-to-end (E2E) average mean opinion score (MOS) to fall below 4.0 as measured over any 5-minute time interval.

NE-000020 [**Required**] The introduction of an NE(s) shall not degrade the E2E measured bit error rate (BER) to more than .03 percent from the baseline minimum E2E digital BER requirement, which is not more than one error in $1x10^9$ bits (averaged over a 9-hour period).

NE-000030 [**Required**] The introduction of an NE(s) shall not degrade secure transmission for secure end devices as defined in Section 12.3, Secure Voice.

NE-000040 [**Required**] The NE(s) shall support a minimum modem transmission speed of 9.6 kbps across the associated NE(s).

NE-000050 [**Required**] The NE(s) shall support a minimum facsimile transmission speed of 9.6 kbps across the associated NE(s).

NE-000060 [**Required**] The NE shall transport all call control signals transparently on an E2E basis.

NE-000070 [**Conditional**] The NEs that support a point-to-multipoint (P2N) capability shall meet the following additional requirements when deployed in a P2N architectural configuration:

a. The aggregate egress from all NEs in the P2NP architecture must be identical to the aggregate ingress of all NEs in the same P2N architecture. However, if all or part of the P2N is operating in a P2MP mode that is applying multicast from a centrally designated NE to one or more of the associated peripheral NEs, the aggregate of the additional multicast traffic must be accounted for in the egress sum total.

b. Excluding latency, the P2N Association Path (AP) shall be measured as though it is a P2P architecture at the P2N AP NE endpoints ingress and egress points. As such, the P2N AP must meet all the other stated requirements of a P2P.

c. For a given P2N AP, the maximum latency allowed E2E, as measured over any 5-minute period at the P2N AP NE ingress and egress points, shall be 5 ms or less, when added in addition to the expected P2P latency. Hence, as an example, if the expected P2P latency requirement for a P2N AP is 50 ms, then P2N AP maximum latency, regardless of the number of NE hops between the ingress and egress NEs, the measured value shall not exceed 55 ms.

11.2.1.1 Alarms

NE-000080 [**Required**] The NE shall be able to propagate Carrier Group Alarms (CGAs) upon physical loss of the TDM interface. The NE shall provide the capability of detecting a CGA. When this alarm is detected, all associated outgoing trunks shall be made busy automatically to subsequent customer call attempts. Call attempts on associated incoming trunks shall not be processed. When possible, the Reverse Make Busy feature shall be exercised on incoming trunks. Voice switching systems using a TDM connection to an NE shall receive the proper CGAs from the NE upon loss of the transport link between NEs, regardless of whether the transport link is TDM, IP, or DLoS between the NEs. The NEs that support IP ingress or egress traffic either as inbound or outbound NE traffic and/or transport between NE(s) shall support one or more of the routing protocols (Link-State and/or Distance-Vector) so that the NE can notify the IP network (e.g., LAN, MAN), using one of these routing protocols, of the condition of its link state for transporting ingress IP traffic, namely operational or down.

11.2.1.2 Congestion Control

The NE shall ensure that congestion between paired NEs does not affect DSN calls in progress or subsequent calls. Call congestion handling shall be met in one or more of the ways specified in the following text.

11.2.1.2.1 For TDM Transport

NE-000090 [**Required**] The NE shall implement TDM congestion control via one of the following methods:

NE-000090.a [**Conditional**] A dynamic load control signal (e.g., contact closure) shall be provided to the DSN switch per the following requirements:

(1) The NE shall provide the capability to handle CGA indications from the carrier systems/equipment using the E-telemetry interface (scan points) for the TDM interfaces provided (e.g., DS0, DS1, and/or OC-X), and comply to the Telcordia Technologies GR-303-CORE, System Generic Requirements, Objectives, and Interface, December 2000, Issue 4, and Telcordia Technologies TR-NWT-000057

that specifies the use of a continuity testing (COT)-generated dc contact closure alarm to indicate an "all-accessible-channels-busy" condition.

(2) The NE, when interfaced to the network that provides an E-telemetry interface type (scan points) for alarm management, shall be capable of CGA management that is used to minimize the effects of carrier failures on switching systems and on service. CGA scan point (binary condition; i.e., "closed" contact for active and "opened" for inactive states), when "closed," should busy out the failed circuits, release customers from the failed circuits, prevent the failed circuits from seizing the DSN trunk equipment, and prevent the NE from seizing the failed circuits.

(3) The DSN CGA System Operation can be divided into three parts: detection of the carrier failure, conditioning the failed trunk, and reaction of the switching equipment to the processing of the failure. Requirements for scan point CGA are as follows:

(a) Sense Point Interface. The switching system shall provide sense points to which external CGAs can be interfaced so that failure of the carrier equipment shall cause the trunks to be removed from service.

(b) Call Processing Actions. Receipt of a CGA shall cause call processing to be aborted on associated trunks that are not in the talking state.

(c) Trunk Conditioning. Receipt of a CGA shall cause the following actions on the affected trunks:

i. Idle trunks shall be removed from the idle list. Subsequent calls for service must be ignored for the duration of the CGA. Busy-back shall be returned on those incoming trunks, which are optioned for busy-back while in the out-of-service state and proper Multilevel Precedence and Preemption (MLPP) treatment shall be applied.

ii. Trunks in the talking state shall be monitored for disconnect, after which they are to be placed in the same state as described previously for idle trunks.

(4) Restoration of Service. All trunks affected shall be returned to their previous state after the CGA is removed.

d. Congestion is not possible in the NE by nature of its functioning (e.g., a TDM multiplexer or transcoder).

e. A software capability in limiting the provisioning of the ingress and egress interfaces making congestion impossible even under the worst congestion scenario. This can be done by limiting the bearer or aggregate provisioning.

NE-000100 [**Conditional**] The addition of NEs with TDM transports shall not increase the one-way latency per NE pair when measured from E2E over any 5-minute period specified as follows:

a. Time Division Multiplexing ingress G.711 (nonsecure calls) to nontranscoding G.711 TDM egress shall not increase delay more than 10 ms per NE pair as measured end-to-end.

b. Time Division Multiplexing ingress G.711 (nonsecure calls) to transcoding TDM egress with compression codecs (Section 11.2.2, Compression) shall not increase delay by more than 100 ms per NE pair as measured end-to-end.

c. Time Division Multiplexing ingress G.711 (secure calls) to nontranscoding TDM egress G.711 shall not increase delay by more than 50 ms per NE pair as measured end-to-end.

d. Time Division Multiplexing ingress G.711 (secure calls) to transcoding TDM egress with compression codecs (Section 11.2.2, Compression) shall not increase delay by more than 250 ms per NE pair as measured end-to-end.

11.2.1.2.2 For IP Transport

NE-000110 [**Required**] The NE(s) using IP transport shall implement IP congestion control. Congestion may be controlled by using Differentiated Services (DiffServ), which shall be capable of providing preferential treatment for call congestion over other media types in accordance with (IAW) Section 6, Network Infrastructure End-to-End Performance, and a capability to limit the provisioning of input and output interfaces so congestion is impossible under the worst transport congestion scenario. The IP interface parameters subject to ingress or egress requirements shall be met IAW Section 11.2.3.9, IP Interface.

11.2.1.2.3 For DLoS Transport

The NE shall implement DLoS congestion control based on the DSN traffic and signaling type to be transported.

NE-000120 [**Required**] The NE transporting only TDM bearer and signaling traffic shall implement DLoS congestion control via one or more of the following methods:

a. A dynamic load control signal (e.g., contact closure).

b. Congestion is not possible in the NE so the maximum ingress throughput into the NE is configured so that it does not exceed the DLoS link maximum egress transport capability to include all DLoS overhead control traffic between the transport devices.

c. A software capability in limiting the provisioning of the ingress and egress interfaces making congestion impossible even under the worst congestion scenario. This can be done by limiting the bearer or aggregate provisioning.

NE-000130 [**Required**] The NE transporting only ingress IP traffic, and using a DLoS transport, excluding 802.11, and/or 802.16 series standards, shall implement DLoS IP congestion control per Section 11.2.1.2.2, For IP Transport. Additionally, IP congestion control may include a standards-based or proprietary protocol between the NEs that will adjust the Quality of Service

(QoS) of the NE based on DLoS transport monitoring feedback to the NE to accommodate for changing environmental link conditions.

NE-000140 [**Conditional**] If the NE transports both TDM and IP ingress traffic simultaneously over the same DLoS transport link, then the following occurs:

a. The NE shall provide congestion control so that it provides the same level of capability, respectively, for the appropriate traffic type, TDM and IP, per the requirements for single traffic type ingress or egress to the NE. Additionally, the congestion control may include a standards-based or proprietary protocol between the NEs that will adjust the QoS of the NE based on DLoS transport monitoring feedback to the NE to accommodate for changing environmental link conditions.

b. The use of DLoS transport shall not increase the one-way latency or packet delay per the requirements for TDM ingress and TDM or IP egress interfaces per Section 11.2.1.2.1, For TDM Transport, and Section 11.2.3.9, IP Interface, respectively.

11.2.2 Compression

NE-000150 [**Required**] The NE used for voice compression shall support at least one of the following standards:

- ITU-T Recommendation G.726.
- ITU-T Recommendation G.728.
- ITU-T Recommendation G.729.

11.2.3 Interface

11.2.3.1 Analog

NE-000160 [**Conditional**] If provided, the NE shall provide for a 2-wire and/or 4-wire analog trunk circuit(s) interface that interfaces using industry standard signaling and facility arrangements per one or more of the following:

a. E&M Trunk Circuits. The NE shall interface with exchange carriers using industry standard ear and mouth (E&M) signaling. The switching system shall interface with Type I and Type II E&M signaling in accordance with paragraph 9 and subparagraphs of GR-506-CORE. The switching system shall interface with Type V E&M signaling as defined in Paragraphs 6.8.5, 6.8.6, 6.8.7.2, 6.8.8.2, and 6.8.8.3 of Telcordia Technologies Document SR-2275. The DSN switch analog trunk interface shall always originate on the M-lead.

b. Single Frequency Trunk Circuits. The NE will interface with external switching facility (SF) equipment using a 4-wire E&M trunk circuit, either Type I or Type II. The DSN in-band signaling equipment utilizing SF will place a 2600 Hz tone on the circuit to indicate

the idle state (on-hook), and the tone will be removed from the circuit to indicate the busy state (off-hook). Signaling states will be conveyed via E and M leads (Type I or II) to the telephone equipment terminating the circuit on the equipment side of the interface. The SF trunk interface consists of only the voice path conductors (T, R, T1, R1), but, at a point between this transmission facility interface and the switching function, the SF signal will be translated back to the 2-state DC signals.

c. Dual-Frequency Trunk Circuits. The Dual Frequency Signaling Unit (DFSU) equipment used in the DSN operates in much the same way as an SF unit, except that, whenever the 2600 Hz tone is removed from the circuit, a 2800 Hz tone is applied for a short period (175 ms maximum). The 2800 Hz tone burst will serve as a confirmation tone; the receiving signaling unit will transition from on-hook to off-hook only if the loss of the 2600 Hz tone is followed by the 2800 Hz tone. This prevents false on-hook to off-hook transitions from occurring because of a break in the communications circuit. Like the SF trunk interface, the dual frequency (DF) trunk interface will consist of only the voice path conductors (T, R, T1, R1). The NE shall interface an external DFSU using a 4-wire E&M trunk circuit with Type I or II E&M signaling. This connection is on the equipment-side of a DF trunk interface.

11.2.3.2 Serial

NE-000170 [**Required**] The NE used for serial interface connections shall be IAW one of the following standards:

- ITU-T Recommendation V.35.
- TIA-232-F.
- EIA-449-1.
- TIA-530-A.

11.2.3.3 BRI ISDN

NE-000180 [**Optional**] The Integrated Services Digital Network (ISDN) basic rate interface (BRI) shall meet the following requirements and conditions:

- Requirements for this feature shall be IAW Telcordia Technologies references SR-NWT-002120, SR-NWT-002343, and TR-NWT-001268.
- The MLPP service capability requirements for this interface shall be IAW American National Standards Institute (ANSI) T1.619-1992 (R1999) and ANSI T1.619a-1994 (R1999).

11.2.3.4 DS1 Interface

NE-000190 [**Conditional**] If provided, the NE shall meet the following DS1 (T1) interface requirements and conditions of a PCM-24 Digital Trunk Interface:

PCM-24 Digital Trunk Interface: An NE shall provide a PCM-24 channel digital interface with a 1.544 Mbps T1 bit stream configured in either the D3/D4 (Superframe) framing format or the D5 Extended Superframe (ESF) framing format. D5 is also referred to as extended frame (EF). The same framing format shall be used in both directions of transmission. Voice signals shall be encoded in the 8-bit μ (255 quantized values) pulse code modulation (PCM) encoding law. Supervisory and dial pulse (DP) signals shall utilize the A and B bits of the D3/D4 format or the A, B, C, and D bits of the D5 format for pre-Common Channeling Signaling System No. 7 (CCS7) configurations. Voice channel address in-band signaling shall be provided on individual channels. The D5 format shall be the preferred and system "goal" digital framing format and shall be provided in accordance with MIL-STD-187-700.

a. Interface Characteristics. The NE shall use the DS1 24 channel standard interface as specified in ANSI T1.102, "Digital Hierarchy – Electrical Interfaces."

Table 11.2-1, PCM-24 Electrical Interface Characteristics, provides the electrical characteristics at the interface. Table 11.2-2 and Table 11.2-3 provide a listing of the framing characteristics.

Table 11.2-1. PCM-24 Electrical Interface Characteristics

NOMINAL LINE RATE	1.544 MEGABITS PER SECOND.
Line Rate Accuracy	In a self-timed, free running mode, the line rate accuracy shall be ± 50 bits/s (± 32 parts per million) or better
Line Code	B8ZS (Bipolar with 8-Zero Substitution) Bipolar/Alternate Mark Inversion may be used until Clear Channel Capability is required
Frame Structure	ESF (D5) or transitionally D3/D4
Medium	One balanced twisted pair shall be used for each direction of transmission
Pulse Amplitude	The amplitude of an isolated pulse shall be between 2.4 volts and 3.6 volts
Pulse Shape	The shape of every pulse that approximates an isolated pulse (is preceded by four zeros and followed by one or more zeros) shall conform to the mask in figure F10/G703 of ITU-T Recommendation G.703
Pulse Imbalance	In any window of seventeen consecutive bits, the maximum variation in pulse amplitudes shall be less than 200mV, and the maximum variation in pulse widths (half amplitude) shall be less than 20 ns
Power Level	For an all-ones signal, the power in a 3 kHz band centered at 772 kHz shall be between 12.6 dBm and 17.9 dBm. The power in a 3 kHz ± 1 kHz band centered at 1544 kHz shall be at least 29 dB below that at 772 kHz
Jitter	Where one Unit Interval (UI) is equal to 648 ns, the jitter of the signal shall not exceed the following limits, in both bands simultaneously: 1) Band 1 - 5.0 UIs, peak-to-peak, and 2) Band 2 - 0.1 UIs, peak-to-peak. Band 1 equals 10 Hz to 40 kHz. Band 2 equals 8 kHz to 40 kHz
DC Power	There shall be no dc power applied to the interface

Table 11.2-2. PCM-24 D3/D4 Interface Characteristics

Frame Organization	24 8-bit PCM words, plus 1 framing bit, in 125 microseconds

Channel PCM Word	Frames 1 through 5: 8-bit encoded voice sample
	Frame 6: 7-bit encoded voice sample; least significant bit is the "A" signaling bit
	Frames 7 through 11: 8-bit encoded voice sample
	Frame 12: 7-bit encoded voice sample; least significant bit is the "B" signaling bit
Channel Sampling Rate	8000 times/second
Channel Time Slot	5.18 microseconds
Bit Time Slot Framing Bit Pattern	648 ns
	Terminal Framing Bit: "101010" in odd-numbered frames (1, 3, 5, 7, 9, 11)
	Signaling Framing Bit: "001110" in even-numbered frames (2, 4, 6, 8, 10, 12)
Maximum Reframe Time	The DSN will reframe on the average within 50 milliseconds after an error free signal is restored

Table 11.2-3. PCM-24 ESF Interface Characteristics

D5 EXTENDED SUPERFRAME FORMAT FRAMING CHARACTERISTICS	
Frame Organization	24 8-bit PCM words, plus 1 framing bit, in 125 ms
Channel PCM Word	Frames 1 through 5: 8-bit encoded voice sample
	Frame 6: 7-bit encoded voice sample; least significant bit is the "A" signaling bit
	Frames 7 through 11: 8-bit encoded voice sample
	Frame 12: 7-bit encoded voice sample; least significant bit is the "B" signaling bit
	Frames 13 through 17: 8-bit encoded voice sample
	Frame 18: 7-bit encoded voice sample; least significant bit is the "C" signaling bit
	Frames 19 through 23: 8-bit encoded voice sample
	Frame 24: 7-bit encoded voice sample; least significant bit is the "D" signaling bit
	8000 times per second
	5.18 microseconds
	648 ns
	Frame and Superframe Synchronization Bit: 001011 (frames 4, 8, 12, 16, 20, 24)
	Cyclical Redundancy Check (CRC) Bit (frames 2, 6, 10, 14, 18, 22)
	Data Channel Link Bit (odd numbered frames 1, 3, 5, 7, 9, 11, 13, 15, 17, 19, 21, 23)
	The DSN will reframe on the average within 50 milliseconds after an error free signal is restored

b. Supervisory Channel Associated Signaling. On-hook and off-hook status of each channel is transmitted and derived from the coding of the "A" and "B" signaling bits. Trunk seizure, answer supervision, DP digits, preemption signals, and all other trunk supervisory information shall be sent and received on a per-channel basis using this scheme. Per-trunk signaling in the DSN switching system shall control the value of the "A" and "B" bits to indicate an on-hook ("A" = 0, "B" = 0) or an off-hook ("A" = 1,

"B" = 1) condition. When receiving supervisory status on digital trunks using the PCM-24 format, the DSN switching system shall interpret the combination of the "A" bit = 0 and the "B" bit = 0 as on-hook, and the combination bit = 1 and "B" bit = 1 as an off-hook indication. When signaling on Voice Frequency (VF) channels using the PCM-24 format, the least significant bit of each channel, every six frames, shall carry signaling information. Utilizing the four-state signaling option of the Superframe (D3) format, frame 6 shall contain the "A" channel signaling information and frame 12 shall contain the "B" channel signaling information. The switching system shall also interpret the combination of "A" bit = 1, "B" bit = 0, with bit position 2 in all 24 channels in the Superframe (D3) format equal to "0" as a channel alarm indication and shall also interpret the combination of "A" bit = 1, "B" bit = 0 as a remote make busy.

In the Extended Superframe (ESF) format ANSI defines a 16-state signaling option that labels the signaling bits "A" (frame 6), "B" (frame 12), "C" (frame 18), and "D" (frame 24). Because DSN does not require the "C" and "D" signaling channels, the 4-state option shall be used to allow changes in "A" and "B" signaling states to be transmitted twice as often. Utilizing Frames 6 and 18 in the 24-frame Extended Superframe shall contain the "A" channel signaling information; frames 12 and 24 shall contain the "B" channel signaling information.

c. Clear Channel Capability. The NE shall be capable of transmitting and receiving B8ZS line coding in accordance with MIL-STD-187-700.

d. Alarm and Restoral Requirements. The NE shall provide the alarm and restoral features on the digital interface unit (DIU) as defined in Table 11.2-4, PCM-24 Alarm and Restoral Requirements.

Table 11.2-4. PCM-24 Alarm and Restoral Requirements

Local Alarm Timing	The DSN PCM-24 DIU will enter the "LOCAL" or "RED" alarm state when it is unable to frame on the received PCM signal, or the received signal is lost, for 2.5 ± 0.5 seconds
Reception of Remote Alarm	The DSN PCM-24 DIU will detect a "REMOTE" or "YELLOW" alarm condition when bit 2 of all 24 channels of Superframe is set to a zero and when the "YELLOW" alarm is sent via the facility data link of Extended Superframe Within 35 to 1000 milliseconds after detecting the REMOTE alarm, the DSN switch will: Release all connections on the affected DIU AND Remove the affected circuits from service
Transmission of Remote Alarm	When the DSN PCM-24 DIU enters the LOCAL alarm state, it will send REMOTE alarm toward the connecting equipment by forcing bit 2 to a zero on all 24 channels of Superframe
Restoral to Service From Local Alarm	Within 15 ± 5 seconds after a valid PCM signal is restored, the DSN DIU will: Remove the REMOTE alarm being sent to the connecting equipment AND Return the affected circuits to service

Restoral to Service From Remote Alarm	Within 20 to 1000 milliseconds after the connecting equipment removes the REMOTE alarm, the DSN switch DIU will restore the affected circuits to service

11.2.3.5 E1 Interface

NE-000200 [**Required**] If provided, the NE shall meet the following E1 interface requirements and conditions of a PCM-30 Digital Trunk Interface:

PCM-30 Digital Trunk Interface: The NE shall provide PCM-30 digital interfaces at a data rate of 2.048 Mbps. The PCM-30 interfaces shall meet the requirements of ITU-T Recommendation G.703 and ITU-T Recommendation G.732. Voice signals in the PCM-30 framing format shall utilize the A-law encoding technique in accordance with ITU-T Recommendation G.772 (REV), "Protected Monitoring Points on Digital Transmission Systems." The pertinent requirements for the PCM-30 interface are summarized in Table 11.2-5, PCM-30 Electrical Interface Characteristics.

Table 11.2-5. PCM-30 Electrical Interface Characteristics

NOMINAL LINE RATE	2.048 MEGABITS PER SECOND
Line Rate Accuracy	In a self-timed, free running mode, the line rate accuracy shall be ± 102 bits/s (± 50 parts per million) or better
Line Code	HDB3
Frame Structure	Frame structure details appear in ITU-T Recommendation G.704
Medium	One balanced twisted pair shall be used for each direction of transmission
Pulse Amplitude	The amplitude of an isolated pulse shall be between 2.2 volts and 3.3 volts
Pulse Shape	The shape of every pulse that approximates an isolated pulse (is preceded by three zeros and followed by one or more zeros) shall conform to the mask in Figure 1 5/G703 of ITU-T Recommendation G.703
Pulse Imbalance	The ratio of amplitudes of positive and negative isolated pulses shall be between 0.95 and 1.05
Power Level	For an all-ones signal, the power in a 3 kHz ± 1 kHz band centered at 1.024 MHz shall be between 13.7 dBm and 17.5 dBm. The power in a 3 kHz ± 1 kHz band centered at 2.048 MHz shall be at least 20 dB below that at 1.024 MHz
Jitter	Where one Unit Interval (UI) is equal to 488 ns, the jitter of the signal shall not exceed the following limits, in both bands simultaneously: 1) Band 1 - 5.0 UIs, peak-to-peak, and 2) Band 2 - 0.1 UIs, peak-to-peak. Band 1 equals 10 Hz to 40 kHz. Band 2 equals 8 kHz to 40 kHz
dc Power	There shall be no dc power applied to the interface
Frame	32 channels (numbered 0 to 31) with 8 bits (numbered 1 to 8) per channel
Organization	PCM words. Frame alignment occupies bit positions 2 through 8 of channel 0, of every other frame
Multiframe Organization	16 consecutive frames, numbered from 0 to 15
Channel Sampling Rate	8000 times per second
Channel PCM Word	Channel time slots 1 to 15, and 17 to 31, are assigned to telephone channels 1 to 30

NOMINAL LINE RATE	2.048 MEGABITS PER SECOND
Channel Time Slot	3.91 microseconds
Tolerance	+50 ppm on line rate of 1.544 megabits per second
Bit Time Slot	488 nanoseconds
Framing Bit Pattern	Bits 2 through 8 of channel 0, every other frame, contains the "0011011" frame alignment signal. To avoid falsely locking to the data contained in channel 0 for frames not containing the frame alignment signal, bit 2 of channel 0 is always a "1" in those frames
Multiframe Alignment	The multiframe alignment signal is "0000" and occupies digit time slots 1 to 4 of channel time slot 16 in frame 0
Framing Strategy	Frame alignment is assumed to be lost if 3 of 4 consecutive frame alignment signals are received with an error
Reframing Algorithm	Frame alignment is assumed to be recovered if the next frame has a "1" in bit 2 of channel 0 and valid framing is present in the frame after that
Multiframe Loss and Recovery	Multiframe alignment is assumed to be lost when two consecutive multiframe alignment signals are received in error. Multiframe alignment is assumed to be restored when the first correct multiframe alignment signal is detected

Table 11.2-6 shows the allocation of time slot 16 for channel associated signaling.

Table 11.2-6. Allocation of Time Slot 16

CHANNEL TIME SLOT 16 OF FRAME 0	CHANNEL TIME SLOT 16 OF FRAME 1		CHANNEL TIME SLOT 16 OF FRAME 2		FR 3-14 18-29	CHANNEL TIME SLOT 16 OF FRAME 15	
0000 xyxx	ABCD Channel 1	ABCD Channel 16	ABCD Channel 2	ABCD Channel 17	3-14 18-29	ABCD Channel 15	ABCD Channel 30
NOTES: When bits B, C, or D are not used they shall have the value: B = 1 C = 0 D = 1 The combination 0000 of bits A, B, C, and D shall not be used for signaling purposes for channels 1-15							
LEGEND x = Spare bit to be made 1 if not used y = Bit used to indicate loss of multiframe alignment (REMOTE alarm)							

a. Supervisory Channel Associated Signaling. When receiving supervisory status on digital trunks using the PCM-30 format, the DSN switching system shall interpret the combination of the "A" signaling channel bit = 1 and the "B" signaling channel bit = 1 as on-hook, and shall interpret the combination of the "A" signaling channel bit = 0 and the "B" signaling channel bit = 1 as an off-hook indication. The DSN switching system shall also interpret the combination of "A" bit = 1 and "B" bit = 0 as a channel alarm indication and a remote make busy. Bits "C" and "D" are not used in the DSN for signaling or control and therefore shall be set to the values "C" = 0 and "D" =1 in accordance with ITU-T Recommendation G.704.

b. Alarm and Restoral Requirements. The NE shall provide the alarm and restoral features on the DIU in order to be compatible with PCM-30 facilities and terminal equipment, as shown in Table 11.2-7, PCM-30 Alarm and Restoral Requirements.

Table 11.2-7. PCM-30 Alarm and Restoral Requirements

Local Alarm Timing	The DSN PCM-30 DIU shall enter the "LOCAL" or "RED" alarm state when framing is lost, or the incoming signal is lost, for 4.5 ± 0.5 seconds
Reception of Remote Alarm	The DSN PCM-30 DIU shall detect a "REMOTE" or "YELLOW" alarm condition when bit 3 of channel time slot 0 in those frames not containing the frame alignment signal is set to a "1," and will interpret this transition as a remote alarm from the connecting equipment. Within 35 to 1000 ms after detecting the REMOTE alarm, the DSN switch will: Release all connections on the affected DIU AND Remove the affected circuits from service
Transmission of Remote Alarm	When the DSN PCM-30 DIU enters the LOCAL alarm state, it shall send within 2 ms a REMOTE alarm toward the connecting equipment by changing bit 3-channel time slot 0 from a "0" to a "1" in those frames not containing the frame alignment signal
Restoral to Service From Local Alarm	Within 15 ± 5 seconds after a valid PCM signal is restored, the DSN switch shall: Remove the REMOTE alarm being sent to the connecting equipment AND Return the affected circuits to service
Restoral to Service From Remote Alarm	Within 20 to 1000 ms after the connecting equipment removes the REMOTE alarm, the DSN switch shall restore the affected circuits to service

11.2.3.6 DS3 Interface

NE-000210 [**Required**] The DS3 interface shall meet the following requirements and conditions.

11.2.3.6.1 Framing

NE-000220 [**Required**] Frame structure shall include M13 framing IAW ANSI T1.107-2002.

NE-000230 [**Optional**] Frame structure may include C-bit parity application IAW ANSI T1.107-2002.

11.2.3.6.2 Line Coding

NE-000240 [**Required**] The line coding shall be bipolar 3 zero substitution (B3ZS) IAW ANSI T1.102-1993.

11.2.3.7 Timing

NE-000250 [**Required**] The NE shall be able to derive a timing signal from an internal source, an incoming digital signal, or an external source IAW Section 10.4, Timing Synchronization.

11.2.3.8 OC-X Interface

NE-000260 [**Required**] The OC-X interface shall be IAW Section 10.3.2, Optical Transport System Interface, and/or appropriate Synchronous Optical Network (SONET) commercial standards.

(NOTE: X stands for the capacity (e.g., 3, 48, 192 and higher).

11.2.3.9 IP Interface

NE-000270 [**Optional**] The NE having an IP interface and using DLoS transport composed of 802.11 and/or 802.16 series standards shall instead meet the requirements for a Wireless Access Bridge (WAB) contained in Section 7.3, Wireless. All other IP configurations shall meet the following:

NE-000270.a [**Required**] Delay. The addition of NEs with IP transports shall not increase the one-way latency per NE pair when measured from end to end over any 5-minute period specified as follows:

(1) Time Division Multiplexing ingress G.711 (nonsecure calls) to non-transcoding G.711 IP egress shall not increase delay more than 50 ms per NE pair as measured end-to-end.

(2) Time Division Multiplexing ingress G.711 (nonsecure calls) to transcoding IP egress with compression codecs (Section 11.2.2, Compression) shall not increase delay by more than 100 ms per NE pair as measured end-to-end.

(3) Time Division Multiplexing ingress G.711 (secure calls) to non-transcoding G.711 IP egress shall not increase delay by more than 50 ms per NE pair as measured end-to-end.

(4) Time Division Multiplexing ingress G.711 (secure calls) to transcoding IP egress with compression codecs (Section 11.2.2, Compression) shall not increase delay by more than 250 ms per NE pair as measured end-to-end.

a. Jitter. The addition of an NE shall not cause jitter measured from ingress to egress to increase by more than 5 ms averaged over any 5-minute period.

b. Packet Loss. The addition of an 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.

NE-000270.b [**Required: F-NE, D-NE**] For VVoIP systems, if the system decrypts the VVoIP traffic and applies a proprietary encryption approach before transmittal between

the two components of the single vendor system, then the system proprietary encryption approach shall be one of the encryption and integrity-approved approaches defined in Section 4, Information Assurance.

NOTE: For example, if the NE decrypts the Assured Services Session Initiation Protocol (AS-SIP) with Transport Layer Security (TLS) packets between the NEs and re-encrypts it using NE proprietary encryption methods, then the proprietary method must be one of the cryptographic methods defined in Section 4, Information Assurance, [e.g., IPSec with AES-128 bit encryption, HMAC-SHA1 for integrity, and DoD Public Key Infrastructure (PKI) for authentication]. All Section 4, Information Assurance, approved encryption and integrity approaches use Federal Information Processing Standard (FIPS) PUB 140-2 cryptographic modules [or have been granted a formal waiver by National Institute of Standards and Technology (NIST)]. Importantly, proprietary only refers to the lack of interoperability with a different vendor's NE and all cryptographic approaches used in Section 4, Information Assurance, are standards based.

NE-000270.c [**Required: F-NE, D-NE**] The VVoIP systems that use proprietary encryption approaches within the system shall restore the VVoIP packets to their original format [e.g., AS-SIP with TLS and Secure Real-Time Transport Protocol (SRTP)] upon exiting from the system to ensure the VVoIP session can complete successfully.

NE-000280 [**Conditional**] The IP interface shall meet the IP requirements detailed in the Department of Defense Information Technology Standards Registry (DISR).

11.2.4 Device Management

11.2.4.1 Management Options

NE-000290 [**Required**] The NE devices are to be managed by at least one of the following two choices note that if option b. then sub (1), (2), and (3) are required:

a. A front or back panel and/or external console control capability shall be provided for local management.

b. Remote monitoring and management by the Advanced DSN Integrated Management Support System (ADIMSS) or similar Network Management (NM) systems developed by DoD Components. The following requirements apply:

   NE-000290.a [**Required: Data Interface**] The NE shall provide network management (NM) data/monitoring via one or more of the 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 data that is collected shall be accessible through these interfaces. For NM purposes, the NE must provide no less than two separate data channels. They may be physically separate (e.g., two distinct physical interface points) or logically separate (e.g., two user sessions through a single Ethernet interface). The data may be sent in ASCII, binary, or hexadecimal data or ASCII text designed for screen/printer display.

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

- Alarm/Log Data.
- Performance Data (e.g., traffic data).
- NE access (to perform NE data fill administration and network controls).

NE-000290.b [**Required: Fault Management**] The DSN telephone switching systems shall detect fault (alarm) conditions and generate alarm notifications. The alarm messages must be sent to the assigned NM Alarm channel in 30 seconds or less. No alarm restriction/filtering are necessary. In addition to the data formats in Section 2.19, Management of Network Appliances, alarms may be sent as Simple Network Management Protocol (SNMP) traps. If this channel is also used to output switch administrative log information, the alarm messages must be distinguishable from an administrative log message.

NE-000290.c [**Required: Configuration Management**] Requirements for this feature shall be in accordance with Telcordia Technologies GR-472-CORE, Section 4.

11.2.4.2 Fault Management

NE-000300 [**Required**] The NE shall report any failure of self-test diagnostic function on nonactive and active channels on a noninterference basis to the assigned NMS.

11.2.4.3 Loopback Capability

NE-000310 [**Required**] The NE shall provide loopback capability on each of the trunk-side interfaces IAW ITU-T Recommendation V.54.

11.2.4.4 Operational Configuration Restoral

NE-000320 [**Required**] Loss of power should not remove configuration settings. Unit should be restored to the last customer-configured state before the power loss, without intervention when power is restored.

11.2.4.5 DLoS Transport MOS, Maximum Transmission Range, and Measuring Methodology

NE-000330 [**Conditional**] The NEs using DLoS transport shall support the following:

NE-000330.a [**Required**] A minimum MOS score as defined in Section 11.2.1, General, performance requirement or better as measured in any 5-minute interval using ITU-T Recommendation P.862 testing standard.

NE-000330.b [**Required**] The minimum acceptable maximum transmission range (MTR) shall be 300 feet based on operating in an open air-minimal obstruction, clear line-of-sight environment with the DLoS transport device operating at or near full power mode. Based on the testing results, the estimated maximum performance range while still maintaining MOS requirements, as required in item a, shall hereby be referred to as the NE DLoS transport MTR.

The MTR baseline-testing environment shall be while operating in an open air-minimal obstruction, clear line-of-sight environment with the DLoS transport device operating at or near full power mode. The NE shall be tested at a minimum operating height of 25 feet with a clear unobstructed line of sight between NEs at a minimum range of 150 feet. The NEs may be tested with attenuation inserted to simulate the actual NE DLoS transport capability from which the maximum MOS performance range MTR can be extrapolated.

The value determined shall be included in the Approved Products List (APL) report. Refer to Section 11.2.5.3, Submission of DLoS Transport NEs to the UC Connection Office (UCCO) for DSN Connection Request, concerning guidelines on submitting the DLoS transport NE engineering analysis package.

11.2.5 DLoS Deployment Guidance

11.2.5.1 DLoS Transport NE Maximum Deployment Range

DoD Components using DLoS transport NEs shall engineer the deployment of said transport devices to compensate for operational capacity usage and impairments. Local weather and clutter or reflections will affect the operational range of free space optics and Radio Frequency (RF) DLoS transport NEs, respectively. Redundancy shall be factored in too. The following calculation will define the maximum deployment range (MDR) for engineering purposes based on local conditions:

MDR=MOR(1-(WD/365))

The MDR between the DLoS transport transmit and receive devices compensated for redundancy, if used, capacity usage, weather, clutter, and reflections, which is to be submitted for engineering analysis per Section 11.2.5.3, Submission of DLoS Transport NEs to UCCO for DSN Connection Request. In mixed redundancy, DLoS transport environments, such as using

free space optics and millimeter wave together, the furthest distance calculated will be the MDR value.

The maximum operational range (MOR) between the DLoS transport transmit and receive devices is based on the MTR as defined in Section 11.2.4.5, DLoS Transport MOS, Maximum Transmission Range, and Measuring Methodology, that is further compensated for local clutter and reflections per the line of sight the NEs are to be deployed. Also included in the calculation is the affecting performance factors for operational bandwidth utilization and required receive power level to maintain MOS 4.0, versus baseband transport utilization requirement. The DLoS transport link redundancy, if used, shall also be factored into the analysis. This calculation is to be submitted as part of the engineering analysis per Section 11.2.5.3, Submission of DLoS Transport NEs to UCCO for DSN Connection Request.

Weather Days (WDs) are the best estimate of yearly average of weather impairment days as calculated over 2 consecutive years from the date of the submittal required per Section 11.2.5.3, Submission of DLoS Transport NEs to UCCO for DSN Connection Request. A WD is an operational weather impairment that is estimated to result in the MOS score to drop below 4.0 for more than 2 consecutive hours during a standard business day at the calculated MOR distance. More than 2 impairment hours constitutes as a single WD. Subsequent weather-related MOS impairments on the same calendar day do not constitute another WD. A summary of the WD data and yearly average calculation will be submitted as part of the engineering analysis per Section 11.2.5.3.

11.2.5.2 TDM Only and IP over TDM Access

An NE with only TDM interfaces that uses a DLoS transport link can be used to transport TDM only or IP over TDM access traffic. Figure 11.2-1, TDM and IP over TDM Access via DLoS Transport NE, provides examples.

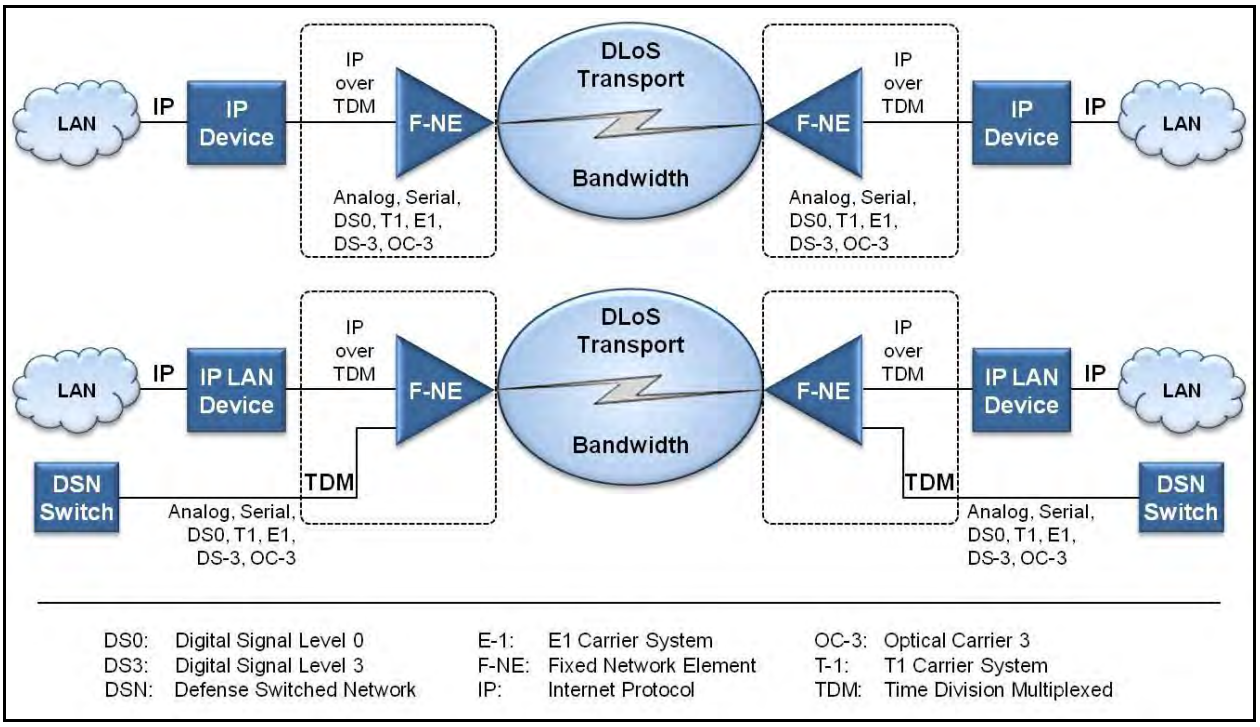


Figure 11.2-1. TDM and IP Over TDM Access via DLoS Transport NE

NE-000340 [**Required**] The NE TDM only or IP over TDM Access interfaces can transport IP traffic provided it is deployed per the following conditions:

a. The IP device is listed on the APL either as a component of an Assured Services LAN (ASLAN) and/or Customer Edge (CE) Router (CE-R).

b. The IP device meets the appropriate IP congestion controls for that IP device.

c. The connection from the IP device to the NE meets one or more of the NE interface requirements, other than IP, as described in Section 11.2.3, Interface.

d. The physical or configured capacity of the interface link (e.g., Section 11.2.3, Interface) from the IP device to the NE shall not exceed the transport capacity of the NE DLoS transport link, as determined in and modified per, or the portion thereof the transport link allocated to transport the IP traffic. The DLoS transport control traffic overhead will be included in traffic capacity determination.

e. Upon DLoS transport link loss in either direction between the NEs for IP over TDM connections, either the generated alarm from the NE shall be interpreted by the IP device as link failure and/or signaling packets, such as keep-alive packets or other standard routing protocol/proprietary control means between the IP devices fails, or will be interpreted by the IP device as failure of the link connected to the NE also.

11.2.5.3 Submission of DLoS Transport NEs to UCCO for DSN Connection Request

NE-000350 [**Conditional**] The DLoS transport NEs shall be engineered properly so that the DLoS transport transmitting or receiving 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. Included is the calculation and data required for determining the MDR, as defined in Section 11.2.5.1, DLoS Transport NE Maximum Deployment Range. For certification procedures, the UCCO submittal shall also include wireless security compliancy as identified in Section 11.2.6, Security.

11.2.6 Security

NE-000360 [**Required**] All components of the NE shall meet security requirements, for each supported mode, as outlined in DoD Instruction (DoDI) 8510.01 and the applicable Security Technical Implementation Guidelines (STIGs).

11.2.7 DLoS Transport Wireless Intrusion Detection System

NE-000370 [**Conditional**] If a DoD-approved Wireless Intrusion Detection System (WIDS) exists for the DLoS transport technology used, the NE DLoS transport link(s) shall be monitored in according with the appropriate STIG(s).

11.3 D-NE

NE-000380 [**Required**] The D-NEs shall meet all NE requirements specified in Section 11.2, DSN F-NE Generic, except as modified by the following paragraphs. The D-NEs shall be tested under a simulated Deployed environment using the operational area network (OAN) architecture framework and the following parameters:

a. Inclusion of satellite-based transmission links. With respect to D-NE testing, the following parameters will be used when injecting burst errors into the network. The D-NE being tested shall continue to function as specified in Section 11.2.1, General, and Section 11.3.1, D-NE General, during such testing:

   (1) Error Burst Density. The D-NE measured error burst density shall be $1x10^{-6}$.

   (2) Error Burst Gap (gap between error bursts in ms). The measured D-NE error burst gap shall be 600 ms.

   (3) Error Burst Length (length of error burst in ms). The measure D-NE error burst length shall be 500 ms.

11.3.1 D-NE General

NE-000390 [**Optional**] The D-NEs may include voice compression, as specified in Section 11.2.2, Compression, to include the following additional compression standard: ITU-T Recommendation G.723.

NE-000400 [**Optional**] Network element latency requirements for various codecs are defined in Section 11.2, DSN F-NE Generic. The D-NE allows for one additional codec, G.723.1. The latency introduced by a single D-NE using the G.723.1 codec shall be less than 90 ms. The latency introduced by a pair of D-NEs using the G.723.1 codec shall be less than 180 ms.

NE-000410 [**Required**] Voice calls placed through a set of D-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.

NE-000420 [**Required**] The introduction of a D-NE shall not cause the E2E digital BER to degrade the Tactical BER below $1x10^{-5}$ by more than 0.03 percent as measured over a 9-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.

NE-000430 [**Required**] The D-NE (when implemented in pairs) shall apply error correction to correct the errors interjected by the transport network between the two D-NEs so the resulting BER of the external facing D-NE interface shall be better than $1x10^{-5}$ as measured over a 9-hour period.

NE-000440 [**Required**] The NE shall ensure that congestion within NEs does not affect DSN calls in progress or subsequent calls. Call congestion handling shall be met in one or more of the following ways:

a. A dynamic load control signal (e.g., contact closure) shall be provided to the DSN switch IAW Section 11.2.1.2, Congestion Control.

b. A software capability in limiting the provisioning of the input and/or output interfaces that make congestion impossible even under the worst congestion scenario.

c. Congestion is not possible in the NE by the nature of its functioning (e.g., a TDM multiplexer or transcoder).

11.3.2 D-NE TDM

NE-000450 [**Conditional**] The D-NE shall support at least one of the interfaces listed in Section 11.2, DSN F-NE Generic. 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 Section 11.2.1.2, Congestion Control.

11.3.3 D-NE IP

Figure 11.3-1, D-NE Connectivity Using IP Transport, shows how IP can be used to provide transport for both D-NEs and Virtual Deployed Network Elements (VD-NEs). The D-NEs also can be used to pass data in addition to UC services (e.g., VVoIP).

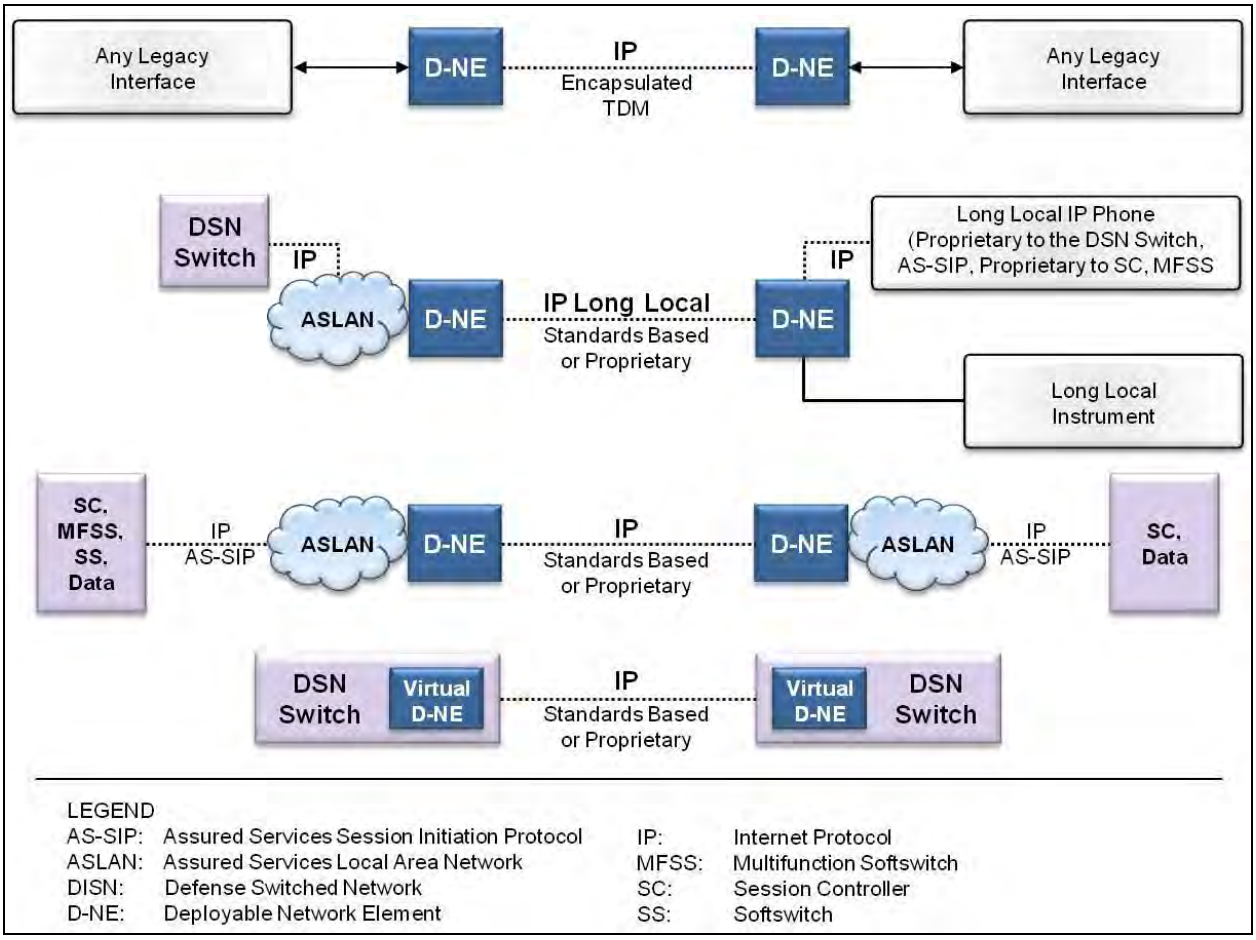


Figure 11.3-1. D-NE Connectivity Using IP Transport

NE-000460 [**Optional**] The D-NEs may use IP as a means to transport voice communications between D NEs. Interfaces supporting IP shall meet the appropriate specifications for that physical interface as stipulated in the latest DISR Baseline Release. The IP transport of voice services across D-NEs shall be accomplished through any one or more of the following methods: encapsulated TDM, long local, or Proprietary IP Trunk (PIPT).

NE-000470 [**Required**] For any IP transport methods used, D-NEs using IP interfaces shall meet the following parameters:

a. The addition of D-NEs shall meet the latency criteria specified in Section 11.3.1, D-NE General.

b. The addition of a D-NE shall not cause jitter measured from ingress to egress to increase by more than 5 ms averaged over any 5-minute period.

c. The addition of a D-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.

11.3.4 Encapsulated TDM

The D-NEs that use encapsulated TDM shall meet all the following requirements:

NE-000480 [**Required**] The D-NE shall use either DS or integrated services to provide preferential treatment over IP transport.

NE-000490 [**Required**] The D-NE shall provide an IP bandwidth reservation or allocation mechanism to allow for the user-specified allocation of bandwidth to support the full nonblocking voice services requirement.

NE-000500 [**Required**] The D-NE shall implement IP congestion control. Congestion may be controlled by using DS that shall be capable of providing preferential treatment for call congestion over other media types IAW Section 6, Network Infrastructure End-to-End Performance, and a capability to limit the provisioning of input and output interfaces, so congestion is impossible under the worst transport congestion scenario.

11.3.5 Carrier Group Alarms

NE-000510 [**Required**] The D-NE shall be able to propagate CGAs IAW Section 11.2.1.1, Alarms, upon physical loss of the ingress TDM interface. Voice switching systems, DSN or Deployable Voice Exchange (DVX), shall receive the proper CGAs from the D-NE upon loss of the IP transport link between D-NEs.

11.3.6 Long-Local

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

NE-000520 [**Required: D-NE**] The D-NE shall provision features and functions to support the long-local device.

NE-000530 [**Required: D-NE**] The D-NE shall allocate enough bandwidth to support the long-local device to ensure assured services and nonblocking requirements are met.

11.3.7 Proprietary IP Trunk

NE-000540 [**Conditional**] Virtual D-NEs that use PIPT shall meet all the requirements specified in the following paragraphs:

> **NE-000540.a** [**Required**] The DVX VD-NE may use proprietary IP signaling for this solution, and this interface shall support E2E ANSI T1.619a features and functions IAW

Section 2.26.1.6, ISDN MLPP Primary Rate Interface (PRI) (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, Session Initiation Protocol, Version 2 (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 Section 2, is provided to the DSN IP telephony subscriber.

NE-000540.b [**Required**] For DVX VD-NE switches that do not support MLPP, this interface shall support end-to-end ISDN PRI National ISDN 1/2 (NI ½) features and functions (i.e., Bearer, Calling Number Delivery). 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.

11.3.8 Secure Call Handling

NE-000550 [**Required**] In processing secure calls [Secure Communications Interoperability Protocol (SCIP)] across conversion boundaries, such as TDM to IP and/or IP to TDM, the D-NE shall use the V.150.1 standards implementation IAW National Security Agency (NSA) SCIP-215 and SCIP 216 for said ingress and egress conversions, respectively. The D-NE shall support this NSA V.150.1 implementation capability on all D-NE interface ports where secure call conversion can occur. The secure call handling implementation on the D-NE also shall meet the requirements of Section 11.2.1, sub-requirement 3.

NE-000560 [**Required**] The secure call shall complete successfully as a minimum equal to or better than 85 percent of the time when used in the Deployed environment.

11.3.9 Voice Packet Multiplexing

NE-000570 [**Optional**] A D-NE that is equipped with voice packet multiplexing, where individual small IP voice packets (from either the same or multiple sources) may be combined into a single larger IP packet. The D-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.

SECTION 12
GENERIC SECURITY DEVICES

12.1 INTRODUCTION

This section of the UCR provides an overview of End Cryptographic Units (ECUs) e.g., High Assurance Internet Protocol Encryptor (HAIPE), Secure Communications Interoperability Protocol (SCIP) Device, and Link Encryptor Family (LEF) and a framework of the interoperability testing of these products.

12.2 HAIPE

ENC-000010 [**Required: HAIPE**] High Assurance Internet Protocol (IP) Encryptor (HAIPE) End Cryptographic Units (ECUs) shall have the capability to be loaded and configured with legacy algorithms and modes to provide legacy-interoperable encryption services with 99 percent reliability.

ENC-000020 [**Required: HAIPE**] HAIPE ECUs shall have an inherent Information Assurance capability to ensure information and process integrity (during storage, processing, transmission, and presentation) to prevent unauthorized or unintended changes with 99 percent reliability.

ENC-000030 [**Required: HAIPE**] HAIPE ECUs shall be capable of loading and accepting keying material (KEYMAT) from National Security Agency (NSA)-approved key fill devices with 99 percent reliability.

ENC-000040 [**Required: HAIPE**] HAIPE ECUs shall include a DS-101 cryptographic fill port interface in accordance with (IAW) Electronic Key Management System (EKMS) 308 with 90 percent reliability.

ENC-000050 [**Required: HAIPE**] The ECUs shall recover last known, good operational state/settings after loss of primary power with 99 percent reliability.

ENC-000060 [**Optional: HAIPE**] The ECUs should have the capability to provide data to management devices to generate user defined high-level operational status reports with 90 percent reliability.

ENC-000070 [**Required: HAIPE**] The HAIPE(s) shall not preclude operation over low bandwidth networks as low as 2.4 kbps with 90 percent reliability.

ENC-000080 [**Optional: HAIPE**] The HAIPEs should have the capability to execute the In-Line Network Encryptor (INE) Management command and control function with 100 percent reliability.

ENC-000090 [**Optional: HAIPE**] The HAIPEs should have the capability to execute the Backup Remote Management (RM) command and control function with 90 percent reliability.

ENC-000100 [**Required: HAIPE**] The ECUs shall prevent the accidental deletion of all loaded operational key with 99 percent reliability.

ENC-000110 [**Required: HAIPE**] As a minimum, new software releases shall be backward compatible with the previous NSA-certified version of software.

ENC-000120 [**Required: HAIPE**] The HAIPE(s) shall be able to recover security associations after loss of power on either one or both ends of the link with 95 percent reliability.

ENC-000130 [**Required: HAIPE**] The HAIPE(s) shall adhere to standard commercial interfaces (e.g., Ethernet, Fast Ethernet, Gigabit Ethernet, or 10Gigabit Ethernet).

ENC-000140 [**Required: HAIPE**] The HAIPE(s) devices shall be compatible with network components such as routers and hosts in common usage within the Global Information Grid (GIG) Information Assurance architecture.

ENC-000150 [**Required: HAIPE**] The HAIPE(s) shall be capable of being reprogrammed with updated cryptographic software and algorithms.

ENC-000160 [**Required: HAIPE**] The HAIPE(s) shall operate over connections to satellite links that experience delays of up to 2 seconds aggregate with 90 percent reliability.

ENC-000170 [**Required: HAIPE**] When subjected to 70 percent or greater of rated throughput, the HAIPE(s) shall maintain secure communications without interruption (i.e., without reboot) with 90 percent reliability.

ENC-000180 [**Required: HAIPE**] The HAIPE(s) devices shall achieve 85 percent of its OEM's advertised throughput.

ENC-000190 [**Required: HAIPE**] The average, minimum, and maximum latency shall be calculated for each frame size at the highest frame rate that yields 0 percent packet loss. Latency Tests are conducted to measure the response time of packets through a pair of Units under Test (UUTs). The latency numbers are pulled from the throughput results. The average, minimum, and maximum latency is calculated for each frame size at the highest frame rate that yields 0 percent packet loss.

ENC-000200 [**Required: HAIPE**] The HAIPE(s) devices shall properly tunnel multicast data from a single host on one RED enclave to multiple hosts on a remote RED enclave 99 percent of the time.

ENC-000210 [**Required: HAIPE**] The HAIPE(s) devices shall demonstrate support for Quality of Service (QoS), if the device can properly bypass Type of Service (TOS) bits 99 percent of the time, in accordance with multiple modes of bypass that the vendor has incorporated.

12.3 LINK ENCRYPTOR FAMILY (LEF)

ENC-000220 [**Required: LEF**] The LEF ECUs shall have the capability to be loaded and configured with legacy algorithms and modes to provide legacy-interoperable encryption services with 90 percent reliability.

ENC-000230 [**Required: LEF**] The LEF ECUs shall have an inherent Information Assurance capability to ensure information and process integrity (during storage, processing, transmission, and presentation) to prevent unauthorized or unintended changes with 90 percent reliability.

ENC-000240 [**Required: LEF**] The LEF ECUs shall be capable of loading and accepting keying material (KEYMAT) from NSA-approved key fill devices with 99 percent reliability.

ENC-000250 [**Required: LEF**] The LEF ECUs shall include a DS-101 cryptographic fill port interface IAW EKMS 308 with 99 percent reliability.

ENC-000260 [**Required: LEF**] The LEF ECUs shall implement data interfaces that conform to the EIA-530 standard.

ENC-000270 [**Required: LEF**] The LEF ECUs shall implement data interfaces that conform to the RS-232 standard.

ENC-000280 [**Required: LEF**] The LEF ECUs shall be able to recover last known, good operational state/settings after loss of primary power with 99 percent reliability.

ENC-000290 [**Optional: LEF**] The ECUs should have the capability to provide data to management devices to generate user defined high-level operational status reports with 90 percent reliability

ENC-000300 [**Required: LEF**] The LEF ECUs shall be capable of operating with legacy Time Division Multiple Access (TDMA) architectures for networked data exchange with 90 percent reliability.

ENC-000310 [**Required: LEF**] The LEF ECUs shall be able to automatically recover security connections after loss of power on one end or both ends of a channel with 90 percent reliability.

ENC-000320 [**Required: LEF**] The ECUs shall prevent the accidental deletion of all loaded operational keys with 99 percent reliability.

ENC-000330 [**Required: LEF**] As a minimum, new software releases shall be backward compatible with the previous NSA-certified version of software with 90 percent reliability.

ENC-000340 [**Required: LEF**] The LEF ECUs shall provide autophase if interoperable with KG-84C with 90 percent reliability.

ENC-000350 [**Required: LEF**] The LEF ECUs shall have Over-the-Air-Rekey (OTAR) capability with 90 percent reliability.

12.4 SECURE VOICE

ENC-000360 [**Required: SCIP Enabled DSCD**] The enabled Department of Defense Secure Communications Device (DSCD) shall be only those that are Type Approved by NSA and are listed on the NSA Secure Product Web site. Each DSCD must support at least one NSA-approved secure protocol. If the DSCD supports more than one secure protocol, then it must meet all the requirements for at least one of the secure protocols, and must minimally support the other protocols that are provided on the DSCD.

ENC-000370 [**Required: SCIP Enabled DSCD**] The DSCD devices that use a two-wire analog or Basic Rate Interface (BRI) shall meet the End Instrument (EI) requirements as specified in Section 3.7, Customer Premises Equipment. The DSCD devices that use an IP interface shall meet the EI requirements as specified in Section 2, Session Control Products. DSCD devices that support Defense Switched Network (DSN) trunk interfaces (Primary Rate Interface [PRI] or IP Assured Services [AS] Session Initiation Protocol [SIP] [AS-SIP]) shall meet the interface requirements defined in the following:

a. Section 2.14.10, MG Support for Integrated Services Digital Network (ISDN) PRI Trunks, of Unified Capabilities Requirements (UCR) 2013.
b. AS-SIP 2013.

ENC-000380 [**Required: SCIP Enabled DSCD**] A DSCD device that supports one of the required signaling modes shall interoperate with and establish secure sessions with other compatible devices with at least an 85 percent secure call completion rate.

ENC-000390 [**Required: SCIP Enabled DSCD**] The DSCD shall be capable of using the protocol(s) provided to establish a secure session within 60 seconds and must maintain secure communications for the duration of the secure portion of the call.

ENC-000400 [**Required: SCIP Enabled DSCD**] The DSCD shall be capable of operating in networks that have an End-to-End latency of up to 600 milliseconds.

ENC-000410 [**Required: SCIP Enabled DSCD**] The DSCD shall achieve and maintain a secure voice connection with a minimum Mean Opinion Score (MOS) of 3.0.

ENC-000420 [**Required: SCIP Enabled DSCD**] Once connected to the rekey center, the DSCD shall obtain a new key and properly process that new key with a 95 percent rekey completion rate.

ENC-000430 [**Conditional: SCIP Enabled DSCD**] If the DSCDs establish secure sessions on a Continuously Variable Slope Delta (CVSD) switch and terminate on a CVSD switch, without ever traversing or otherwise interacting with the DSN, Defense RED Switch Network (DRSN), or Public Switched Telephone Network (PSTN), then it must do so with a 50 percent completion rate.

ENC-000440 [**Conditional: SCIP enabled DSCD**] If the DSCDs establish secure sessions on IP networks using Secure Communications Interoperability Protocol (SCIP), then it shall satisfy all the end point requirements described SCIP-215 and SCIP-216.

ENC-000450 [**Required: SCIP Enabled DSCD**] The DSCD devices shall support a minimum data rate and facsimile transmission rate of 9.6 kbps.

SECTION 13
SECURITY DEVICES

13.1 INTRODUCTION

This section describes the requirements for security devices that will be on the Approved Products List (APL). This version contains requirements for Firewalls (FWs), Intrusion Prevention Systems (IPSs), Network Access Controller (NAC), and Virtual Private Network (VPN) devices. Future updates to this section will expand on the devices discussed.

Based on the Unified Capabilities (UC) Information Assurance design, threats, and countermeasures, a set of derived requirements were developed. Different vendors combine different functions into their appliances to meet the requirements of a particular type of product. For the purposes of the Unified Capabilities Requirements (UCR), the requirements are levied on the individual appliance, as applicable, to secure the entire product. The terms "user" and "customer" are used in the same context as in Telcordia Technologies GR-815-CORE. It is understood that the Information Assurance design provides a high-level description of how the security services are applied to the appliance and how the appliances interact in a secure manner. In addition, the appropriate Security Technical Implementation Guidelines (STIGs) will further clarify how the Information Assurance design and requirements are implemented on the appliance. All security devices shall comply with the "Application Security Technical Implementation Guide." This section is intended to provide a level of security requirements consistent with the level of security requirements defined for the UC, but adapted for the unique Department of Defense (DoD) UC environment consistent with the requirements in the UCR.

Finally, the derived requirements do not include all administrative requirements (nontechnical) associated with policy and the STIGs. For instance, if someone is required to administratively document something (e.g., waiver, pilot request), that requirement is not included. The acronyms and appliances used for specifying the type of component are shown in Table 13.1-1, Acronyms and Appliances Specifying Type of Component.

Table 13.1-1. Acronyms and Appliances Specifying Type of Component

ACRONYM	APPLIANCES
FW	Firewall
IAT	Information Assurance Tool
IPC	Internet Protocol Count
IPS	Intrusion Prevention System
ISS	Integrated Security Solution
NAC	Network Access Controller
VPN	Virtual Private Network – concentrator and termination
WIDS	Wireless Intrusion Detection System

13.2 REQUIREMENTS

13.2.1 Conformance

SEC-000010 [**Required: VPN**] The security device shall conform to all of the MUST requirements found in Request for Comments (RFC) 3948, "UDP Encapsulation of IPSec Packets."

13.2.2 General

SEC-000020 [**Required: FW, IPS, VPN, NAC, WIDS**] The security device shall support interoperability with Network Time Protocol (NTP) version 3 (NTPv3).

SEC-000030 [**Required: NAC, VPN**] The security device shall be managed from a central place, clients, and servers.

SEC-000040 [**Required: FW, IPS, VPN**] The security device shall properly implement an ordered list policy procedure.

SEC-000050 [**Required: FW, IPS, NAC**] The security device shall apply a set of rules in monitoring events and based on these rules indicate a potential violation of the security device security policy.

SEC-000060 [**Required: FW, IPS, VPN**] An automated, continuous online monitoring and audit trail creation capability is deployed with the capability to immediately alert personnel of any unusual or inappropriate activity with potential Information Assurance implications.

SEC-000070 [**Required: FW, IPS**] If the security device allows configuration of access settings, the security device shall provide minimum recorded security-relevant events including any activity caught by the "deny all" rule at the end of the security device rule base.

SEC-000080 [**Required: FW~~, IPS, WIDS~~**] The security device shall log matches to filter rules that deny access when configured to do so.

SEC-000090 [**Required: IPS, VPN**] The security device shall log an information flow between a source subject and a destination subject via a controlled operation if the information security attributes match the attributes in an information flow policy rule (contained in the information flow policy).

SEC-000100 [**Required: IPS, VPN**] The security device shall log data and audit events when a replay is detected.

SEC-000110 [**Required: IPS, VPN, WIDS**] The security device shall be able to collect the following: Identification, Authentication, and Authorization events at the layer which they are operating; i.e., WIDS may only operate at Layer 2.

SEC-000120 [**Required: IPS, VPN, WIDS**] The security device shall be able to collect network traffic at the layer in which it is operating. The network traffic collected will be a COTS feature of the system and documented in a Letter of Compliance (LOC).

SEC-000130 [**Required: IPS, VPN, WIDS**] The security device shall be able to collect detected known vulnerabilities.

SEC-000140 [**Required: FW, IPS, NAC, VPN**] The security device's controlled interface shall be configured such that its operational failure or degradation shall not result in any unauthorized release of information outside the Information Security (IS) perimeter nor result in any external information entering the IS perimeter.

SEC-000150 [**Required: FW, IPS, NAC, VPN, WIDS**] The security device must protect itself against attempts by unauthorized users to bypass, deactivate, or tamper with security device security functions.

SEC-000160 [**Required: FW, IPS, NAC, VPN**] The security device shall drop all packets with an Internet protocol (IP) version 4 (IPv4) source address of all zeros.

SEC-000170 [**Required: FW, IPS, NAC, VPN**] The security device shall drop all traffic from the internal network that does not use a legitimate internal address range as its source address.

SEC-000180 [**Required: FW, IPS, WIDS**] The security device shall pass traffic without altering the contents, unless the security device has identified the traffic as being a security problem, or as necessary to perform functions such as Network Address Translation (NAT).

SEC-000190 [**Required: FW, IPS, WIDS**] A security device shall prevent all known network-based current attack techniques (Common Vulnerabilities and Exploits) from compromising the security device.

SEC-000200 [**Required: FW, IPS**] The security device shall mediate the flow of all information between a user on an internal network connected to the security device and a user on an external network connected to the security device and must ensure that residual information from a previous information flow is not transmitted.

SEC-000210 [**Required: FW, IPS, NAC, VPN**] The security device shall reject requests for access or services in which the presumed source identity of the source subject is an external Information Technology (IT) entity on a broadcast network.

SEC-000220 [**Required: IPS, NAC, VPN, WIDS**] The security device shall detect replay attacks using either security device data or security attributes.

SEC-000230 [**Required: FW, IPS, VPN**] The security device shall ensure that the security policy enforcement functions are invoked and succeed before each function within the security functions scope of control is allowed to proceed.

SEC-000240 [**Required: FW~~, IPS, VPN~~**] The security device shall enforce System Administrator policy regarding Instant Messaging traffic.

SEC-000250 [**Required: FW~~, IPS, VPN~~**] The security device shall enforce System Administrator policy regarding Voice and Video over Internet Protocol (VVoIP) traffic.

SEC-000260 [**Required: FW, IPS, NAC, VPN**] The controlled interface shall provide the ability to restore its functionality fully in accordance with documented restoration procedures.

SEC-000270 [**Required: FW, IPS**] Each controlled interface shall be configured to ensure that all (incoming and outgoing) communications protocols, services, and communications not explicitly permitted are prohibited.

SEC-000280 [**Required: FW, IPS, VPN, NAC**] The security device shall provide a high availability failover capability that maintains state. This capability shall be configurable.

The security device shall ensure that security device data will be maintained if the following occurs to the security device:

SEC-000290 [**Required: FW, IPS, VPN, NAC**] Fails.

SEC-000300 [**Required: FW, IPS, VPN, NAC**] Is attacked.

SEC-000310 [**Required: FW, IPC, VPN, NAC**] Storage becomes exhausted.

SEC-000320 [**Required: FW, IPC, VPN, NAC**] Fails to restart/reboot.

13.2.3 Performance

Security without performance brings productivity to a standstill. Security devices are intended to mitigate the threats enclaves face from external sources while permitting transmission of legitimate traffic in both directions. Performance tests attempt to validate a security device's ability to maintain that legitimate traffic stream while the network is under attack.

SEC-000330 [**Required: FW, IPS, VPN, WIPS**] The developer must specify the security device's bandwidth requirements and capabilities. This shall include the maximum bandwidth speeds the device will operate on as well as the security device bandwidth requirements (bandwidth in kbps) documented by whom the device communicates with, frequency, and kbps transmitted and received (e.g., product downloads, signature files).

SEC-000340 [**Required: FW, IPS, VPN**] The security device, as configured, must process new connections at the rate of the expected maximum number of connections as advertised by the vendor within a 1-minute period.

SEC-000350 [**Required: FW, IPS, VPN**] The security device, as configured, must process new HyperText Transfer Protocol (HTTP) connections at the rate of the expected maximum number of connections as advertised by the vendor within a 1-minute period.

SEC-000360 [**Required: FW, IPS, VPN**] The security device, as configured, must process new secure File Transfer Protocol (FTP) connections at the rate of the expected maximum number of connections as advertised by the vendor within a 1-minute period.

SEC-000370 [**Required: FW, IPS, VPN, WIPS**] The security device shall use a commercial best practice defensive solution and maintain advertised normal operation packet loss rates for all legitimate data packets when under a SYN Flood attack.

SEC-000380 [**Required: FW**] The security device shall demonstrate a latency variance of less than 20 percent and a packet loss variance of less than 10 percent of the manufacturer-specified nominal values for all operational conditions.

13.2.4 Functionality

13.2.4.1 Firewall and VPN

13.2.4.1.1 Policy

This section identifies the need for a security device to respond to policy-based actions set by a System Administrator. While not mandating specific options, the System Administrator should have granular control of the security device. Options of responses the security device could perform because of specific acts might include one or more of the following:

- Ceasing to operate (failing to secure).
- Terminating encrypted connections.
- Sending alerts via console message.

SEC-000390 [**Required: FW, VPN**] The security device shall enforce the policy pertaining to any indication of a potential security violation.

SEC-000400 [**Required: FW, VPN**] The security device shall be configurable to perform actions based on different information flow policies.

SEC-000410 [**Required: FW, VPN**] The security device shall deny establishment of an authorized user session based on network source (i.e., source IP address).

SEC-000420 [**Required: FW**] The security device shall enforce the System Administrator's specified maximum quota of transport-layer open connections that a source subject identifier can use over a specified period.

SEC-000430 [**Required: FW, VPN**] The security device shall enforce the System Administrator's policy options pertaining to network traffic violations to a specific TCP port within a specified period.

SEC-000440 [**Required: FW, VPN**] The security device shall enforce the System Administrator's policy options pertaining to violations of network traffic rules within a specified period.

SEC-000450 [**Required: FW, VPN**] The security device shall enforce the System Administrator's policy options pertaining to any security device-detected replay of data and/or nested security attributes.

SEC-000460 [**Required: VPN**] The security device shall provide the ability to push policy to the VPN client and the ability to monitor the client's activity.

SEC-000470 [**Required: FW**] The security device shall have five Ethernet ports, one pair for primary ingress and egress, one pair for backup, and one for Out-of-Band Management (OOBM).

SEC-000480 [**Required: FW**] The security device, when configured, shall log the event of dropping packets and the reason for dropping them.

SEC-000490 [**Required: VPN**] At a minimum, the following confidentiality policy adjudication features shall be provided for each controlled interface. Encrypt, as needed, all outgoing communication including the body and attachment of the communication.

SEC-000500 [**Required: FW**] A security device shall properly enforce the TCP state.

SEC-000510 [**Required: FW**] A security device shall properly accept and deny traffic based on multiple rules.

13.2.4.1.2 Filtering

This section addresses the ability of a firewall to perform basic filtering functions. It does not mandate a specific filtering configuration for firewalls.

The integrity policy adjudication feature known as filtering shall be provided. The security device's controlled interface must support and filter communications protocols/services from outside the perimeter of the interconnected ISs according to IS-appropriate needs (e.g., filter based on addresses, identity, protocol, authenticated traffic, and applications). Filtering is defined as having the ability to block on a per-interface basis, defaulting to block, and defaulting to disabled, if supported on the security device itself.

SEC-000520 [**Required: FW**] A security device will apply filtering to the service User Datagram Protocol (UDP) echo (port 7).

SEC-000530 [**Required: FW**] A security device will apply filtering to the service UDP discard (port 9).

SEC-000540 [**Required: FW**] A security device will apply filtering to the service UDP chargen (port 19).

SEC-000550 [**Required: FW**] A security device will apply filtering to the service UDP TCP Multiplexer (TCPMUX) (port 1).

SEC-000560 [**Required: FW**] A security device will apply filtering to the service UDP daytime (port 13).

SEC-000570 [**Required: FW**] A security device will apply filtering to the service UDP time (port 37).

SEC-000580 [**Required: FW**] A security device will apply filtering to the service UDP supdup (port 95).

SEC-000590 [**Required: FW**] A security device will apply filtering to the service UDP sunrpc (port 111).

SEC-000600 [**Required: FW**] A security device will apply filtering to the service UDP loc-srv (port 135).

SEC-000610 [**Required: FW**] A security device will apply filtering to the service UDP netbios-ns (port 137).

SEC-000620 [**Required: FW**] A security device will apply filtering to the service UDP netbios-dgm (port 138).

SEC-000630 [**Required: FW**] A security device will apply filtering to the service UDP netbios-ssn (port 139).

SEC-000640 [**Required: FW**] A security device will apply filtering to the service UDP BootP (port 67).

SEC-000650 [**Required: FW**] A security device will apply filtering to the service UDP Trivial File Transfer Protocol (TFTP) (port 69).

SEC-000660 [**Required: FW**] A security device will apply filtering to the service UDP X Display Manager Control Protocol (XDMCP) (port 177).

SEC-000670 [**Required: FW**] A security device will apply filtering to the service UDP syslog (port 514).

SEC-000680 [**Required: FW**] A security device will apply filtering to the service UDP talk (port 517).

SEC-000690 [**Required: FW**] A security device will apply filtering to the service UDP ntalk (port 518).

SEC-000700 [**Required: FW**] A security device will apply filtering to the service UDP MS SQL Server (port 1434).

SEC-000710 [**Required: FW**] A security device will apply filtering to the service UDP MS Universal Plug and Play (UPnP) System Services Delivery Point (SSDP) (port 5000).

SEC-000720 [**Required: FW**] A security device will apply filtering to the service UDP Network File System (NFS) (port 2049).

SEC-000730 [**Required: FW**] A security device will apply filtering to the service UDP Back Orifice (port 31337).

SEC-000740 [**Required: FW**] A security device will apply filtering to the service TCP TCPMUX (port 1).

SEC-000750 [**Required: FW**] A security device will apply filtering to the service TCP echo (port 7).

SEC-000760 [**Required: FW**] A security device will apply filtering to the service TCP discard (port 9).

SEC-000770 [**Required: FW**] A security device will apply filtering to the service TCP systat (port 11).

SEC-000780 [**Required: FW**] A security device will apply filtering to the service TCP daytime (port 13).

SEC-000790 [**Required: FW**] A security device will apply filtering to the service TCP netstat (port 15).

SEC-000800 [**Required: FW**] A security device will apply filtering to the service TCP chargen (port 19).

SEC-000810 [**Required: FW**] A security device will apply filtering to the service TCP time (port 37).

SEC-000820 [**Required: FW**] A security device will apply filtering to the service TCP whois (port 43).

SEC-000830 [**Required: FW**] A security device will apply filtering to the service TCP supdup (port 95).

SEC-000840 [**Required: FW**] A security device will apply filtering to the service TCP sunrpc (port 111).

SEC-000850 [**Required: FW**] A security device will apply filtering to the service TCP loc-srv (port 135).

SEC-000860 [**Required: FW**] A security device will apply filtering to the service TCP netbios-ns (port 137).

SEC-000870 [**Required: FW**] A security device will apply filtering to the service TCP netbios-dgm (port 138).

SEC-000880 [**Required: FW**] A security device will apply filtering to the service TCP netbios-ssn (port 139).

SEC-000890 [**Required: FW**] A security device will apply filtering to the service TCP netbios-ds (port 445).

SEC-000900 [**Required: FW**] A security device will apply filtering to the service TCP rexec (port 512).

SEC-000910 [**Required: FW**] A security device will apply filtering to the service TCP lpr (port 515).

SEC-000920 [**Required: FW**] A security device will apply filtering to the service TCP uucp (port 540).

SEC-000930 [**Required: FW**] A security device will apply filtering to the service TCP Microsoft UPnP SSDP (port 1900).

SEC-000940 [**Required: FW**] A security device will apply filtering to the service TCP X-Window System (ports 6000–6063).

SEC-000950 [**Required: FW**] A security device will apply filtering to the service TCP Internet Relay Chat (IRC) (port 6667).

SEC-000960 [**Required: FW**] A security device will apply filtering to the service TCP NetBus (ports 12345–12346).

SEC-000970 [**Required: FW**] A security device will apply filtering to the service TCP Back Orifice (port 31337).

SEC-000980 [**Required: FW**] A security device will apply filtering to the service TCP finger (port 79).

SEC-000990 [**Required: FW**] A security device will apply filtering to the service TCP Simple Network Management Protocol (SNMP) (port 161).

SEC-001000 [**Required: FW**] A security device will apply filtering to the service UDP SNMP (port 161).

SEC-001010 [**Required: FW**] A security device will apply filtering to the service TCP SNMP trap (port 162).

SEC-001020 [**Required: FW**] A security device will apply filtering to the service UDP SNMP trap (port 162).

SEC-001030 [**Required: FW**] A security device will apply filtering to the service TCP rlogin (port 513).

SEC-001040 [**Required: FW**] A security device will apply filtering to the service UDP who (port 513).

SEC-001050 [**Required: FW**] A security device will apply filtering to the service TCP rsh, rcp, rdist, and rdump (port 514).

SEC-001060 [**Required: FW**] A security device will apply filtering to the service TCP new who (port 550).

SEC-001070 [**Required: FW**] A security device will apply filtering to the service UDP new who (port 550).

SEC-001080 [**Required: FW**] A security device will apply filtering to the service Network Time Protocol (NTP).

SEC-001090 [**Required: FW**] A security device will apply filtering to the service Cisco Discovery Protocol (CDP).

SEC-001100 [**Required: FW**] A security device will apply filtering to Voice and Video Services [Assured Services Session Initiation Protocol (AS-SIP)], H.323, and Resource Reservation Protocol (RSVP).

SEC-001110 [**Required: FW**] A security device will apply filtering to the service UDP Secure Real-Time Transport Control Protocol (SRTCP) and Real-Time Transport Control Protocol (RTCP).

SEC-001120 [**Required: FW**] A security device will apply filtering to the service Differentiated Services Code Point (DSCP).

13.2.4.2 IPS, WIDS Functionality

SEC-001130 [**Required: IPS**] The security device shall detect and protect against a focused method of attack: Footprinting and Scanning.

SEC-001140 [**Required: IPS**] The security device shall detect and protect against a focused method of attack: Enumeration.

SEC-001150 [**Required: IPS**] The security device shall detect and protect against a focused method of attack: Gaining Access.

SEC-001160 [**Required: IPS**] The security device shall detect and protect against a focused method of attack: Escalation of Privilege.

SEC-001170 [**Required: IPS**] The security device shall detect and protect against a focused method of attack: Network Exploitation.

SEC-001180 [**Required: IPS**] The security device shall detect and protect against a focused method of attack: Cover Tracks.

SEC-001190 [**Required: IPS**] The security device shall have the capability to provide proper notification upon detection of a potential security violation or to forward event status data to a Network Management System (NMS) that will take the appropriate action to include providing notification of the event.

SEC-001200 [**Required: IPS**] The security device shall have the capability to alert the administrator immediately by displaying a message at the local and remote administrative consoles when an administrative session exists for each of the defined administrative roles.

SEC-001210 [**Required: IPS, WIDS**] The security device shall generate an audit record of all failures to reassemble fragmented packets.

SEC-001220 [**Required: IPS**] The security device shall log requests in which the information received by the security device contains the route (set of host network identifiers) by which information shall flow from the source subject to the destination subject.

SEC-001230 [**Required: IPS**] The security device shall log an information flow between a source subject and a destination subject via a controlled operation if the source subject has successfully authenticated to the security device.

SEC-001240 [**Required: IPS**] The security device shall reject data when a replay is detected.

13.2.4.2.1 IPS VVoIP Signal and Media Inspection

The following requirements are for any IPS device that has the capability to inspect VVoIP signals correctly.

SEC-001250 [**Optional: IPS**] The device shall support the capability to detect and send alarms in responses to threats identified in VVoIP signaling.

SEC-001260 [**Optional: IPS**] The IPS shall support the capability to detect an abnormal number of 401/407 AS-SIP response messages, indicating that a possibly unauthorized user or device is attempting to connect to the system.

SEC-001270 [**Optional: IPS**] The IPS shall support the capability to detect when an abnormal time-out for an AS-SIP request occurs (e.g., large numbers of repeated AS-SIP requests or responses, unusual number of AS-SIP requests sent with no matching response).

NOTE: If an AS-SIP request time-out occurs, it could be an indication that the system has failed because of a denial of service (DoS) attack resulting from a maliciously crafted request.

SEC-001280 [**Optional: IPS**] The device shall support the capability to detect when AS-SIP messages exceed a configurable maximum message length.

SEC-001290 [**Optional: IPS**] The device shall support the capability to detect when an AS-SIP message contains nonprintable characters.

NOTE: The presence of nonprintable characters could indicate an attempt by an adversary to insert executable code or cause abnormal behavior in a system.

SEC-001300 [**Optional: IPS**] The device shall support the capability to detect attempts to inject SQL queries into AS-SIP signaling messages.

SEC-001310 [**Optional: IPS**] The device shall support the capability to detect unusual IPv4 or IPv6 addresses contained in AS-SIP messages (e.g., the local host/loopback address, link local addresses).

SEC-001320 [**Optional: IPS**] The device shall support the capability to detect traffic that does not have the characteristics of AS-SIP traffic, but is still sent over a channel established for sending AS-SIP messages (e.g., strings of characters that are not AS-SIP related).

SEC-001330 [**Optional: IPS**] The device shall support the capability to detect and send alarms in response to threats identified in VVoIP media traffic and other traffic that flows across the Session Border Controller (SBC) boundary.

SEC-001340 [**Optional: IPS**] The device shall detect attempts to inject packets into a media stream or perform replay attacks (e.g., duplicate sequence numbers appearing in a Real-time Transport Protocol [RTP] stream).

SEC-001350 [**Optional: IPS**] The device shall support the capability to detect traffic that should be VVoIP traffic based on its headers, but does not have the characteristics of a VVoIP traffic stream.

SEC-001360 [**Optional: IPS**] The device shall support the capability to detect signatures associated with the presence of data, files, executables, SQL commands, viruses, or other unusual data contained within a media stream intended for VVoIP.

SEC-001370 [**Optional: IPS**] The device shall support the capability to detect abnormally sized packets in the VVoIP media stream.

SEC-001380 [**Optional: IPS**] At a minimum, the device shall support the capability to detect unusually large packets associated with the codec types specified in Section 2.9, End Instruments.

NOTE: This requires the device to support the capability to recognize the codec that should be represented within the packet and determine the appropriate packet size based on that information.

SEC-001390 [**Optional: IPS**] The device shall support the capability to receive periodic VVoIP signaling, media, and other threat signature updates from an authenticated source in an automated manner.

13.2.4.3 Integrated Security Systems

Integrated Security Systems (ISSs) are systems that provide the functionality of more than one Information Assurance device in one integrated device.

SEC-001400 [**Required: ISS**] The device shall ensure that each function implemented shall be logically separate from the other functions.

SEC-001410 [**Required: ISS**] The device must comply with all applicable UCR requirements for any implemented functions.

13.2.4.4 Information Assurance Tools

Information Assurance tools (IATs) are a category of Information Assurance devices that are not yet fully defined. These devices must meet the Information Assurance requirements for DoD systems as defined in Section 4, Information Assurance. Functional requirements will be added in future versions of this document.

13.2.4.5 Network Access Controllers

Network Access Controller (NAC) systems attempt to control access to a network with policies including pre-admission endpoint security policy checks and post-admission controls over where users and devices can go on a network and what they can do. A system is composed of many elements and is not a single device.

SEC-001420 [**Required: NAC**] The system shall be able to authenticate all devices before allowing access to the network.

SEC-001430 [**Required: NAC**] The system shall be capable of denying access to any device that fails authentication.

SEC-001440 [**Required: NAC**] The system shall support 802.1X-based policy enforcement points and Layer 3 policy enforcement points with 802.1X-based policy enforcement preferred.

SEC-001450 [**Required: NAC**] The system shall operate in both in-band and out-of-band modes to support network segments that both can and cannot utilize 802.1X.

SEC-001460 [**Required: NAC**] The system shall allow an administrator to override the authentication assessment and allow or deny a device to enter the authorized network.

SEC-001470 [**Required: NAC**] The system shall provide the administrator with a means for configuring exception policies to accommodate authorized devices that do not support NAC agents or other means for authentication such as 802.1X.

SEC-001480 [**Required: NAC**] The system shall allow security managers and administrators the ability to create, manipulate, and maintain multiple device NAC policies for different classes of devices.

SEC-001490 [**Required: NAC**] The system shall be capable of being configured for both distributed NAC policy and localized NAC policy enforcement administration.

SEC-001500 [**Required: NAC**] The system shall allow an administrator to manually configure event publication; e.g., set filters on event types to be displayed, alerted.

SEC-001510 [**Required: NAC**] The system shall have the ability to be configured to log, but not enforce, NAC policies. The system shall provide the ability to log and notify, but not enforce, optionally all of the following: compliance OR device authentication OR remediation notifications.

SEC-001520 [**Required: NAC**] The system shall provide the capability to either turn off or disable the NAC functionality globally, and on a NAC-controlled interface basis.

SEC-001530 [**Required: NAC**] The system shall allow administrators to receive information on a device's NAC status.

SEC-001540 [**Required: NAC**] The system shall be capable of placing the end user machine into an alternate network (quarantine) if the end user machine is not authorized to connect to the trusted network, regardless of its enforcement method.

NOTE: The network components [e.g., VPN, Local Area Network (LAN) Server] must be configured so that end devices do not have access to other untrusted devices while quarantined.

SEC-001550 [**Required: NAC**] The system shall allow isolated segments of the network to be designated for clients that meet a specified configuration policy compliance status.

SEC-001560 [**Required: NAC**] For all devices, the system shall support the capability to remove an asset from the group of its managed assets without sympathetic errors (e.g., popup window saying "invalid command"), thus allowing the user to remove managed devices without issue.

SEC-001570 [**Required: NAC**] The system shall require an authentication procedure to process new clients requesting downloads.

SEC-001580 [**Required: NAC**] The system shall support the capability to allow end devices to automatically and securely download required patches or software when the device is found to be non-compliant. Any NAC agent functionality shall support the capability to install downloaded patches manually.

SEC-001590 [**Required: NAC**] The system's remediation checks shall be customizable by security managers and administrators.

SEC-001600 [**Required: NAC**] The system shall not interfere with the operation of DoD-approved antivirus software (e.g., Symantec and McAfee), Host-Based Security System (HBSS), and Federal Desktop Core Configuration (FDCC).

NOTE: Interoperability with HBSS is preferred.

SEC-001610 [**Required: NAC**] The system shall be configurable to fail closed.

SEC-001620 [**Required: NAC**] The system shall provide encrypted communications from the NAC client agent to the NAC device using Federal Information Processing Standards (FIPS)-validated encryption.

SEC-001630 [**Required: NAC**] The system shall protect against subversive network access activity. This may be provided by interfacing with post authentication policy enforcement of third-party devices using widely- accepted technologies such as Trusted Network Control Interface – Metadata Access Point (IF-MAP) Protocol.

SEC-001640 [**Required: NAC**] NAC management devices shall have the capability for manual and, optionally, automatic recovery from failed operations to return to normal settings/ operations/systems, to include log merging.

SEC-001650 [**Required: NAC**] The system shall support the capability to export logs in an open standard format (e.g., Syslog).

SEC-001660 [**Required: NAC**] The system shall provide the capability to queue events when communication is lost.

SEC-001670 [**Required: NAC**] The system shall be capable of reporting alerts to multiple management consoles for all administratively specified events.

SEC-001680 [**Required: NAC**] The system shall provide detailed logs of all administratively specified events.

SEC-001690 [**Required: NAC**] The system shall have the ability to time-stamp all events using Greenwich Mean Time (GMT), to include log data, in a consistent frame of reference.

SEC-001700 [**Required: NAC**] The product shall support a concept of operations which allows individual managers to support large numbers of distributed managed elements.

SEC-001710 [**Required: NAC**] The system shall allow configurable reporting, based on administrator-selected attributes/thresholds, to control how and when reports are generated.

SEC-001720 [**Required: NAC**] The system shall support the capability to identify connecting clients that do not have an 802.1X supplicant or NAC agent/remediation software installed.

SEC-001730 [**Required: NAC**] The system shall support the capability to check for syntax errors and duplicate policies before NAC policies are implemented.

SEC-001740 [**Required: NAC**] The system shall support the capability to integrate with and use Active Directory when authenticating connected devices.

SEC-001750 [**Required: NAC**] The system shall support the capability to periodically perform reauthentication and remediation in automated manner at a configurable interval.

SEC-001760 [**Required: NAC**] NAC systems using 802.1X must be compliant with the relevant and current Institute of Electrical and Electronics Engineers (IEEE) standards for 802.1X.

SEC-001770 [**Required: NAC**] The system shall have the ability to work with any Remote Authentication Dial-In User Server (RADIUS) in 802.1X enforcement mode.

SEC-001780 [**Required: NAC**] The system shall have the ability to support short-term client disconnections, such as taking a laptop to a meeting, and then reconnecting to the network without requiring the client to pass through the testing process.

SECTION 14
ONLINE STORAGE CONTROLLER

14.1 INTRODUCTION

A Data Storage Controller (DSC) is a specialized multiprotocol computer system with an attached disk array that serves in the role of a disk array controller and end node in Base/Post/Camp/Station (B/P/C/S) networks. The DSC is typically a Military Department (MILDEP) asset connected to the Assured Services Local Area Network (ASLAN), but the DSC is not considered part of the ASLAN.

The DSC features and capabilities listed in this section may be offered as part of a unified capability offering associated with other products on the APL. The definitions for DSC are found in Unified Capabilities (UC) Framework 2013, Appendix C, Definitions, Abbreviations and Acronyms, and References.

14.2 STORAGE SYSTEM

DAT-000010 [**Required: DSC**] The system shall provide a Redundant Array of Independent Disks (RAID) for multiple disk drives. The system shall provide a configuration option to select the specific RAID level to be provisioned in the disk array. The RAID levels available for use shall be subject to the specific vendor implementation. At a minimum, the RAID level shall be dual parity RAID-6 for Serial Advanced Technology Attachment (SATA) drives and RAID-5 for Serial Attached Small Computer Systems Interface (SCSI) and Fibre Channel (FC) drives, although stronger RAID levels are acceptable.

DAT-000020 [**Required: DSC**] The system shall be capable of 99.9 percent availability.

DAT-000030 [**Required: DSC**] The system shall provide a management control function for low-level system monitoring and control functions, interface functions, and remote management. The management control function shall provide an Ethernet physical interface(s) for connection to the owner's (i.e., MILDEP) management network/Local Area Network (LAN) and also provide status. The monitoring shall include an initial system check, system cooling fans, temperatures, power supplies, voltages, and system power state tracking and logging.

DAT-000040 [**Required: DSC**] The system shall provide data storage replication (e.g., mirroring) services [Internet protocol (IP) version 4 (IPv4) and version 6 (IPv6)] between systems that are configured as source and destination replication pairs. The replication operations shall provide capabilities for data backup replication, system replication and migration, and system disaster recovery (DR) services in support of continuity of operations (COOP) planning.

DAT-000050 [**Required: DSC**] When the system interfaces to an Integrated Data Protection (IDP) service and the IDP makes copies of data storage information on to another DSC for periodic data storage backup, DR/COOP, migration, and data archiving operation, the system

replication service shall complete the replication regardless of the host connection protocols used between the application servers and the DSC.

DAT-000060 [**Required: DSC**] The system replication and migration services shall provide capabilities to replicate data storage and configuration information onto another standby DSC system for migrating data storage information.

DAT-000070 [**Required: DSC**] The system DR services shall provide capabilities to replicate data storage and configuration information onto another standby DSC system for DR/COOP.

NOTE: This approach provides the threshold capability. Other replication techniques are permitted to ensure communication optimization.

DAT-000080 [**Optional: DSC**] The system shall provide configurable modes for replication (mirroring) operations between the source DSC and the destination DSC. During replication, both the source and the destination must be in a known good state. The configurable modes shall be Asynchronous or Synchronous and are depicted in Table 14.2-1, Replication Operation Modes.

Table 14.2-1. Replication Operation Modes

REPLICATION MODE	DESCRIPTION
Asynchronous (Async)	Incremental, block-based replication between DSCs that occurs as frequently as once per minute by scheduling or manually entering a command to trigger the replication operations.
Synchronous (Sync)	Real-time replication between DSCs that occurs as data is stored or as it changes.

14.3 STORAGE PROTOCOL

DAT-000090 [**Required: DSC**] The system shall provide a Network File System version 3 (NFSv3) server for file systems data input/output (I/O).

DAT-000100 [**Optional: DSC**] The system shall provide a Network File System version 4 (NFSv4) server for file systems data I/O.

DAT-000110 [**Optional: DSC**] The system shall provide a Network File System version 4.1 (NFSv4.1) server, including support for parallel NFS for file systems data I/O.

DAT-000120 [**Required: DCS**] The system shall provide a Common Internet File System version 1.0 (CIFSv1.0) server for file systems data I/O.

DAT-000130 [**Optional: DCS**] The system shall provide a Common Internet File System version 2.0 (CIFSv2.0) server for file systems data I/O.

DAT-000140 [**Optional: DCS**] The system shall provide Internet Small Computer Systems Interface (iSCSI) server (target) operations for data I/O of Logical Units (LUNs) to clients (initiators).

DAT-000150 [**Optional: DCS**] The system shall provide Fibre Channel Protocol (FCP) server (target) operations for data I/O of FCP LUNs to clients (initiators).

DAT-000160 [**Optional: DCS**] The system shall provide Fibre Channel over Ethernet (FCoE) server (target) operations for data I/O of FCP LUNs to clients (initiators).

DAT-000170 [**Optional: DCS**] The system shall provide a HyperText Transfer Protocol Secure (HTTPS) server for file system data I/O and management access to the storage controller operating system. The session shall be secured with Secure Socket Layer (SSL) or Transport Layer Security (TLS), per Internet Engineering Task Force (IETF) Request for Comment (RFC) 5246, and shall comply with Section 4, Information Assurance, for that protocol.

DAT-000180 [**Required: DCS**] The system shall provide Secure Shell version 2 (SSHv2) or SSL for management access to the storage controller operating system. The SSHv2 or SSL implementation shall comply with Section 4, Information Assurance, for that protocol.

DAT-000190 [**Optional: DCS**] The system shall provide Web-based Distributed Authoring and Versioning (WebDAV), per IETF RFC 4918, in support of Cloud-based virtualized storage infrastructures.

DAT-000200 [**Optional: DCS**] The system shall implement the Representational State Transfer (REST) software architecture for distributed hypermedia systems and Cloud-based virtualized storage infrastructures.

DAT-000210 [**Optional: DCS**] The system shall implement the Storage Networking Industry Association (SNIA) Cloud Data Management Interface (CDMI) standard.

DAT-000220 [**Required: DCS**] The system shall provide Global Name Space (GNS) or single name space functionality. The GNS functionality shall provide the capability to aggregate disparate and remote network-based file systems to provide a consolidated view to reduce complexities of localized file management and administration. The GNS functionality shall provide large (i.e., 14 Petabyte [PB] or greater) working pools of disks, transparent data migration, and it shall serve to reduce the number of storage mount points and shares. Each system shall have a dedicated and unique GNS.

NOTE: A GNS functionality is provided with the assumption that it will only be used in deployments where latency is less than 200 ms.

14.4 NETWORK ATTACHED STORAGE INTERFACE

DAT-000230 [**Required: DSC**] The system shall provide physical interfaces for Gigabit Ethernet (GbE) and 10 Gigabit Ethernet (10 GbE) services in conformance with Institute of Electrical and Electronics Engineers (IEEE) 802.3 for Ethernet LAN interfaces.

DAT-000240 [**Required: DSC**] The system shall be able to provision, monitor, and detect faults, and to restore Ethernet services in an automated fashion.

DAT-000250 [**Required: DSC**] The system shall provide physical interfaces for out-of-band management (OOBM) access and services with 10/100 Mbps Ethernet interfaces as a minimum. Services shall include remote access with at least one of the following protocols: SSHv2, SSL, HTTPS, and SNMPv3; and the protocols shall be secured in accordance with Section 4, Information Assurance.

DAT-000260 [**Required: DSC**] When the system uses Ethernet, Fast Ethernet, Gigabit Ethernet (GbE), and 10GbE interfaces, the interfaces shall be autosensing, autodetecting, and autoconfiguring with incoming and corresponding Ethernet link negotiation signals.

DAT-000270 [**Required: DSC**] Ethernet services of the system and the Logical Link Interworking Function (IWF) of the system shall terminate the Media Access Control (MAC) layer of Ethernet as described in Ethernet Standard IEEE 802.3.

DAT-000280 [**Required: DSC**] Ethernet services of the system shall support jumbo frames with a configurable Maximum Transmission Unit (MTU) of 9000 bytes or greater, excluding Ethernet encapsulation. When Ethernet encapsulation is included in the frame size calculation, an additional 22 bytes must be included for the MAC header (14 bytes), the Virtual LAN (VLAN) tag (4 bytes), and the Cyclical Redundancy Check (CRC) Checksum (4 bytes) fields in the Ethernet frame, resulting in a maximum of 9022 bytes or greater. The system shall also support a configurable MTU between 1280 bytes and 1540 bytes to ensure packets can transit type 1 encryptors. The system default MTU shall be 1540 bytes.

DAT-000290 [**Required: DSC**] Ethernet services of the system shall allocate a unique Ethernet MAC address to each Ethernet interface associated with a VLAN, as per IEEE 802.1Q.

DAT-000300 [**Required: DSC**] Ethernet services of the system shall support "Link Aggregation," as per IEEE 802.3ad or IEEE 802.1AX-2008, and use with the Link Aggregation Control Protocol.

DAT-000310 [**Optional: DSC**] Ethernet services of the system shall provide Link Layer Discovery Protocol (LLDP), as per IEEE 802.1AB.

14.5 STORAGE ARRAY NETWORK INTERFACE

DAT-000320 [**Optional: DSC**] The system shall provide Fibre Channel (FC) physical interfaces and FCP interfaces and services as per American National Standards Institute (ANSI) X3.230, X3.297, and X3.303.

14.6 CONVERGED NETWORK ADAPTER INTERFACE

DAT-000330 [**Optional: DSC**] The system shall provide physical interfaces for FCoE services over a 10GbE physical interface in conformance with the ANSI T11 FC-BB-5 standard for FCoE with a Converged Network Adapter (CNA).

DAT-000340 [**Optional: DSC**] The system shall provide physical interfaces for Data Center Bridging [DCB, also known as Converged Enhanced Ethernet (CEE)] features, and functionality, per the standards depicted in Table 14.6-1, Physical Interfaces for Data Center Bridging.

Table 14.6-1. Physical Interfaces for Data Center Bridging

DCB STANDARD	DESCRIPTION
IEEE 802.1Qbb for Priority-Based Flow Control (PFC)	Per-Priority PAUSE adds fields to the standard PAUSE frame that allows a device to inhibit transmission of frames on certain priorities as opposed to inhibiting all frame transmissions.
IEEE 802.1Qaz for Enhanced Transmission Selection (ETS)	Enhanced Transmission Selection provides a means for network administrators to allocate link bandwidth to different priorities on the basis of a percentage of total link bandwidth.
IEEE 802.1Qaz Data Center Bridging Exchange Protocol (DCBX)	DCB Exchange is the mechanism in which peers can exchange capabilities to one another with LLDP.
IEEE 802.1Qau for Congestion Notification	Congestion Notification is a mechanism to transmit congestion information on an end-to-end basis per traffic flow.
LEGEND	
DCB: Data Center Bridging	LLDP: Link Layer Discovery Protocol
DCBX: Data Center Bridging Exchange	PFC: Priority-Based Flow Control
ETS: Enhanced Transmission Selection	

14.7 IP NETWORKING

DAT-000350 [**Required: DSC**] The system shall meet the IPv6 requirements defined in Section 5.2.2, Mapping of RFCs to UC Profile Categories, for a simple server/network appliance.

DAT-000360 [**Required: DSC**] The system shall provide statically provisioned or dynamically adjusted large IP packet receive buffers for replication (mirroring) session traffic received on the Ethernet physical interfaces. The receive buffers may be statically provisioned or the operating system of the system may dynamically self-adjust the packet receive buffer size based on

measurements of the E2E path bandwidth, Maximum Segment Size (MSS), Round Trip Time (RTT), and the percentage of packet loss. The system shall provide a default and minimum IP packet receive buffer size of 2048 KB per replication (mirroring) session. The system shall provide a statically provisioned or dynamically adjusting maximum IP packet receive buffer size of up to 8192 KB per replication (mirroring) session.

These IP packet receive buffer size requirements are conceptually based on either the Satellite or Transoceanic and Terrestrial Fiber Optic Cable E2E IP transport path models as depicted in Table 14.7-1, IP End-to-End Transport Path Models.

Table 14.7-1. IP End-to-End Transport Path Models

PATH MODEL	DESCRIPTION
Transoceanic and Terrestrial Fiber Optic Cable	Where an end-to-end terrestrial OC-3 path with 155 Mbps of bandwidth that has an RTT of approximately 250 µs with packet loss of 0.01 percent or less. These characteristics are typical of a transoceanic and terrestrial fiber optic cable path between a pair of cities, such as London and Tokyo. The 2,048 KB buffer size is suitable for these path characteristics.
Satellite	Where an end-to-end satellite DS1 path with 1.544 Mbps of bandwidth that has an RTT of approximately 600 µs with packet loss of 1.0 percent or greater. These characteristics are typical of a satellite path between two locations within the same VSAT footprint. The 8,192 KB buffer size is suitable for these path characteristics.
LEGEND	
DS1: Digital Signal Level 1	µs: Microsecond KB: Kilobyte Mbps: Megabits per Second OC-3: Optical Carrier 3 RTT: Round Trip Time VSAT: Very Small Aperture Terminal

DAT-000370 [**Required: DSC**] The system shall provide an optimized congestion control (congestion avoidance) algorithm in Transmission Control Protocol (TCP) for avoidance of traffic loss on communications paths in high-speed networks with high latency or large bandwidth-delay products.

NOTE: Two examples of these algorithms currently implemented in modern operating systems are CUBIC TCP in Linux® 2.6.19 and later, and Compound TCP (CTCP) in various Microsoft® operating system products.

14.8 NAME SERVICES

DAT-000380 [**Required: DSC**] The system shall provide Lightweight Directory Access Protocol (LDAP) directory services per IETF RFC 4510.

DAT-000390 [**Required: DSC**] The system shall provide Kerberos authentication service per IETF RFC 4120.

DAT-000400 [**Required: DSC**] The system shall provide Domain Name System (DNS) client functionality.

DAT-000410 [**Required: DSC**] The system shall provide DNS client-side Load Balancing.

DAT-000420 [**Required: DSC**] The system shall provide Network Information Service (NIS) client directory service functionality.

DAT-000430 [**Required: DSC**] The system shall provide NIS Netgroups client directory service functionality.

DAT-000440 [**Optional: DSC**] The system shall provide Network Basic Input/Output System (NETBIOS) over TCP/IP (NBT) Name Resolution and Windows Internet Name Service (WINS).

DAT-000450 [**Required: DSC**] The system shall provide Internet Storage Name Service (iSNS) client functionality per IETF RFC 4171.

DAT-000460 [**Conditional: DSC**] If the system has a Fiber Channel (FC) interface then the system shall provide FC Name and Zone Service.

14.9 SECURITY SERVICES

DAT-000470 [**Optional: DSC**] The system shall provide IPSec per RFC 4301.

DAT-000480 [**Optional: DSC**] The system shall provide Encapsulating Security Payload (ESP) per RFC 4303.

DAT-000490 [**Optional: DSC**] The system shall provide Internet Key Exchange version 2 (IKEv2) per RFC 4306.

DAT-000500 [**Optional: DSC**] The system shall provide a configurable Packet Filter (Firewall) service to block unauthorized access (for intrusion prevention) while permitting authorized communications. The Packet Filter service shall use a "stateless" design that does not degrade performance and shall filter all packets received based on interface, source IP address, protocol, port, Type of Service (TOS), or Time To Live (TTL). The Packet Filter service shall provide a configuration policy for defining combinations of multiple packet match rules and processing actions.

DAT-000510 [**Required: DSC**] The system shall provide encryption of data at rest at a minimum of AES-256 in accordance with Federal Information Processing Standard (FIPS) 140-2 level 1 or higher to provide the following capabilities:

a. Rapid crypto-shredding (destruction) of data, in accordance with National Institute of Standards and Technology (NIST) 800-88, for tactical systems that operate in harm's way and may fall into enemy hands.

b. Rapid recovery from sensitive data spills, where the wrong data is accidentally written to the wrong place.

DAT-000520 [**Required: DSC**] The system shall comply with all appropriate STIGs to include the Database Security Technical Implementation Guide.

14.10 INTEROPERABILITY

DAT-000530 [**Required: DSC**] The system shall provide an Application Programming Interface (API) to enable interaction with other software and systems. The interactions shall include routines, data structures, object classes, and protocols used to communicate between the consumer and implementer of the API. The API protocol and message format (e.g., Extensible Markup Language [XML]) shall be subject to the specific vendor system operating system implementation.

14.11 CLASS OF SERVICE AND QUALITY OF SERVICE

DAT-000540 [**Optoional: DSC**] The system shall provide Class of Service (CoS) and Quality of Service (QoS) marking on egress traffic at layer 2 per IEEE 802.1p and, Section 7.2.1.3, Class of Service Markings, and Section 7.2.1.4, Virtual LAN Capabilities. Traffic classification and marking must occur before the egress transmission of the Ethernet frame with a rule or policy engine that matches on various storage and management protocol types as offered by the system.

NOTE: Examples of Storage Protocols and Management Protocols are listed in Table 14.11-1, Example Storage and Management Protocols.

Table 14.11-1. Example Storage and Management Protocols

STORAGE PROTOCOLS			
NFSv3	NFSv4	NFSv4.1	CIFSv1.0
CIFSv2.0	iSCSI	FCOE	
MANAGEMENT PROTOCOLS			
SSHv2	HTTP/HTTPS/REST	SFTP	SNMP
FTPS	User-defined protocols (e.g., proprietary system to system mirroring protocols		

The marking is made in Ethernet VLAN tags by setting the priority value to between zero and seven, inclusive for various traffic classes. These are to be used in the ASLAN, non-ASLAN, and extended networks for per-hop CoS and QoS traffic conditioning by the network elements.

DAT-000550 [**Required: DSC**] The system shall provide CoS and QoS marking on egress traffic at layer 3 per Section 6, Network Infrastructure End-to-End Performance. Traffic classification and marking must occur before the egress transmission of the IP packet with a rule or policy engine that matches on various storage and management protocols that occur within the system, such as those listed in Table 14.11-1.

NOTE: The IP packets are marked in the TOS field of the IPv6 packet header with Differentiated Services Code Point (DSCP) values from 0 and 63, inclusive. These are to be used in the ASLAN, non-ASLAN, and extended networks for per-hop CoS and QoS traffic conditioning by the network elements.

14.12 VIRTUALIZATION

DAT-000560 [**Optional: DSC**] The system shall provide virtualized Data Storage Controller (vDSC) functionality and individual protocol server processes. The vDSC shall meet all the requirements of a DSC with minor exceptions that are related to design and technical limitations associated with the complete virtualization of an operating system, which include internal counters for attributes of the physical system, QoS traffic processing, and per vDSC Mobile IP correspondent node binding cache limitations.

NOTE: Within the DSC system, a vendor may integrate a third party component(s) that enables virtualization of heterogeneous file servers and provides a GNS capability.

DAT-000570 [**Optional: DSC**] The vDSC capability within the system shall provide secure, Private Networking Domains (PNDs) for Ethernet, VLANs, and IP that isolate the network domains of system units. The PND shall support the use of duplicate IP addresses and IP subnet address ranges among those of any other configured vDSC in the system. The PND shall provide a dedicated IP Forwarding Information Base (FIB) per vDSC.

DAT-000580 [**Optional: DSC**] The vDSC shall provide an individual Command Line Interface (CLI) context with the full command set of the system, with the scope of the commands limited to the individual vDSC CLI context.

DAT-000590 [**Optional: DSC**] The vDSC shall provide a programmatic API with the full command set of the system with the scope of the API commands limited to the individual vDSC context.

DAT-000600 [**Optional: DSC**] The vDSC capability within the system shall provide an individual GNS unique from the system or shall provide a single name space that provides the capability to aggregate disparate hardware and storage architectures into a single file system. The GNS shall provide the capability to aggregate disparate and remote network-based file systems, providing a consolidated view to reduce complexities of localized file management and administration. The GNS shall provide large working pools of disks and transparent data migration, and shall serve to reduce the number of storage mount points and shares. The single name space shall be spread across multiple physical Network Access Server (NAS) heads all representing the same file system without replication. The single name space shall include the ability to tier data automatically within the same file system.

SECTION 15
ENTERPRISE AND NETWORK MANAGEMENT SYSTEMS

15.1 INTRODUCTION

This section identifies basic requirements for enterprise and network management systems. This section does not specify requirements for how an enterprise or network management system shall display performance data on a user interface, nor the data elements a management system must collect from a Unified Capabilities (UC) product. The individual Unified Capabilities Requirements (UCR) sections describe requirements as to what data elements (e.g., alarms, performance, and status) a UC product is required to send to a network management system for performance and status monitoring.

15.2 MINIMUM

Enterprise and network management systems must do the following:

EMS-000010 [**Required**] Meet all Information Assurance and Security Technical Implementation Guideline (STIG) requirements.

EMS-000020 [**Required**] Must interoperate with UC products' commercial off-the-shelf (COTS) Network Management (NM) interface/system for monitoring and commanding the UC product.

EMS-000030 [**Required**] Leverage COTS interface of UC products to be managed in a secure manner.

EMS-000040 [**Required**] Must be capable of exchanging data with other network management systems for information sharing purposes.

15.2.1 Connectivity to Monitored Network Elements

The management system must have the capability to establish the following protocols for communication with a UC product:

EMS-000050 [**Required**] Receiving Simple Network Management Protocol (SNMP) version 3 (SNMPv3) traps from a monitored product.

EMS-000060 [**Required**] Sending SNMP [Management Information Base (MIB)] poll requests to a monitored product.

EMS-000070 [**Required**] Collecting and mediating Call Detail Records (CDRs) and Internet protocol (IP) Detail Records (IPDRs) from a monitored product in a secure manner.

EMS-000080 [**Required**] Securing the connection using Transport Layer Security (TLS).

15.2.2 Segregation of Network Management Data Into Categories

The Element Message System (EMS) must be capable of receiving and analyzing the following NM data categories:

EMS-000090 [**Required**] System Events.

EMS-000100 [**Required**] Security Events.

EMS-000110 [**Required**] Performance Events (5-minute polls).

EMS-000120 [**Required**] Performance (15-minute polls).

EMS-000130 [**Required**] CDRs.

APPENDIX A
UNIQUE DEPLOYED (TACTICAL)

A.1 INTRODUCTION

This appendix identifies and develops Tactical interoperability requirements as certification criteria for joint networked-communications systems. In pursuing acquisition initiatives, Combatant Commands (COCOMs), military services, and defense agencies shall use this appendix as a guideline for the purchase of commercial off-the-shelf (COTS) equipment as well as for the development of systems that need to interoperate in tactical network environments. The Tactical networked communications community of the Department of Defense (DoD) shall adhere to this appendix in compliance with DoD Instruction (DoDI) 8100.04.

This appendix defines unique Deployed (Tactical) requirements for Deployed products and systems. Detailed information and guidance on Requirements Categories, Language, specific terminology, principles, and procedures are provided in the Unified Capabilities (UC) Framework 2013 document.

A.1.1 Purpose

This appendix defines the unique requirements for Deployed products and systems. These are requirements that are not contained in other sections of the Unified Capabilities Requirements (UCR), and define requirements that are modified to support unique tactical users.

This appendix 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 appendix provides guidance for satisfying the certification requirements for Deployed voice systems used as part of an Operational Area Network (OAN), which is the deployed extension of the GIG. This appendix also defines other UCR elements applicable to the Deployed community, and serves as a ready reference to be used by the Joint Interoperability Test Command (JITC) when writing the Deployed annex to the UC Test Plan (UTP).

A.1.2 Applicability

The requirements described in this appendix apply to Network Elements (NEs), Local Area Networks (LANs) when used in Deployed (Tactical) environments, Deployed Cellular Voice Exchange (DCVX) Systems, and Session Controllers (SCs).

A.1.3 Definitions

Definitions and acronyms are provided in UC Framework 2013, Appendix C, Definitions, Abbreviations and Acronyms, and References.

A.2 CIRCUIT-SWITCHED-BASED DEPLOYABLE NETWORK DESIGNS AND COMPONENTS

Circuit-switched-based deployable requirements defined by previous editions of the UCR remain in effect during the remaining lifecycle of deployed circuit-switched products.

A.3 DEPLOYED VOICE QUALITY

The desired objective for Deployed 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. UC Framework Appendix A contains additional information on Deployed Voice Quality.

A.4 DEPLOYED NE GENERAL

Section 11, Network Elements, contains the Deployed NE general requirements.

A.5 DCVX SYSTEM

A.5.1 Introduction and Purpose

The following sections describe the requirements that shall be met by all deployed DCVX systems to be certified and used in the OAN tier of the 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 (MUFs), and, therefore, is not the same as commercially deployed cellular systems.

It is recognized that not all components are needed for a specific application. The requirements discussed in this appendix are similar to those for a Deployed Voice Exchange-Commercial (DVX-C) and/or SC, and are dependent on the network configuration as well as the specific authorized gateway connection.

A.5.2 Applicability

The requirements within this appendix are applicable to the following:

- All DCVX systems that connect directly or indirectly to the Defense Information Systems Network (DISN) voice systems, including the UC Services Network, Defense Switched Network (DSN), Defense RED Switch Network (DRSN) Secure Phone Gateways, and/or commercial Public Switched Telephone Network (PSTN).

- Procured or leased commercial cellular systems that connect to any DISN service gateway. Commercial cellular services are not currently allowed to be directly connected to DISN service gateways unless the connection is Time Division Multiplexing (TDM) based (e.g., Analog, Primary Rate Interface [PRI], or Integrated Services Digital Network [ISDN]), excluding the use of Signaling System No. 7 (SS7). Future commercial cellular services' Internet protocol (IP)-based connections will be allowed once the Information Assurance policy and Security Technical Implementation Guidelines (STIGs) are established. In both instances, the DISN service gateway may or may not be protected by a separate or built-in encrypted gateway on the commercial cellular services connection. Encrypted gateway requirements are excluded from the DCVX section.
- Procured or leased cellular systems using leased commercial cellular frequencies that connect to any DISN service gateway.

Terminal devices procured and/or leased, whose primary carrier service is owned and operated solely by a commercial carrier service (e.g., Verizon, Sprint) are not considered elements of a DCVX and are exempt from this appendix. The current version of the UCR 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 the UCR take precedence over the explicit or implicit requirements of any other requirements document except for those requirements specified in the documents listed in Section A.5.3, Policy and Reference Documents.

A.5.3 Policy and Reference Documents

The following policy and instruction documents, in conjunction with the current version of the UCR, will be used as the basis for Approved Products List (APL) certification:

1. Policy for the use of commercial wireless devices, services, and technologies in the DoD GIG, as outlined in DoD Directive (DoDD) 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)" or current edition.
3. "Wireless Priority Service (WPS) Industry Requirements for the Full Operating Capability (FOC) for GSM-Based Systems" or current edition.
4. 3G TS 24.067 V3.0.0 (1999-05), 3rd Generation Partnership Project; Technical Specification Group Core Network; enhanced Multilevel Precedence and Preemption (MLPP) (eMLPP) – Stage 3 or current edition.

A.5.4 DCVX General

A.5.4.1 Coverage and Signaling Strength

TAC-000010 [**Required**] The signal strength shall not be less than the current Global System for Mobile (GSM) [Second Generation (2G), Third Generation (3G), Pre-Fourth Generation (4G)], Code Division Multiple Access (CDMA), Mobile Worldwide Interoperability for Microwave Access (WiMAX), and 4G authorized international standards and specifications. The GSM (2G, 3G, Pre-4G), CDMA, Mobile WiMAX, and 4G technology are spectrum based; therefore, GSM (2G, 3G, Pre-4G), CDMA, Mobile WiMAX, and 4G band, coverage, signal strength, and power are the basis for a planned "area of support." Environment, weather, geography, topography, and adjacent spectrums are elements that must be considered when applying the basis for an area of support. For testing purposes, the generic set of parameters presented in Table A.5-1, Current Cellular Systems Parameters, shall be used for JITC certification either by testing and/or as determined by JITC.

Table A.5-1. Current Cellular Systems Parameters

DCVX GSM/GPRS (2G, 3G, PRE-4G)	
Bands	As provided by standards and/or DoD GSM Cellular Band (e.g., 450 MHz, 850MHz, 900MHz, and 1900 MHz)
Specification on Coverage	As provided by standards (e.g., ITU-R 2G. 2.5G, 3G, 3GSM, UMTS, 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 CDMA	
Bands	As provided by standards (e.g., 450 MHz, 700 MHz, 800 MHz, 850 MHz, 900 MHz, 1700 MHz, 1800 MHz, 1900 MHz, and 2100 MHz)
Specification on coverage	As provided by standards (e.g., TIA, IS-95, 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.
DCVX (4G IMT-ADVANCED)	
Bands	As provided by standards (e.g., GSM: 700 MHz, 850 MHz, 900 MHz, 1700 MHz, 1800 MHz, 1900 MHz, 2100 MHz and 2600 MHz, Mobile WiMAX: 500 MHz to 3.5 GHz)
Specification on Coverage	As provided by standards (e.g., GSM: 4G-Advanced, Mobile WiMAX, 802.16m, Pre-4G: 802.16-2009)
DCVX (4G IMT-ADVANCED)	
Distance Transmit/ Receive	Up to 25 and 30 miles for 4G-Advanced and WiMAX respectively depending on topology/manmade structures and frequencies also determine coverage parameters

TERMINAL DEVICE	
Bands	As provided by standards (CDMA/GSM/4G-Advanced) and/or DoD GSM Cellular (e.g., 450 MHz, 700 MHz, 800 MHz, 850 MHz, 900 MHz, 1700 MHz, 1800 MHz, 1900 MHz, 2100 MHz, and 2600 MHz, Mobile WiMAX, 500 MHz to 3.5 GHz)
CDMA Specification	As provided by standards (e.g., CDMA (IS95), CDMA2000, 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)
4G Specifications	As provided by standards (e.g., GSM: 4G-Advanced; Mobile WiMAX; 802.16m, Pre-4G: 802.16-2009)
Distance Transmit/ Receive	Up to 8 miles depending on topology/manmade structures and frequencies also determine coverage parameters.

LEGEND

1xEVDO: One Times EVDO	CDMA2000: Code Division Multiple Access 2000	IS-95: Interim Standard 95
1XRTT: One Times Radio Transmission Technology	DCVX: Deployed Cellular Voice Exchange	ITU-R: International Telecommunications Union – Radiocommunication Sector
3G: Third Generation	DMSC: Deployed Mobile Switching Center	MHz: Megahertz
3GPP2: Third Generation Partnership Project 2	DoD: Department of Defense	TIA: Telecommunications Industry Association
3GSM: Third Global System for Mobile	EVDO: Evolution-Data Optimized	WCDMA: Wideband CDMA
4G: Fourth Generation	GPRS: General Packet Radio Service	WiMAX: Worldwide Interoperability for Microwave Access
BSS: Base Station Subsystem	GSM: Global System for Mobile	
CDMA: Code Division Multiple Access	IMT-2000: International Mobile Telecommunications 2000	

A.5.4.2 Protocol/Format

TAC-000020 [**Required**] The DCVX shall support at least one or more of the following protocols:

a. GSM/General Packet Radio Service (GPRS) GPRS [2G, 2.5G, Third Generation (3G), Third Global System for Mobile (3GSM), GSM Edge].

b. Wideband CDMA (WCDMA).

c. CDMA2000.

d. CDMA One Times Radio Transmission Technology (1XRTT).

e. Universal Mobile Telecommunications System (UMTS).

f. Evolution-Data Optimized (EVDO) (or EV-DO).

g. Mobile WiMAX (802.16-2009).

h. Fourth Generation IMT-Advanced.

i. 4G-Advanced.

j. Mobile WiMAX Series (802.16m and beyond).

A.5.4.3 MOS and Measuring Methodology

TAC-000030 [**Required**] The DCVX shall support the minimum MOS scores as defined in Section 6, Network Infrastructure End-to-End Performance, or better as measured in any 5-minute interval using International Telecommunications Union – Telecommunication (ITU-T) Recommendation P.862 testing standard. The baseline test environment shall be operated in an open air, clear of obstruction, line-of-sight environment, with the specific requirements as outlined in Table A.5-1. Based on the results, the estimated MOS performance range will be extrapolated and provided in the vendor Letter of Compliance (LOC) based on the Access Network operating at or near full power mode and, at a minimum, operating at a height of 80 feet. The values provided in the vendor LOC will be included in the APL report.

A.5.4.4 Availability

TAC-000040 [**Required**] The DCVX shall have an availability of 99.97 percent, which includes scheduled maintenance.

A.5.4.5 Encryption

TAC-000050 [**Conditional**] Depending upon which of the following encryption types a terminal device provides to support secure calls: Secure Communications Interoperability Protocol (SCIP), other National Security Agency (NSA)-accredited encryption scheme(s), and/or other required accredited encryption schemes as defined in appropriate cellular STIGs, the DCVX must provide appropriate radio and network transport bandwidth to support the terminal device encryption requirements contained in Section A.5.5.4, Terminal Device Encryption.

TAC-000060 [**Conditional**] If a secure call capability is provided in the terminal device(s), then the DCVX shall support SCIP, other NSA-accredited encryption scheme(s), and/or required accredited encryption schemes as defined in the appropriate cellular STIGs. The DCVX that supports SCIP (also known as terminal device) will be required to go secure E2E with another SCIP Phone and/or via a SCIP Gateway if the Assured Services (AS) Session Initiation Protocol (SIP) (AS-SIP) is used while the DCVX supports the establishment and maintenance of the secure call.

TAC-000070 [**Optional**] The DCVX may have the capability to provide secure SCIP Gateway functions.

A.5.4.6 Calling Features

A.5.4.6.1 Call Waiting Feature Requirement

The Call Waiting (CW) feature interacts with MLPP and Assured Service for TDM and IP, respectively. If a precedence and preemption capability is available in the DCVX, then the preemption interactions must meet the requirements described in Section A.5.4.10.1, Precedence Call Waiting. Call Waiting is a feature where a line in the talking state is alerted by a CW tone when another call is attempting to complete to that line. A CW tone is only audible to the line with the CW feature activated.

TAC-000080 [**Required**] The CW feature shall generate a CW tone only audible to the line with the CW feature activated.

TAC-000090 [**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.

A.5.4.6.2 Three-Way Calling Requirement

The Three-Way Calling (TWC) feature interacts with MLPP and Assured Service for TDM and IP, respectively. If a precedence and preemption capability is provided in the DCVX, then the MLPP interactions must meet the requirements described in Section A.5.4.10.2, Precedence Three-Way Calling (TWC).

TAC-000100 [**Optional**] The TWC feature 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 first line off hold to establish the TWC connection. This may occur at 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, then the TWC is returned to a two-party connection between the remaining parties.

TAC-000110 [**Optional**] The terminal device may support signaling to allow TWC.

A.5.4.6.3 Conference Calling

The Conference Calling feature is Conditional because it interacts with MLPP and Assured Service for TDM and IP, respectively. If precedence and preemption and conference calling capabilities are provided in the DCVX, then the preemption interactions must meet the requirements described in Section A.5.4.10.3, Precedence Conference Calling.

TAC-000120 [**Optional**] The Conference Calling 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.

TAC-000130 [**Optional**] The terminal device may support signaling to allow conference calling.

A.5.4.7 Roaming

TAC-000140 [**Optional**] The DCVX system may only support roaming to one or more DCVXs. The DCVX roaming numbering capability shall support the following:

a. Tactical Global Block Numbering Plan (GBNP).

b. Tactical Routing and Numbering: The DCVX shall be equipped and operationally capable of the dialing format for User Dialing Format to Coalition Forces as defined in North Atlantic Treaty Organization (NATO) Standardization Agreement (STANAG) 4214, "International Rating and Directory for Tactical Communications Systems," Edition 3, Version T, 7 January 2005, or current edition.

Direct network connections from the DCVX to commercial cellular provider systems in support of terminal device roaming on the commercial cellular provider network(s) are not allowed.

A.5.4.8 Precedence and Preemption

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

TAC-000150 [**Optional**] The DCVX may support the cellular version of precedence and preemption, called eMLPP, and/or a proprietary methodology. When precedence and preemption are available, the interface to the DSN/UC Networks and/or the supporting DVX-C shall support one or more of the interfaces.

TAC-000160 [**Conditional**] The DCVX will support a preemption and precedence capability under one or more of the following conditions:

a. The DCVX supports GSM in the DoD GSM cellular band.

b. The DCVX supports the use of leased cellular frequency in one of the bands and protocol(s) listed in Table A.5-1, Current Cellular Systems Parameters.

c. The DCVX supports one or more of the cellular bands and protocol(s), as described in Table A.5-1, Current Cellular Systems Parameters, in an environment that is outside the

continental United States (OCONUS), where the local Forces-Status Agreement allows eMLPP/proprietary version operation.

d. The DCVX supports one or more of the cellular bands and protocol(s), as described in Table A.5-1, Current Cellular Systems Parameters, dependent on the operational environment and usage of cellular frequencies allowed by local and/or U.S. National Civilian Authorities.

A.5.4.9 Precedence Capability Terminal Device Activation/Deactivation

TAC-000170 [**Conditional**] If a precedence and preemption capability is provided in the DCVX, then the DCVX may be capable of providing on any supported terminal device the user's Precedence Class Table Assigned features. These features are provided to the terminal device based on the user entering a specified personal identification number (PIN) on the same terminal device. The DCVX will assign to the terminal device the entire user's precedence capability as defined in the DCVX's class features table(s). This will allow the user to make precedence calls from 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 reentering the same or different PIN on the terminal device. The precedence capability user's activation or deactivation PIN may be stored in the DCVX or in another database accessible by the DCVX to validate the user's PIN(s) associated with the user's precedence capability. The user's precedence activation or deactivation PIN may be assigned and/or user settable after an initial assigned PIN has been provided.

A.5.4.10 Precedence and Preemption Calling Features

TAC-000180 [**Conditional**] If a precedence and preemption capability is provided in the DCVX, then the following applies under the following calling features:

a. If no active call is in progress, then the terminal device will receive precedence notification per Section 2, Table 2.9-1, UC Ringing Tones and Cadences.

b. If a ROUTINE or lower precedence call is in progress to the terminal device, and a calling party calls at a higher precedence level, then the current call will be preempted.

   If a precedence call has been connected to the terminal device and is in progress, then the calling party of equal or lower precedence will receive a notification that the lower precedence call was rejected. The following provides the precedence interactions for calls in progress to terminal devices.

A.5.4.10.1 Precedence Call Waiting

TAC-000190 [**Conditional**] The following Precedence CW treatments shall apply to precedence levels of PRIORITY and above if the precedence and preemption capability is provided in the DCVX.

A.5.4.10.1.1 Busy With Higher Precedence Call

TAC-000200 [**Required**] If the precedence level of the incoming call is lower than the existing precedence call, then precedence CW shall be invoked. In an active call, if the incoming call is PRIORITY precedence or above, the precedence CW tone shall be applied to the called party per AS-SIP 2013, Section 6, Table 6.1-4, UC Information Signals.

A.5.4.10.1.2 Busy With Equal Precedence Call

TAC-000210 [**Required**] The DCVX shall provide the precedence CW signal to the called station per AS-SIP 2013, Section 6, Table 6.1-4, UC Information Signals. 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.

A.5.4.10.1.3 Busy With Lower Precedence Call

TAC-000220 [**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 3 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 ring per Section 2, Table 2.9-1, UC Ringing Tones and Cadences, or comparable vibration cadence. The station shall be connected to the preempting call after going off-hook.

A.5.4.10.1.4 No Answer

TAC-000230 [**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 IAW Section 2.2.10, Precedence Call Diversion.

A.5.4.10.2 Precedence Three-Way Calling (TWC)

TAC-000240 [**Conditional**] If precedence and preemption and TWC are provided in the DCVX, then the following TWC requirements apply:

> **TAC-000240.a** [**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.
>
> **TAC-000240.b** [**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 the TWC that have a higher precedence than the higher of the two segments shall preempt unless the call is marked non-preemptable.

TAC-000240.c [**Required**] When a higher precedence call is placed to any one of the TWC participants, that participant receives the preemption tone per AS-SIP 2013, Section 6, Table 6.1-4, UC Information Signals. 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.

TAC-000240.d [**Required**] In a TWC call where each connection is established at a different precedence level, the precedence level of the participant who initiated the TWC call shall be assigned the highest precedence of the two connections.

A.5.4.10.3 Precedence Conference Calling

TAC-000250 [**Conditional**] If precedence and preemption and conference calling are provided in the DCVX, then the following precedence conference calling requirement is required:

TAC-000250.a [**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, then ROUTINE precedence conference call attempts shall be connected to a "line busy" tone, and call attempts at precedence levels above the ROUTINE precedence shall re-examine all conference bridges on a preemptive basis.

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

(3) When a conference bridge is preempted, a 2-second burst of preemption tone per AS-SIP 2013, Section 6, Table 6.1-4, UC Information Signals, 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) per Section 2.9.1.2.2, Announcements.

A.5.4.10.4 Voice Mail

The Voice Mail feature interacts with precedence and preemption. If precedence and preemption capability and voice mail are provided in the DCVX or voice mail added externally, then the precedence and preemption interactions must meet the requirements described in Section 2.25.2.3, Precedence Call Diversion.

TAC-000260 [**Optional**] The DCVX may provide ROUTINE calls only voice mail capability for users. Additional features, such as message forwarding, may be provided in addition to a

basic voice mail capability provided they do not interfere with precedence and preemption if the capability is provided in the switch.

A.5.4.10.4.1 Precedence and Preemption Interaction With Voice Mail

TAC-000270 [**Conditional**] If precedence and preemption are provided in the DCVX and voice mail capability is provided internally to the DCVX or connected externally to the DCVX as an adjunct, then the following requirement applies:

> **TAC-000270.a** [**Required**] The DCVX shall divert all precedence calls above ROUTINE that are destined for voice mail IAW Section 2.25.2.3, Precedence Call Diversion.

A.5.4.11 Management Capabilities for Terminal Devices

TAC-000280 [**Required**] The DCVX shall have the capability to manage its supported terminal devices as published in its users' database [e.g., HLR or Mobility Management Entity (MME)] so it can assign, transfer, or terminate services, features, and calling capability to include telephone numbers for its terminal devices.

A.5.4.12 Security

TAC-000290 [**Required**] All components of the DCVX shall meet security requirements as outlined in DoDI 8510.01 and the applicable STIG(s).

A.5.5 Terminal Device-Specific

Cellular handsets, often referred to as mobile subscribers, handsets, PDAs, Smartphones, BlackBerrys, and any other end user cellular 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 handheld unit, a mounted mobile device, or a fixed location device.

A.5.5.1 Terminal Device

TAC-000300 [**Required**] The terminal device shall provide the following status information to the network:

a. Powered on.

b. Moved to a new location.

c. Alerting.

d. Dialing.

TAC-000310 [**Required**] The terminal device shall display the following status information to the end user:

a. Signal strength.

b. Battery capacity.

c. Roaming status.

d. Service not available.

e. Call progress status.

TAC-000320 [**Required**] If no STIG exists for the terminal device, then the terminal device shall have the ability to provide key-locking ability to lock the terminal device's keypad and unlock the keypad after providing the appropriate key sequence or PIN entries as provided by the vendor in the terminal device. The lock and unlock key sequence or PIN shall be set by the user. If the user PIN is unavailable or not supplied, then an administrator method, which can be vendor proprietary, shall unlock the terminal device.

TAC-000330 [**Optional**] 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.

TAC-000340 [**Conditional**] Removable and Exchangeable Subscriber Identity Module (SIM): If a SIM card is utilized, then the SIM card in commercially available terminal devices shall be removable and exchangeable into other similar commercially available terminal devices that are compatible with the DCVX system (applicable to a GSM-based system). This excludes secure terminal devices and other terminal devices not readily commercially available.

A.5.5.2 Terminal Device Signaling

TAC-000350 [**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 in active call status.

A.5.5.3 Terminal Device Frequency Band Support

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

TAC-000360 [**Optional**] A terminal device may support multiple (e.g., five) frequency bands as specified in Table A.5-1, Current Cellular Systems Parameters, for each protocol supported in Section A.5.4.2, Protocol/Format.

TAC-000370 [**Optional**] 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.

A.5.5.4 Terminal Device Encryption

TAC-000380 [**Conditional**] If SCIP and/or other NSA-accredited encryption are implemented in the terminal device, then 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-capable terminal device, and via the DCVX, to a non-cellular NSA encryption-capable device per the requirements specified in Section 3.8, DoD Secure Communications Devices (DSCD). The SCIP and/or other NSA-accredited encryption device shall provide E2E encryption within the DCVX, from DCVX to DCVX (roaming) and from DCVX to external networks such as DSN, UC Network, and/or PSTN.

TAC-000390 [**Optional**] The terminal device may support other non-NSA encryption schemas, such as Advanced Encryption Standard (AES) encryption as used by the Government Emergency Telecommunications Service (GETS) system.

A.5.5.5 Device Battery

TAC-000400 [**Required**] The commercially available nonsecure terminal device that is readily available must have a battery that shall provide as a minimum 6 days standby time in total and 3 hours nonsecure talk time in total but not both requirements sequentially on the same battery charge. The NSA encryption secure terminal devices (e.g., PDA Secure Mobile Environment Portable Electronic Device [SME PED]) must provide their specified battery and secure or nonsecure talk time. All other terminal devices must provide their specified battery and nonsecure talk time and/or secure talk time, if applicable.

TAC-000410 [**Required**] The terminal device shall have the capability, when the primary battery is removed or drained, to retain primary network and user settings on the device before another primary battery is installed or recharged. This is required to ensure the terminal device is able to reconnect to the DCVX upon power-up.

A.5.5.6 Terminal Device Secure Call Handling

TAC-000420 [**Conditional**] If the terminal device supports SCIP or other NSA-accredited encryption scheme(s), then the terminal device and/or DCVX system will provide classified secure call handling features, as defined in Section 11.3.8, Secure Call Handling, if conversion is made from TDM to IP Network boundaries.

A.5.5.7 Terminal Device Display and Alerting Features

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

TAC-000430 [**Required**] Power-On Status. When the terminal device is powered on, the display shall indicate:

a. Signal strength.

b. Remaining battery capacity.

c. Active call status.

d. Registration results (either success or failure).

TAC-000440 [**Required**] ROUTINE Call Alerting. The idle, registered terminal device shall provide or be provided with an auditory and/or visual display alert for incoming ROUTINE calls.

TAC-000450 [**Optional**] Precedence Call Alerting. The DCVX may be required to meet the eMLPP functionalities specified in Section A.5.4.8, Precedence and Preemption. The eMLPP references or uses a proprietary methodology. If precedence and preemption capability is provided, then, upon receiving a precedence call, the idle, registered terminal device will provide or be provided with a precedence alert and/or tone notification. Whether using eMLPP or a proprietary version, the terminal device shall issue the same alerting tone(s) for precedence calls IAW eMLPP requirements. Upon notification, the user will have the capability to select or reject the call of higher precedence.

A.5.6 Access Network-Specific

Specific Access Network capability is as follows.

A.5.6.1 Signaling

TAC-000460 [**Required**] The Access Network will determine which channel to use for call setup IAW the appropriate supported protocols listed in Section A.5.4.2, Protocol/Format, as outlined in Table A.5-1, Current Cellular Systems Parameters.

A.5.6.2 Strength

TAC-000470 [**Required**] The Access Network 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 Section A.5.4.2, Protocol/Format.

A.5.6.3 Protocol/Format

TAC-000480 [**Required**] The Access Network shall support one or more of the protocols listed in the DCVX general requirements, in Section A.5.4.2, Protocol/Format, and as outlined in Table A.5-1, Current Cellular Systems Parameters.

A.5.6.4 Coverage

TAC-000490 [**Required**] The Access Network will assign the strongest cell to the terminal device per the standards. The coverage area this system will provide shall be IAW the GSM (2G, 3G, Pre-4G), CDMA, Mobile WiMAX and/or 4G standards and specifications IAW Table A.5-1, Current Cellular Systems Parameters, and in Section A.5.4.2, Protocol/Format. Actual coverage will depend on topology and/or manmade structures and frequencies.

A.5.6.5 Preemption

TAC-000500 [**Conditional**] If precedence and preemption capability is provided in the DCVX, then, in the event of a preemption for reuse, the Access Network and/or Core Network must disable the old call and maintain the current channel assignment to the terminal device in order to allow the set up of the new call. In the event where there are no idle channels available and preemption for reuse does not occur, then when a precedence call is received, the DCVX will find the lowest precedence channel and preempt that channel to allow for the higher-level precedence call to be completed.

A.5.7 Core Network-Specific

Because of the differences between the various cellular generations (2G, 3G, Pre-4G, 4G), it is not feasible to identify specific component requirements. Thus, this appendix refers to Core Network functionality instead. Additionally, the HLR functionality is not required to be a local component part of the Core Network, but it will be necessary for the Core Network to access a home location register at some location to determine the attributes of its supported terminal device. Whether the home location registry functionality is local with the Core Network or it is remotely queried, the home location registry functionality is a component of the DCVX under test.

A.5.7.1 Visitor Location Register Functionality

TAC-000510 [**Required**] The Core Network shall maintain a Visitor Location Register Functionality to allow service to any authorized active terminal device within its domain per in Section A.5.4.2, Protocol/Format. Visitor Location Register (VLR) functionality may be updated by the DCVX resident HLR functionality, a shared HLR functionality with another DCVX, and/or via roaming between DCVXs.

A.5.7.2 Home Location Register Functionality

TAC-000520 [**Required**] The Core Network shall connect to an HLR functionality to determine the attributes of the terminal device currently being served by the DCVX. The HLR Functionality can be co-located with the Core Network or accessed remotely. Access to the remote HLR Functionality may be by one or more of the following connection types:

a. ISDN PRI (T1/E1).

b. MLPP ISDN PRI (T1/E1).

c. IP AS-SIP (signaling and associated bearer channel).

d. Signaling Transport (SIGTRAN) (CCS7 over IP).

e. 2G, 3G, and/or 4G Standards interconnection protocols transported across DoD Networks.

TAC-000530 [**Required**] HLR Storage. The HLR Functionality must store and support information on each terminal device registered to the network that the HLR Functionality serves.

TAC-000540 [**Required**] HLR Change and Propagation. The HLR Functionality must support changes to the terminal device information. Once the HLR receives the supported change information, the HLR, whether local or remote from the Core Network, has 3 minutes to propagate the change information to the VLR Functionality. If the DCVX supports roaming, then the HLR change must also propagate to the querying VLRs.

TAC-000550 [**Conditional**] Intra-DCVX Queries. If a roaming capability is supported in the DCVX, then the HLR Functionality must support queries from other DCVXs using specified protocol methods for obtaining terminal device information [e.g., GSM (2G, 3G, Pre-4G), CDMA, Mobile WiMAX, and/or 4G standards] based queries.

A.5.7.3 Equipment Identity Register Functionality

TAC-000560 [**Required**] To validate terminal devices to prevent a compromised terminal device from connecting to the cellular switch and obtain services, an Equipment Identity Register (EIR) functionality must be provided and integrated to work in conjunction with the Terminal Device Authentication Center functionality as stated in Section A.5.7.4, Terminal Device Authentication Center Functionality, to prevent compromising the DCVX.

A.5.7.4 Terminal Device Authentication Center Functionality

TAC-000570 [**Required**] To authenticate terminal devices as valid terminal devices associated with the DCVX, the cellular switch will use standard cellular techniques, industry best practices, and/or vendor proprietary processes integrated into the switch.

TAC-000580 [**Optional**] Terminal devices not assigned to the supporting Deployed Mobile Switching Center (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.

A.5.7.5 Core Network External Network Trunks and Interfaces

TAC-000590 [**Required**] The Core Network shall support one or more of the following TDM and/or IP trunks and interfaces. The Core Network can support simultaneous interface connections to the DSN and UC VVoIP/Data networks using TDM and IP respectively, but not use TDM and AS-SIP protocol simultaneously in support of voice and/or video calls.

A.5.7.5.1 TDM Support

TAC-000600 [**Conditional**] If TDM trunks are supported, then the following requirements apply as directed:

> **TAC-000600.a** [**Required**] The Core Network will support ISDN PRI (T1/E1) as defined in Section 2.25.1, National ISDN 1/2 Basic Access for trunks that connect to the DSN/PSTN without MLPP capability.
>
> **TAC-000600.b** [**Conditional**] If a precedence and preemption capability is provided in the DCVX, then the Core Network will support MLPP PRI (American National Standards Institute [ANSI] T1.619a, ITU Q.955.3 and/or Q.735.3) per Section 2.25.2.7, ISDN MLPP PRI.
>
> **TAC-000600.c** [**Conditional**] The Core Network may support a DS1 Interface (e.g., PCM-24, PCM-30) per Section 11.2.3.4, DS1 Interface.

A.5.7.5.2 AS-SIP IP Trunking Support

TAC-000610 [**Conditional**] If AS-SIP IP trunks are supported, then the DCVX shall comply with the stated requirements of an SC, and if required, act as a SIP Back-to-Back User Agent (B2BUA). The Core Network and terminal devices supporting UC VVoIP Services are required to meet the conditions as stated in Section 8, Information Security.

A.5.7.5.3 DCVX Interconnection (Roaming)

Including the connections provided in Section A.5.7.5.1, TDM Support, and Section A.5.7.5.2, AS-SIP IP Trunking Support, one or more of the following connections can be used for connecting DCVXs together on DoD networks within the Tactical OAN in support of roaming capability and/or querying the local or remote HLR Functionality. Neither connection type below shall connect to the PSTN and/or other non-Government networks.

TAC-000620 [**Optional**] SIGTRAN: The Core Network may support CCS7 over IP using SIGTRAN IAW Internet Engineering Task Force (IETF) Request for Comments (RFC) 2719, and other associated supporting RFCs.

TAC-000630 [**Optional**] 2G, 3G, and/or 4G Standards: The interconnection portion of the protocols contained within the 2G, 3G, Pre-4G, Wideband WiMAX, and/or 4G Standards, as

delineated in Section A.5.4.2, Protocol/Format, may be used to interconnect DCVX systems when said protocols are transported over DoD operated and/or controlled networks.

A.5.7.5.4 Non-MLPP Networks Support

TAC-000640 [**Optional**] The Core Network may support an ISDN PRI (T1/E1) non-MLPP trunk for connecting to the PSTN and/or other non-Government networks. ISDN PRI (T1/E1) requirements are contained within Section 2.25.1, National ISDN 1/2 Basic Access.

A.5.7.6 Call Handling

TAC-000650 [**Required**] The Core Network shall handle both intraswitch calls and calls to and from the DSN, PSTN, and/or UC Services Network, while recognizing a powered-on terminal device that comes into its operational area.

A.5.8 Security

TAC-000660 [**Required**] All components of the DCVX shall meet security requirements as outlined in DoDI 8510.01 and the applicable STIG.

A.5.9 DCVX Network Management

TAC-000670 [**Required**] The DCVX is to be managed by at least one or more of the following:

TAC-000670.a [**Optional**] A front or back panel and/or external console control capability shall be provided for local management.

TAC-000670.b [**Optional**] Remote monitoring and management by the Advanced DSN Integrated Management Support System (ADIMSS) or similar Network Management (NM) systems developed by DoD Components. The following requirements apply:

TAC-000670.b.1 [**Required**] Data Interface: The NE shall provide NM data/monitoring via one or more of the following physical interfaces:

(a) Ethernet/Transmission Control Protocol (TCP)/IP (IEEE 802.3).

(b) Serial (RS-232)/Asynchronous.

(c) Serial/Synchronous (X.25 and/or BX.25 variant).

All data that is collected shall be accessible through these interfaces. For NM purposes, the NE must provide no less than two separate data channels. They may be physically separate (e.g., two distinct physical interface points) or logically separate (e.g., two user sessions through a single Ethernet interface). The data may be sent in ASCII, binary, or hexadecimal data or ASCII text designed for screen/printer display.

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

i. Alarm/Log Data.

ii. Accounting data (e.g., Call Detail Record [CDR]).

iii. Performance Data (e.g., traffic data).

iv. DCVX access (to perform DCVX data fill administration and network controls).

TAC-000670.b.2 [**Required**] Fault Management: The DCVX shall detect fault (alarm) conditions and generate alarm notifications. The alarm messages must be sent to the assigned NM Alarm channel in near-real time. No alarm restriction/filtering is necessary. In addition to the data formats in Section 11.2.4, Device Management, alarms may be sent as Simple Network Management Protocol (SNMP) traps. If this channel is also used to output switch administrative log information, then the alarm messages must be distinguishable from an administrative log message.

TAC-000670.b.3 [**Required**] Configuration Management: Requirements for this feature shall be in accordance with Telcordia Technologies GR-472-CORE, Section 4.

A.6 DEPLOYED (TACTICAL) MASTER SC AND SUBTENDED SC REQUIREMENTS AND DASAC REQUIREMENTS IN SUPPORT OF BANDWIDTH CONSTRAINED LINKS

Since these requirements are applicable to the Fixed (Strategic Enterprise), as well as to the Deployed (Tactical) environment, these requirements are defined in Section 2.24, MSC and SSC. Many of these requirements, which are mandatory for the Deployed environment, are conditional for the Fixed environment.

A.7 DEPLOYED WIDE AREA NETWORK OPTIMIZATION CONTROLLER

A.7.1 Introduction

This product category defines the functions and requirements specific to a Deployed Wide Area Network (WAN) Optimization Controller (WOC).

A.7.2 WOC Functional Description

WAN optimization appliances provide efficiencies in WAN data transmission in the deployed environment over all RF or wired connections where deployed. Data efficiency are determined by measurable values and related to the function of the WAN Optimization Appliance type.

A.7.3 Throughput Acceleration Requirements

TAC-000680 [**Required: WOC**] The optimization appliance shall have proxies or strategies for accelerating Hyper Text Transfer Protocol (HTTP) and HTTP Secure (HTTPS) traffic.

TAC-000690 [**Required: WOC**] The optimization appliance shall have proxies or strategies for accelerating File Transfer Protocol (FTP), Secure Copy Protocol (SCP) and Secure File Transfer Protocol (SFTP) traffic.

TAC-000700 [**Required: WOC**] The optimization appliance shall have proxies or strategies for accelerating Common Internet File System (CIFS) and Microsoft SharePoint traffic.

TAC-000710 [**Required: WOC**] The optimization appliance shall have proxies or strategies for accelerating Citrix traffic and Windows Remote Desktop connections.

TAC-000720 [**Required: WOC**] The optimization appliance shall provide a service that allows proactive pre-positioning of files at peering appliances across a WAN segment.

TAC-000730 [**Required: WOC**] The optimization appliance shall have proxies or strategies for accelerating email interfaces. Examples of email interfaces include but are not limited to the IETF standard Simple Mail Transport Protocol (SMTP) and the Microsoft proprietary Messaging Application Programming Interface (MAPI).

TAC-000740 [**Required: WOC**] The optimization appliance shall increase the throughput of all TCP connections. Data Efficiency is measured by: WAN Data Reduction = (LAN [Kbytes] - WAN [Kbytes]) / LAN (Kbytes) %.

TAC-000750 [**Required: WOC**] The optimization appliance, when conducting TCP transfers with Transport Layer Security (TLS), shall at least match the throughput performance of the standard Space Communications Protocol Specification-Transport Protocol (SCPS-TP) protocol.

A.7.4 Data Reduction Requirements

TAC-000760 [**Required: WOC**] The optimization appliance shall have the ability to perform transparent, lossless, data compression on individual TCP connections.

TAC-000770 [**Required: WOC**] The optimization appliance shall be capable of compression and data reduction of TCP traffic. Data Efficiency is measured by: WAN Data Reduction = (LAN [Kbytes] - WAN [Kbytes]) / LAN (Kbytes) %.

TAC-000780 [**Required: WOC**] The optimization appliance shall be capable of compression and data reduction of User Datagram Protocol (UDP) traffic (objective).

TAC-000790 [**Required: WOC**] The optimization appliance shall be capable of compression and data reduction of Generic Routing Encapsulation (GRE) tunnel traffic (objective).

A.7.5 Quality of Service Requirements

TAC-000800 [**Required: WOC**] The optimization appliance shall have the capability to provide the quality-of-service functions such as: packet identification and marking, traffic shaping, and traffic policing.

TAC-000810 [**Required: WOC**] The optimization appliance shall have features to assign minimum and maximum bandwidth to particular traffic flows, as identified by any combination of source and destination addresses, TCP/UDP port, Differentiated Services Code Point (DSCP), or application protocol. Data Efficiency is measured by: High Priority traffic flow (Kbps) on Non-congested WAN = High Priority traffic flow (Kbps) on Congested WAN.

TAC-000820 [**Required: WOC**] The optimization appliance shall be capable of applying DSCP markings according to user-configurable rules.

A.7.6 Real-Time Traffic Requirements

TAC-000830 [**Required: WOC**] The appliance shall be capable of performing Robust Header Compression (ROHC) for all voice over IP packets, per IETF RFC 3095.

TAC-000840 [**Required: WOC**] The appliance shall be capable of concatenating small UDP packets together while minimizing jitter; the capture window size (in msec) shall be user adjustable, and provide multiple queues for different DSCP values.

TAC-000850 [**Required: WOC**] The optimization appliance shall allow bypassing specific IP UDP, and TCP flows from the processing requirements defined in prior sections. The flows will be identified by IP protocol number, source and destination pair, {address, port} tuples, UDP/TCP ports, or DSCP. The appliance shall not degrade performance (i.e., packet loss, delay and jitter) for such flows.

A.7.7 Network Monitoring Requirements

TAC-000860 [**Required: WOC**] The optimization appliance shall be capable of capturing at least 1 GB of complete packets (headers and payloads), and exporting them in a standard packet capture formatted files (such as PCAP) to network accessible storage.

TAC-000870 [**Required: WOC**] The optimization appliance shall collect and present real-time traffic statistics and graphs, including: (a) a listing of the concurrent TCP and UDP flows; (b) percentage of traffic by protocol; (c) the top-ten flows by bandwidth; and (d) the top-ten flows by duration. The statistics and graphs shall cover scales from 5 minutes to 1 week. The data used to

draw the graphs shall be transferable to network accessible storage in comma-separated values (csv) or Microsoft Excel (xls) format.

A.7.8 IPv6 Requirements

TAC-000880 [**Required: WOC**] The appliance shall process IP version 6 (IPv6) traffic with performance at least equal to IP version 4 (IPv4).

TAC-000890 [**Required: WOC**] The WAN optimization appliance shall be capable of supporting IPv4 and IPv6 simultaneously.

TAC-000900 [**Required: WOC**] The WOC shall meet the IPv6 requirements specified in Section 5, IPv6 Requirements, identified for Network Appliance/Simple Server (NA/SS).

A.7.9 Appliance Management Requirements

TAC-000910 [**Required: WOC**] The optimization appliance shall automatically discover its peers, without manual configuration.

TAC-000920 [**Required: WOC**] The optimization appliance shall be able to discover the conditions of the WAN connection and adjust to changes in operating characteristics (e.g., bandwidth, delay, and packet loss rates), without manual configuration or foreknowledge of the characteristics of the WAN connection.

TAC-000930 [**Optional: WOC**] The optimization appliance shall present a Management Information Base (MIB) accessible via the SNMP protocol, using Federal Information Processing Standards (FIPS) 140-2 compliant algorithms (Protocol Data Unit [PDU]).

TAC-000940 [**Optional: WOC**] The optimization appliance shall provide a device manager via a HTTP/HTTPS Graphical User Interface (GUI).

TAC-000950 [**Optional: WOC**] The optimization appliance shall provide a full featured Command Line Interface (CLI).

TAC-000960 [**Optional: WOC**] The optimization appliance shall support SNMPv3 Authentication and Encryption.

A.7.10 Packet Loss Mitigation Requirements

TAC-000970 [**Required: WOC**] The optimization appliance shall have methods to mitigate IP packet loss through the application of forward error correction and packet order correction.

A.7.11 Deployed Link Requirements

TAC-000980 [**Required: WOC**] The optimization appliance shall remain fully operational when the connection bandwidth is as low as 56 kbps bidirectional.

TAC-000990 [**Required: WOC**] The optimization appliance shall remain fully operational when the packet loss rate on a connection is as high as 5 percent.

TAC-001000 [**Required: WOC**] The optimization appliance shall remain fully operational when the WAN connection has up to 3 seconds of one-way delay.

TAC-001010 [**Required: WOC**] The optimization appliance shall remain fully operational with 0.5-second delays in the forward direction and up to 2.5 seconds in the return direction.

TAC-001020 [**Required: WOC**] The optimization appliance shall remain fully operational with bandwidth asymmetries of up to 75:1 (forward TCP: return ACK).

A.7.12 Fail-Over Requirements

TAC-001030 [**Required: WOC**] The optimization appliance shall have a fail-to-wire capability that engages during power outages, during system reboot, and when the accelerator is powered off.

TAC-001040 [**Required: WOC**] The optimization appliance shall be resilient to loss of power. The appliance must self-restore to the last configured state before loss of power without intervention when power is restored.

A.7.13 Security Requirements

TAC-001050 [**Required: WOC**] The optimization appliance's CLI shall be accessed in-band only via secure login and shall be restricted to authorized users with individual user-identification and password.

TAC-001060 [**Required: WOC**] The optimization appliance will limit the number of sequential unsuccessful Secure Shell (SSH) login attempts per account to three, and shall lock out access to that account after that many failed attempts.

TAC-001070 [**Required: WOC**] The optimization appliance must log all management and configuration accesses.

TAC-001080 [**Required: WOC**] The optimization appliance's local serial-port access shall be restricted to authorized users with individual user-identification and password.

TAC-001090 [**Required: WOC**] The traffic from the remote management console to the management sub-system and vice-versa shall be encrypted, via TLS/SSL or IPSec encapsulation.

TAC-001100 [**Required: WOC**] The optimization appliance shall maintain security of any sensitive cached data by providing the appropriate encryption for any non-volatile storage media.

TAC-001110 [**Required: WOC**] The optimization appliance shall include data-erase capability such that the appliance returns to a sanitized state when the power is removed.

A.7.14 Interface Requirements

TAC-001120 [**Required: WOC**] WAN and LAN network interfaces shall be 10/100 (10/100/1000) speed and duplex auto-sensing wired Ethernet, in accordance with applicable Institute of Electrical and Electronics Engineers (IEEE) Std 802.3 standards.

A.7.15 Interoperability Requirements

TAC-001130 [**Required: WOC**] The optimization appliance shall support a mode of operation that uses the standard SCPS-TP.

TAC-001140 [**Optional: WOC**] The optimization appliance shall support a mode of operation that uses the standard SCPS-SP.

TAC-001150 [**Required: WOC**] The optimization appliance shall produce "routable" traffic, i.e., traffic that is proper IPv4 or IPv6 traffic. Traffic between two optimizers must be standard IPv4 (or IPv6) packets.

A.7.16 Physical Characteristics

TAC-001160 [**Required: WOC**] The system shall not incur damage when stored without power, heat, and air conditioning for 30 days, subject to the environmental conditions contained in this specification.

TAC-001170 [**Required: WOC**] All rack-mountable system equipment shall be installed in EIA-standard 19 inch (48.31 centimeters) electronic equipment rack(s), in accordance with EIA-RS310D. A depth of no more than 24" should be considered in cases where the system or its components may be installed in Transit Cased systems.

A.7.17 Power

TAC-001180 [**Required: WOC**] The system and its components shall be capable of operation with voltage ranges from 110–240VA, 50/60 Hertz (Hz).

TAC-001190 [**Conditional: WOC**] If auto-sensing input power supplies are not utilized then the system shall utilize manual switch setting for different voltage ranges.

TAC-001200 [**Required: WOC**] The system shall have dual power supplies acting in redundant mode.

TAC-001210 [**Required: WOC**] The WAN Optimization appliance shall be capable of continued operations in the event of a power supply failure.

TAC-001220 [**Required: WOC**] The system shall comply with best commercial practices and standards, including National Fire Protection Association (NFPA) 70 (National Electrical Code) and UL 60950 (Safety of Information Technology Equipment) for the electrical design of system

components. The system shall not present uncontrolled hazards during operation, maintenance, or disposal of equipment.

A.7.18 Safety

TAC-001230 [**Required: WOC**] A means shall be provided for disconnecting AC and DC power to each item of rack-mounted electronic equipment.

TAC-001240 [**Required: WOC**] Personnel shall be protected from accidental exposure to sharp projections and corners, as specified in MIL-HDBK-454, Guideline No. 1.

TAC-001250 [**Required: WOC**] Components of the system utilizing LASER or Fiber Optic interfaces shall be appropriately labeled in accordance with ANSI Z136.2—January 1988: American National Standard for Safe Use of Optical Fiber Communications Systems Utilizing Laser Diode and Light Emitting Diode (LED) Sources.

A.7.19 Environment

TAC-001260 [**Required: WOC**] The system and its components shall operate normally within the threshold temperature range of 0 to 40 degrees C (+32 to +104 degrees F) with an objective temperature range of -30 degrees C to +49 degrees C (-22 to +120 degrees F). The system shall withstand storage and transportation in temperature extremes from –30 to +50 degrees C (-22 to 122 degrees F).

TAC-001270 [**Required: WOC**] In the operating mode, the system and its components shall operate when exposed to relative humidity up to 95 percent non-condensing.

TAC-001280 [**Required: WOC**] The system and its components shall, in its operational configuration, withstand exposure to settling dust and shall sustain no dust penetration that affects operational service requirements. Use of filters is acceptable.

TAC-001290 [**Required: WOC**] The system and its components shall, during operation and while in storage/transport conditions, withstand exposure to environments such as those found in coastal areas or aboard ships.

TAC-001300 [**Required: WOC**] No element of the system and its components shall operate at an acoustic noise level in excess of 65 dB(A). The acoustic noise level during temporary noise conditions, such as equipment alarms, shall not be considered part of the normal operational state.

A.7.20 Corrosion Control

TAC-001310 [**Required: WOC**] Connective components of the system (bolts, washers, nuts, etc.) shall be manufactured from corrosion-resistant or non-corrosive materials.

TAC-001320 [**Required: WOC**] All external parts and materials subject to corrosion shall be coated with anti-corrosion compounds and/or fabricated from non-corrosive materials.

A.7.21 Nuclear, Biological, and Chemical (NBC) Survivability

TAC-001330 [**Required: WOC**] The system and its components shall be capable of operation and maintenance by personnel wearing full NBC-contaminant protective clothing (Mission Oriented Protective Posture [MOPP] IV level).

TAC-001340 [**Required: WOC**] The external portion of the system and its components shall be capable of decontamination using NBC-decontamination procedures and equipment. MIL-HDBK-783 and MIL-STD-810F, Test Method 504 may be used as guidance on contamination avoidance and decontamination procedures.

A.8 RADIO GATEWAY REQUIREMENTS

A.8.1 Introduction

This section establishes the requirements for the components that are used in a Radio Gateway (RG).

A.8.1.1 Purpose

The UCR Radio Gateway (RG) Requirements product category is specific to the functionality of the RG. The functionality is available to support UC APL products and products that may not require UC APL certification. For example, DoD radio equipment, Radio End Instruments (REIs), and Voice Net Access Radios (VNARs) are not on the Unified Capability APL but are the critical communication asset that the RG MUST interface to. In addition to the radio assets, an IP End Instrument (EI) or its application may not be part of the UC APL. This is due to the new support capabilities of the RG's Stream Function. This function is capable of receiving and transmitting Real-Time Transport Protocol (RTP) voice traffic over multicast. While this category defines the RG's multicast requirements, the IP EI must also meet specific multicast requirements—similar to the requirements defined under the Stream Function.

A.8.1.2 General

The RG's primary function is to connect a VNAR with interested but dissimilar DISN End Instruments (EI)s. The RG can be one physical device, performing all of the necessary functions, or be a host of components and functions that are separated by the technologies that make up a portion of the DISN architecture. Figure A.8-1, Radio Gateway Components, provides a high-level overview of the core RG components.

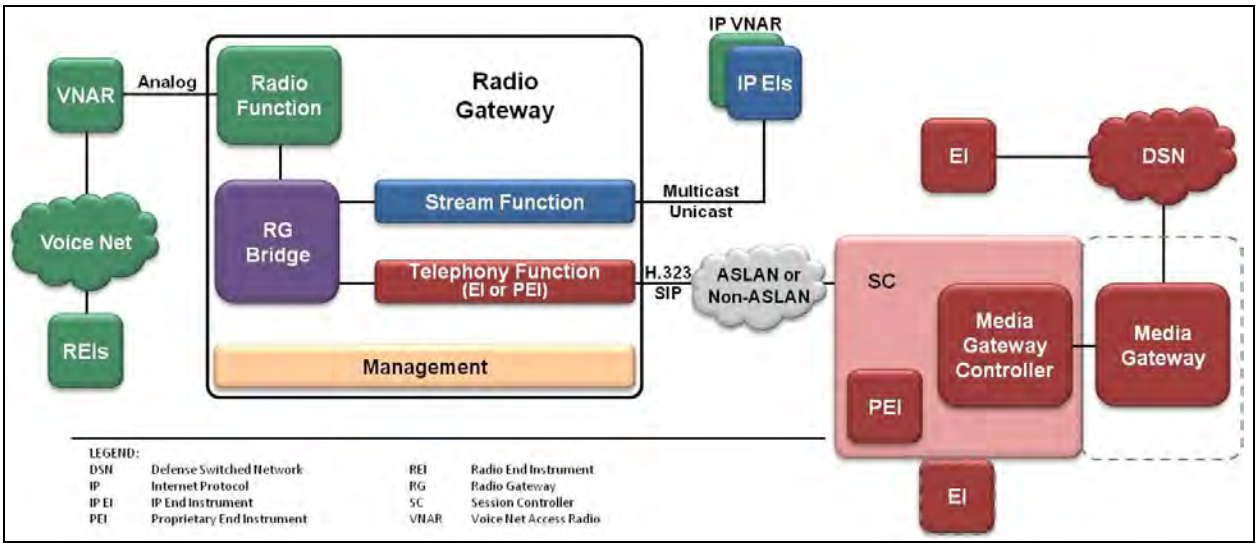


Figure A.8-1. Radio Gateway Components

A.8.2 Interfaces

The interfaces that the RG supports can be divided into three categories – Analog, Network, and Serial. Each of these performs a specific role to provide external access to various EIs. Figure A.8-2, Radio Gateway Interfaces, provides a high-level overview of the RG interfaces. These functions and the interface requirements are listed in the following text.

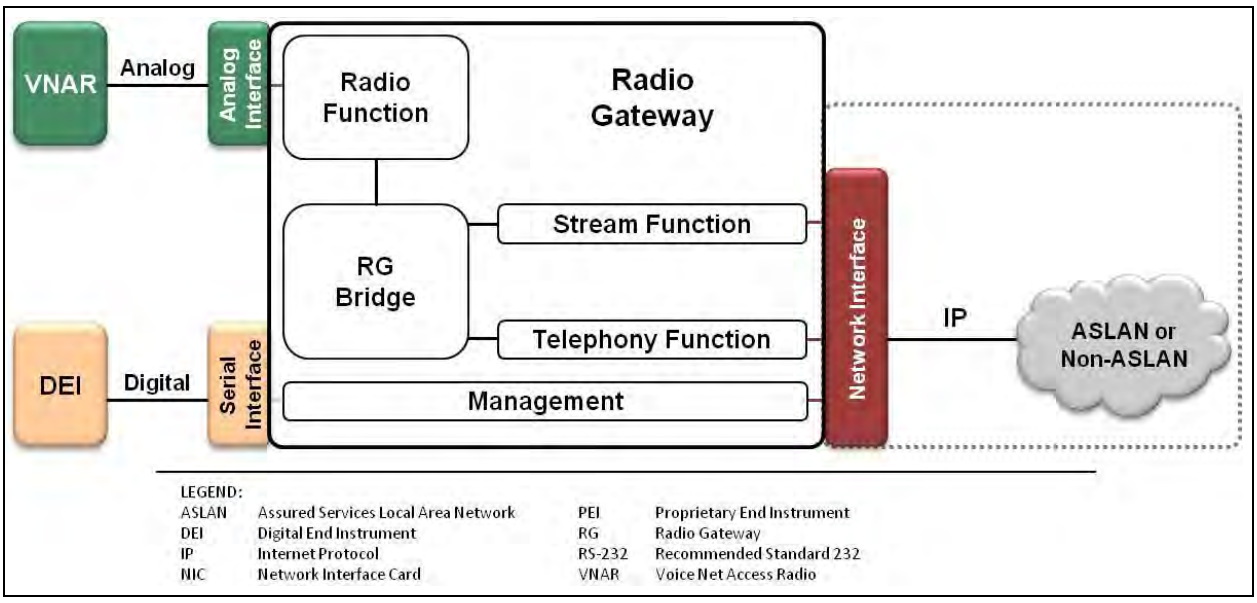


Figure A.8-2. Radio Gateway Interfaces

A.8.2.1 Analog Interface (Radio Function)

TAC-001350 [**Required: RG**] The RG shall contain an Analog Interface.

TAC-001360 [**Required: RG**] The RG Analog Interface shall support 4 and 2 wire configurations.

TAC-001370 [**Required: RG**] The RG's analog interface shall support an impedance of 600Ω balanced or unbalanced.

TAC-001380 [**Required: RG**] The RG's analog interface shall support an impedance of 47kΩ.

TAC-001390 [**Optional: RG**] The RG's analog interface may support high impedances dictated by the radio being connected to the RG.

A.8.2.2 Network Interface (Telephony and Stream Functions)

TAC-001400 [**Required: RG**] Ethernet interfaces shall be in accordance with IEEE 802.3-2002.

TAC-001410 [**Required: RG**] The RG shall support the following Ethernet types:

a. 10 Base-x.

b. 100 Base-x.

c. 1000 Base-x.

A.8.2.3 Network & Serial Interface (Management Functions)

TAC-001420 [**Required: RG**] The RG's Management interface shall be provided by one or more of the following serial or Ethernet interfaces.

TAC-001430 [**Optional: RG**] The RG's Management interface may support Serial or Ethernet interfaces: Ethernet interfaces shall be in accordance with IEEE 802.3-2002. Serial interfaces shall be in accordance with one of the following standards:

d. ITU-T Recommendation V.35.

e. TIA-232-F.

f. EIA-449-1.

g. TIA-530-A.

A.8.3 Functional Requirements

This section defines the functional requirements that the RG performs in order to support voice flow between EIs and VNARs. Figure A.8-3, Bearer and Signal Paths, provides an overview of the bearer channels and Push To Talk (PTT) signaling links necessary to provide connectivity between the different EIs and a VNAR. PTT signaling is required for all RG deployments. This signal instructs the VNAR to accept remote VNAR and/or EI bearer traffic and relay it to the associated radio voice net. Without this instruction, bearer traffic could be sent to the VNAR but no audio would pass to the REIs that share the same voice net.

The flow shown in Figure A.8-3, Bearer and Signal Paths, illustrates a number of different PTT signaling methods. The PTT signaling method/s used will be determined by the VNAR, EIs, and the RG.

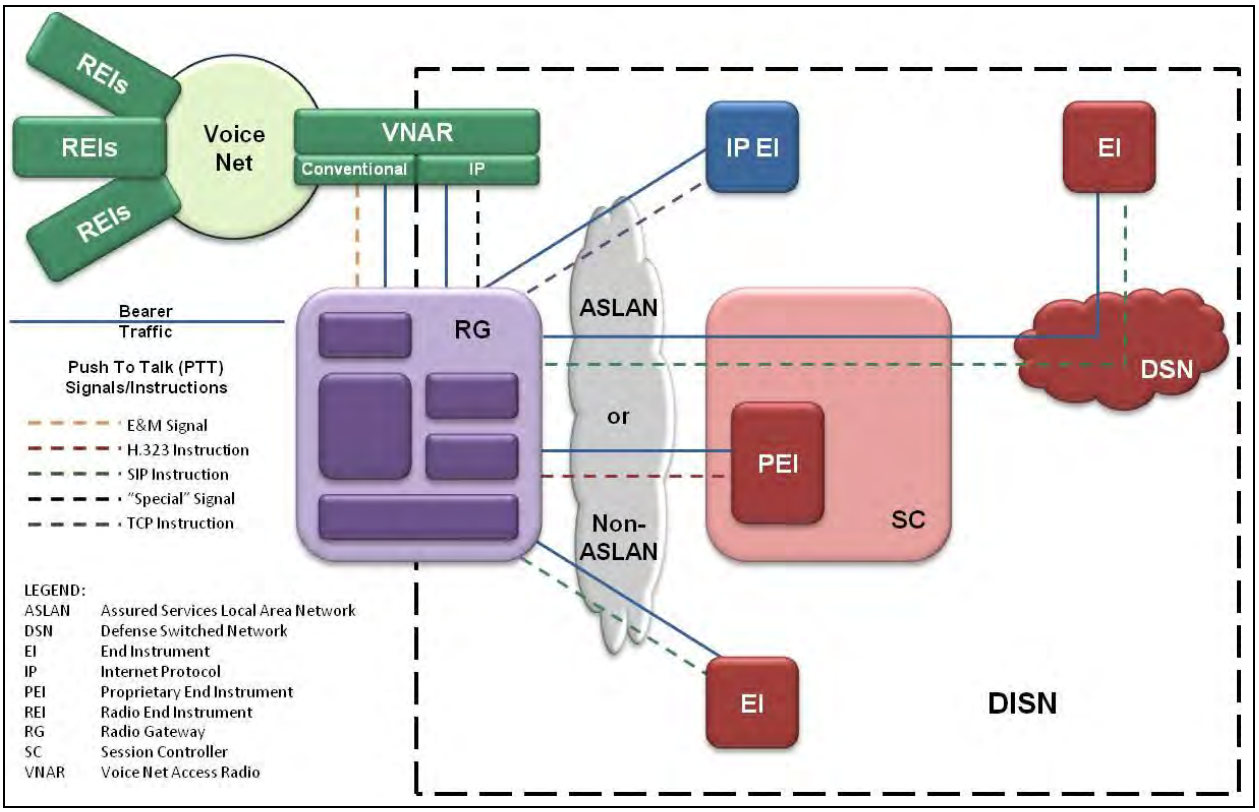


Figure A.8-3. Bearer and Signal Paths

A.8.3.1 VNAR PTT

When an EI wants to send audio to the radio, a PTT instruction is sent to the RG using the EI's connection protocols and technologies. The RG interprets these instructions and then sends the PTT signal in the VNAR's proper format.

TAC-001440 [**Required: RG**] The RG shall support Ear and Mouth (E&M) PTT signaling in accordance with "MILSTD 188.141C" for connecting to the VNAR.

TAC-001450 [**Required: RG**] The RG shall support in-ban PTT signaling for connecting to the VNAR.

TAC-001460 [**Required: RG**] The RG shall support Pass-through. Pass-through is an RG method that, when bearer traffic is received from a remote EI, the traffic is passed to the VNAR with no special RG PTT signaling. The PTT mechanisms are all internal to the radio (i.e., VOX).

TAC-001470 [**Required: RG**] when configured to support VOX the RG shall not clip the beginning of the audio received.

TAC-001480 [**Required: RG**] The RG shall support configurable Tone Signaling.

TAC-001490 [**Optional: RG**] The RG may support tone signaling configurable between the 0Hz and 3201Hz frequency range.

TAC-001500 [Optional: RG] The RG may support a dB Level or Amplitude tone signal configurable at or between -50 and 3dB.

TAC-001510 [**Required**: RG] The RG ~~may~~ shall support tone duration configurable at or between 10 and 2000ms.

TAC-001520 [**Required**: RG] The RG shall support Guard Tones configurable for an infinite duration.

TAC-001530 [**Required**: RG] The RG shall support sequential order tone patterns.

TAC-001540 [**Required**: RG] The RG shall support a minimum of 8 signaling tones.

TAC-001550 [Optional: RG] The RG analog interface may support 2/4-wire Type III E&M signaling.

TAC-001560 [Optional: RG] The RG analog interface may support 2/4-wire Type V E&M signaling.

A.8.3.2 COR, COS, and VAD

TAC-001570 [**Required: RG**] The RG shall support Carrier Operated Relay (COR) or Carrier Operated Switch (COS) Signaling.

TAC-001580 [**Required: RG**] The RG shall be capable of inspecting the incoming VNAR RF audio stream to determine if it is valid audio traffic or refuse the propagation of noise.

A.8.3.3 Audio Manipulation

To gain optimal stream behavior between the RG and VNAR, several processes are used by the radio function.

TAC-001590 [**Required: RG**] The RG shall support the capability of performing both half-duplex and full-duplex signaling.

TAC-001600 [**Required: RG**] The RG shall support the ability to lower or raise the amplitude of the transmitted or received audio stream within the minimum range of 0 and 10dB.

TAC-001610 [**Required: RG**] The RG shall support the ability to configure from 0ms - 2000ms. Receive Audio Timeout after transmitted audio to the VNAR has ceased.

TAC-001620 [**Required: RG**] The RG shall support relay of audio signals that are above a configurable dB threshold.

A.8.4 Telephony Functions

A.8.4.1 Telephony EI PTT Instruction Functionality

TAC-001630 [**Conditional: RG**] If the RG supports SIP Instructions from the EI, then the RG shall support the following:

a. In-Band PTT instructions ('start' and 'stop') by receiving EI generated Dual-Tone Multifrequency (DTMF) tones over the RTP audio bearer per RFC 4733, RTP Payload for DTMF Digits, Telephony Tones, and Telephony Signals.

   OR

b. Out-of-Band EI PTT instructions ('start' and 'stop') by receiving Key Press Stimulus Protocol (KPML) DTMF events as defined by RFC 4730, A Session Initiation Protocol (SIP) Event Package for Key Press Stimulus (KPML).

TAC-001640 [**Conditional: RG**] If the RG supports H.323 instructions from the EI, then the RG shall support the following:

a. In-Band EI PTT instructions ('start' and 'stop') by receiving the DTMF tones over the RTP audio bearer per RFC 4733 RTP Payload for DTMF Digits, Telephony Tones, and Telephony Signals.

   OR

b. Out-of-Band alphanumeric user input messages as defined by the ITU H.245 Standard.

A.8.4.2 Audio Manipulations

TAC-001650 [**Required: RG**] The RG shall support a buffer that can withstand a variable delay of received voice segments of at least 1500ms.

TAC-001660 [**Required: RG**] The RG shall support the ability to provide a unique telephone number or Dial-in Number (DN) for each telephony function.

TAC-001670 [**Conditional: RG**] If the RG supports more than one telephony function; then, the RG shall support the following:

a. Direct-Inward-Dial (DID). This method connects the caller directly to a Telephony Function with no voice prompt requesting the user for selection.

   OR

b. The RG may support Interactive Voice Response (IVR). This method uses voice prompts to request that the caller select a Telephony Function by entering the Dial-in Number (DN) or extension of the Telephony Function.

   OR

c. Operator/Attendant Routing. This method allows an authorized operator/attendant to route a caller to the appropriate Telephony Function. This routing may be accomplished locally (e.g., using direct RG controls) or remotely (e.g., using an RG administrative network connection).

A.8.5 Authentication

TAC-001680 [**Required: RG**] The RG shall support authentication of inbound callers before allowing access to each connected Radio Bridge.

TAC-001690 [**Optional: RG**] The RG may support a Participant Code function. This code is required, before allowing a caller access to the connected Radio Bridge.

TAC-001700 [**Optional: RG**] The RG may support Operator/Attendant Authentication. – Each Telephony Function may be configured to allow a live operator/attendant to authenticate a caller by offline means before allowing access to the connected Radio Bridge.

TAC-001710 [**Required: RG**] The RG shall support an audible tone or IVR voice message to the caller if the authentication process determines that the caller is unauthorized.

TAC-001720 [**Required: RG**] The RG shall support a configurable parameter-determined period; in which the system will terminate the call if the unauthorized caller does not hang up.

TAC-001730 [**Required: RG**] The RG shall support an audible tone or IVR voice message to the caller acknowledging successful entry into the Radio Bridge.

A.8.6 Dial Plan and Routing Requirements

(Reference UCR Section 2.18, Worldwide Numbering and Dialing Plan, and UC Framework [UCF] Appendix A Section A.9.9, GBNP).

TAC-001740 [**Required: RG**] Each Telephony Function shall be assigned a routable user identity, which can be one of the following: DSN number, Tel- Uniform Resource Identifier (URI), SIP-URI, Fully Qualified Domain Name (FQDN), or internal ID.

A.8.7 Streaming Functions

A.8.7.1 IP VNAR PTT Functionality

IP VNARs can be directly connected to the DISN network using its own internal TCP/IP stack.

TAC-001750 [**Conditional: RG**] If the RG supports an IP VNAR, then the RG shall support the following:

a. Pass-Through. Pass-through is an RG method that, when bearer traffic is received from a remote EI, the traffic is passed to the VNAR with no special RG PTT signaling. The PTT mechanisms are all internal to the radio.

OR

b. DTMF Signaling the IP VNAR will accept the bearer traffic.

TAC-001760 [**Conditional: RG**] If the IP VNAR accepts SIP DTMF tones, then the RG shall support the following:

a. In-Band PTT signaling by transmitting the DTMF tone over the RTP audio bearer per RFC 4733, RTP Payload for DTMF Digits, Telephony Tones, and Telephony Signals.

   OR

b. Out-of-Band PTT signaling by transmitting KPML DTMF events to the IP VNAR as defined by RFC 4730, A Session Initiation Protocol (SIP) Event Package for Key Press Stimulus (KPML).

TAC-001770 [**Conditional: RG**] If the IP VNAR accepts H323 signaling, then the RG shall support the following:

a. In-Band PTT signaling by transmitting the DTMF tone over the RTP audio bearer per RFC 4733 RTP Payload for DTMF Digits, Telephony Tones, and Telephony Signals.

   OR

b. Out-of-Band alphanumeric user input messages, as defined by the ITU H.245 Standard.

A.8.7.2 IP EI PTT Instruction Functionality

For an RG to act on an IP EI's request to pass traffic through a connected VNAR, the RG has to be instructed to do so.

TAC-001780 [**Optional: RG**] The RG may support the capability of inspecting the incoming EI audio to determine if it is valid audio traffic or refuse the propagation of noise.

TAC-001790 [**Optional: RG**] The RG may support the capability of sending IP EI In-band Generated Tones to the VNAR with no voice inspection.

TAC-001800 [**Optional: RG**] The RG may support the capability of generating and mixing with the incoming Bearer traffic to the VNAR the necessary tones upon the detection of an IP EI voice stream.

A.8.7.3 Audio Manipulation

TAC-001810 [**Required: RG**] The RG shall support a Jitter Buffer capable of withstanding a variable delay of received voice segments of at least 1500ms.

A.8.7.4 Multicast

The RG's Stream Function can accept bearer traffic using strictly unicast point-to-point communications or multicast.

TAC-001820 [**Conditional: RG**] If the RG supports streaming RTP traffic between the Stream Function and a remotely connected EI, via multicast, then the RG shall support the following:

a. The RG shall support the Internet Group Management Protocol, Version 3 (IGMPv3) for IPv4 multicast management and multicast group membership reporting to neighboring multicast NE as defined by RFC 3376.

b. The RG shall support Multicast Listener (MLD), Version 2 for IPv6 multicast NEs to discover the presence of multicast listeners as defined by RFC 4604.

c. The RG shall support administratively scoped addresses (239/8) and multicast administrative boundaries as described in RFC 2365.

A.8.8 Bridge Functions

Once suitable audio is received by the RG from one of its functions, the RG MUST transcode the traffic and bridge it to the protocol and technology that the destination understands. The RG is responsible for bridging the functions and the connected endpoints together.

TAC-001830 [**Required: RG**] The RG shall support the capability of at a minimum, bridging a connected VNAR or IP VNAR in one of the following configurations:

a. Local Configuration. A local configuration connects more than one conventional VNAR together through the RG's backplane or internal processes (see Figure A.8-4). Note that this only applies to RGs containing more than one Radio Function.

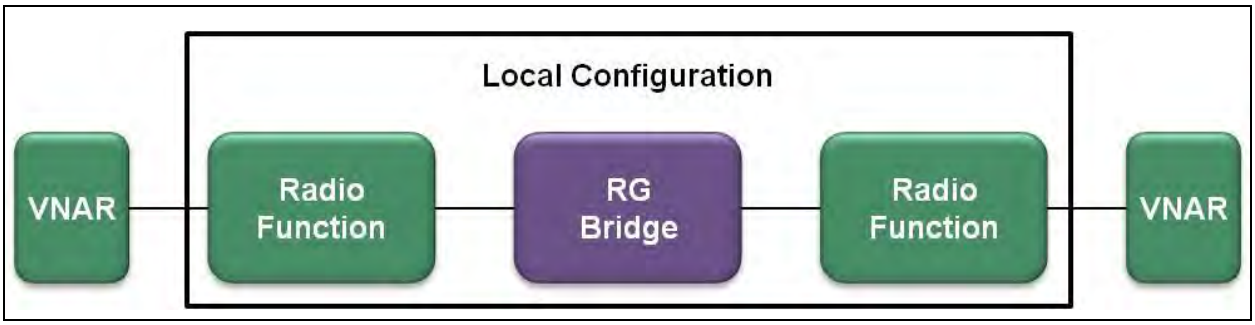


Figure A.8-4. RG Bridge Local Configuration

b. Telephony Configuration. The telephony configuration connects a VNAR or IP VNAR to a SIP/H.323 EI, remote IP VNAR, or trunk (see Figure A.8-5).

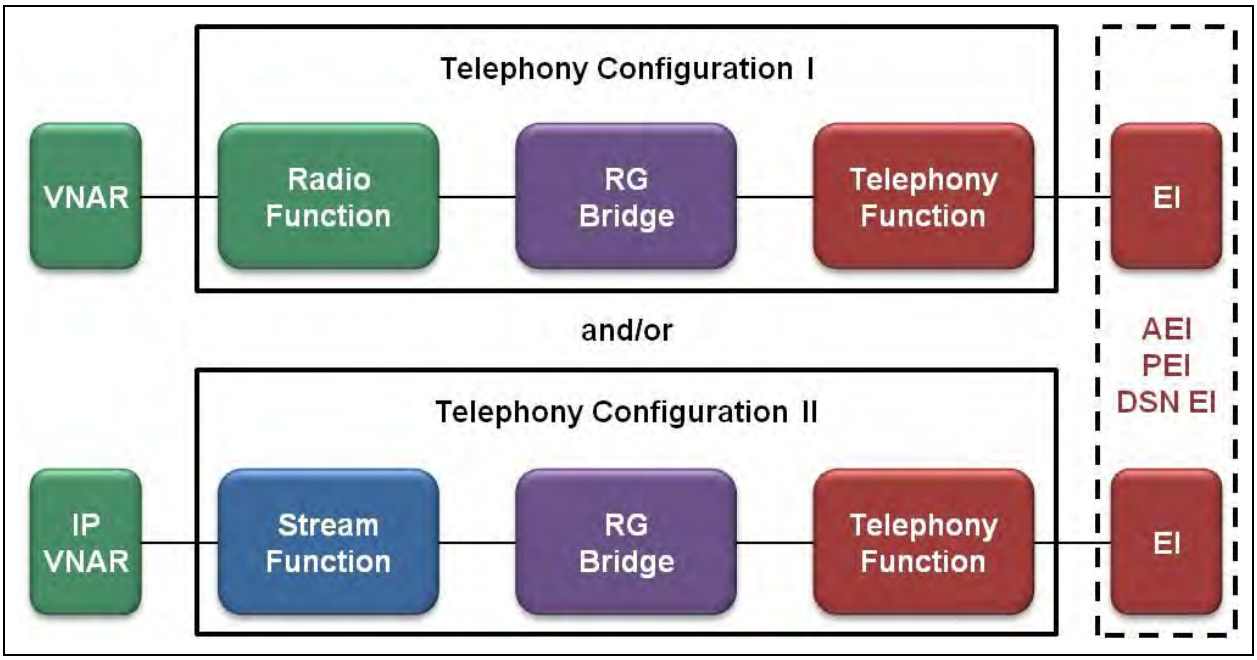


Figure A.8-5. RG Bridge Telephony Configuration

c. Stream Configuration. The stream configuration connects a VNAR or IP VNAR to a unicast or multicast voice EI or remote IP VNAR (see Figure A.8-6).

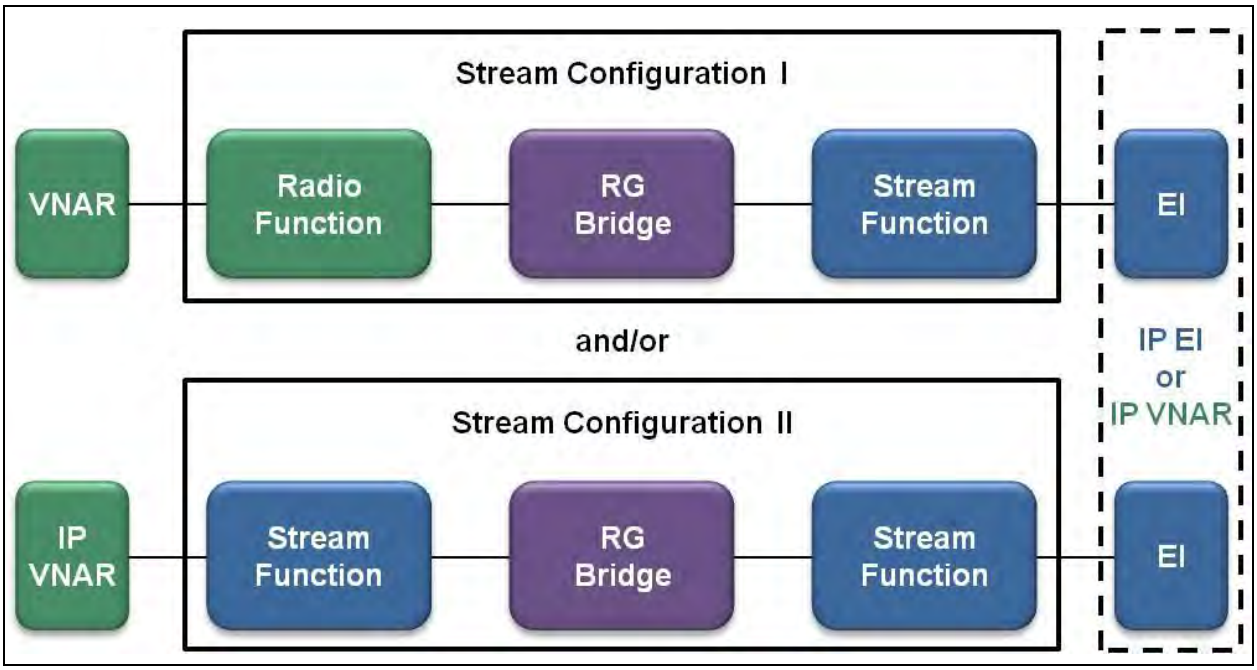


Figure A.8-6. RG Bridge Stream Configuration

TAC-001840 [**Required: RG**] The RG shall support the capability of decoding RTP traffic.

TAC-001850 [**Required: RG**] The RG shall support the capability of receiving multiple RTP streams, mixing these streams, and sending the single mixed RTP stream to an EI or VNAR (conventional or IP).

A.8.9 Bearer Traffic

In addition to acting as a PTT signaling and instruction interpreter, the RG MUST be able to receive and send audio traffic between the different endpoints (VNARs and EIs) using protocols and technologies that the RG and endpoints both support.

TAC-001860 [**Required: RG**] The RG shall support the following DSN Approved Codecs:

d. G.711 (μ law or a law).

e. G.729 or G.729A.

TAC-001870 [**Optional: RG**] IP EI Stream Codecs: In addition to the DSN Approved Codecs, the IP EI may support additional codecs.

a. G.711 (μlaw or a law).

b. G.723.1.

c. G.721.

d. G.726 (16, 24, or 32 kbps).

e. G.729 or G.729A.

f. GSM Full rate.

g. MELPe.

h. PCM 16 bit @ 128 kbps.

i. Ramalho G.711 Lossless (RGL) (μlaw or alaw).

j. Speex (2.15, 5.95, 8, 11, 15, 18.2, or 24.6 kbps).

k. G.722.1.

A.8.10 Quality of Service

TAC-001880 [**Required: RG**] The RG shall support Differentiated Services (DiffServ) per hop behaviors (PHBs) and traffic conditioning IAW RFCs 2474, 2597, 2598, 3140, and 3246.

TAC-001890 [**Required: RG**] The RG shall support a configurable mechanism to mark DSCPs in the header of IP packets. The default marking shall be as defined in UCR Section 6, Network Infrastructure End-to-End Performance Requirements.

TAC-001900 [**Required: RG**] The RG shall support a configurable fail-safe mechanism to prevent a VoIP EI from streaming continuous voice traffic to a PTT-based Voice Net.

TAC-001910 [**Required: RG**] The RG fail-safe mechanism shall only reinstate transmissions based on completion of a configurable specific, positive action by the EI.

A.8.11 Internet Protocol Version 6

TAC-001920 [**Required: RG**] The RG shall support the IPv6 requirements as defined for NA/SS in UCR Section 5, IPv6.

A.8.12 NMFCAPS

TAC-001930 [**Required: RG**] The RG shall support General Network Management requirements as specified in UCR Section 15, Enterprise and Network Management Systems.

A.8.13 Information Assurance

TAC-001940 [**Required: RG**] The RG shall support the Information Assurance (IA) requirements for a LAN Switch as defined in UCR Section 4, Information Assurance.

TAC-001950 [**Required: RG**] The RG shall apply the appropriate STIGs for an NA/SS.

A.9 IP MODEM

A.9.1 Overview

This specification establishes the performance requirements for an IP Modem that will be used for transmissions over DoD and commercial satellite systems. COTS technology, products, standards, documentation, and methods usage are recommended to the greatest extent possible.

A.9.2 IP Modem Functions

The underlying source of user requirements for an IP Modem is the Functional Capabilities Description (FCD), TIA-157. Section 3 of the FCD refers only to the Baseline IP Modem features associated with the Hub-Spoke network topology.

The following FCD sections are not applicable to or not required of an IP Modem:

1. Requirements identified in the FCD for the Mesh network topology are optional.
2. Requirements identified in the FCD for the Point-to-Point network topology are not applicable to an IP Modem. These capabilities will be provided by the MD-1366 Enhanced Bandwidth Efficient Modem (EBEM) being procured separately.
3. An IP Modem is not required to adhere to the Software Communications Architecture described in the FCD.

A.9.3 Requirements

A.9.3.1 Precedence

The commercial and DoD standards are applicable to the IP Modem to the extent specified herein. This specification shall take precedence in the event of a conflict between provisions of this document and corresponding provisions of the standards cited.

A.9.3.2 Digital Video Broadcasting – Return Channel via Satellite

The IP Modem shall implement the following standards-based air interface:

TAC-001960 [**Required**] The IP Modem shall use a return channel air interface that employs Multifrequency – Time Division Multiple Access (MF-TDMA) in a manner broadly similar to EN 301 790. The air interface shall, however, be substantially more capable of performing than EN 301 790, including the use of a better turbo code as well as additional modulation schemes (BPSK, 8PSK, spread-spectrum BPSK). The forward channel shall be compliant with DVB-S2 (EN 302 307).

TAC-001970 [**Required**] The IP Modem system shall be equipped with necessary timing and frequency generation functions sufficiently stable and accurate to support network requirements.

TAC-001980 [**Required**] The IP Modem shall accept reference timing and frequency signals available from its associated satellite terminal and use these signals as sources for generating internal operating frequencies and clocks.

TAC-001990 [**Required**] The IP Modem shall not transmit over the air any modem position and/or location information relative to any of the modems within the network.

TAC-002000 [**Required**] The IP Modem shall utilize a startup mechanism whereby it performs acquisition and logon without operator intervention using only information stored within the modem or obtained from the forward link carrier.

TAC-002010 [**Required**] Operator input of the Transmission Security (TRANSEC) passphrase shall be required at each startup. The IP Modem may also use an over-the-air authentication mechanism based on exchange of X.509 certificates over a PKI infrastructure. The IP modem should be certified according to FIPS 140-2.

A.9.3.2.1 Compliance With ETSI EN 301 790

TAC-002020 [**Required**] The IP Modem may support several burst payload size options, including choices that are identical or similar to the MPEG profile of DVB-RCS (EN 301 790). Aside from modulation and coding advantages addressed elsewhere, the IP Modem may offer features not included in the DVB-RCS MPEG profile. This includes in-band capacity requests for rapid reaction to changes in capacity demand. The IP Modem may use HDLC for IP packet encapsulation; this method has very low overhead.

A.9.3.2.2 Compliance With ETSI EN 302 307

TAC-002030 [**Required**] The IP Modem shall comply with the non-optional requirements of ETSI EN 302 307. The IP Modem shall comply with all "Professional Services" normative requirements of ETSI EN 302 307. Implementation of 32APSK is not required in the IP Modem. The use of "normal" frames is not required. Support for Transport Streams is not required if support for generic streams is provided.

A.9.3.3 Satellite Network Modem System (ISNMP)

TAC-002040 [**Required**] Network Management Interfaces: IP Modem products shall provide at least the following interface rates (other rates and IEEE standards may be provided as conditional interfaces):

a. 10 Mbps IAW IEEE 802.3i.

b. 100 Mbps IAW IEEE 802.3u.

TAC-002050 [**Required**] The IP Modem shall comply with the following sections and subsections of TIA/EIA 1073-000, 1, Section 4.1: Hub Spoke Topology.

A.9.3.4 Logon and Synchronization

TAC-002060 [**Required**] After failure, an IP Modem shall be able to logon to the satellite network in less than ninety (90) seconds.

TAC-002070 [**Required**] The IP Modem shall achieve synchronization and the ability to pass IP traffic bi-directionally within five (5) seconds after login.

TAC-002080 [**Required**] The IP modem shall automatically synchronize to the network timing reference after initial power-on and after loss of time synchronization.

TAC-002090 [**Required**] The IP Modem shall be able to self-correct timing to compensate for changes in satellite locations. This shall be accomplished without the input of satellite ephemeris data.

TAC-002100 [**Required**] The IP Modem shall synchronize its clock with the Network Timing Reference received on the forward link.

A.9.3.5 Network Requirements

A.9.3.5.1 LAN Interface

TAC-002110 [**Required**] IP Modem products shall provide a multiport managed Ethernet switch with a minimum of 8 10/100 Ethernet ports.

TAC-002120 [**Required**] The switch shall provide a high-speed switch fabric with support for 2048 MAC address entries with automatic learning and aging.

TAC-002130 [**Required**]The switch shall provide port-based VLAN (IEEE 802.1q) assignment and configuration.

TAC-002140 [**Required**] The switch shall support IEEE 802.1p.

TAC-002150 [**Required**] Each switch port shall be full duplex and shall support auto-negotiation (IEEE 802.3) and flow control (IEEE 802.3x).

TAC-002160 [**Required**] Spanning Tree IAW IEEE 802.1D.

TAC-002170 [**Required**] The IP Modem shall support all packet sizes from 64 to 1500 bytes on all interfaces.

A.9.3.5.1.1 IP Header and Payload Compression

TAC-002180 [**Required**] The IP Modem shall provide IP Header and Payload Compression [Transmission Control Protocol (TCP)/IP and Real Time Protocol (RTP)/User Datagram Protocol (UDP)/IP] for efficient bandwidth utilization in accordance with RFC 3759, RFC 4362, RFC 3173, and the IETF Draft document "draft-ietf-rohc-rfc4995."

A.9.3.5.1.2 IP Encapsulation

TAC-002190 IM019 [**Required**] The IP Modem shall provide Generic Stream Encapsulation (GSE) on the forward link. The IP Modem may alternatively provide other encapsulation, provided the functionality and performance is at least equivalent to GSE.

A.9.3.5.1.3 IP Packet Routing

TAC-002200 [**Required**] The IP Modem shall support the following IP dynamic routing protocols for IPv4 Unicast and multicast traffic:

a. Open Shortest Path First (OSPF), version 2 (OSPF v2) per RFC 2328.
b. Border Gateway Protocol (BGP), version 4 per RFC 4271.
c. Routing Information Protocol, version 2 (RIPv2) per RFC 2453.

TAC-002210 [**Required**] The IP Modem shall support DHCP.

TAC-002220 [**Required**] The IP Modem shall support a local DNS cache for IPv4 addresses.

TAC-002230 [**Required**] The IP Modem shall be capable of static routing of IPv4 and IPv6 multicast packets.

a. The IP Modem shall support local configuration of static IGMP joins and leaves to include IGMP v3 capability to filter by source address. This capability is intended to provide the IP Modem with the flexibility to manually add and delete individual multicast streams.

b. The IP Modem shall comply with standard IPv4 multicast routing protocols as defined by RFC 1112 and RFC 3376 (IGMPv3).

TAC-002240 [**Required**] The IP Modem shall support IPv4 Unicast static routing.

TAC-002250 [**Required**] The IP Modem shall be capable of distributing all static and dynamic routes, including changes.

TAC-002260 [**Required**] The metrics for the routing protocols shall be configurable to enable a routing policy such that the satellite link can act as the primary link, or a backup link, or possibly the primary in one direction and a backup in another direction.

A.9.3.5.1.4 IP Packet Forwarding

TAC-002270 [**Required**] The IP Modem shall support IP connectivity, be capable of extracting information from IP packet headers, and support transparent IPv4 packet forwarding for unicast and multicast services in accordance with Paragraph 7 of TIA-1073-001, SNMS Network Layer Standard.

A.9.3.5.1.5 IP Encapsulation

TAC-002280 [**Required**] The IP Modem shall support the following IP characteristics:

a. The IP Modem shall provide a Single Transport Stream or a single generic stream for the forward link carrier.

b. The IP Modem shall provide encapsulation of IP packets on the forward link that is compliant with MPE (EN 301 192), GSE (TS 102 606) or equivalent.

A.9.3.5.1.6 IPv6

TAC-002290 [**Required**] The IP Modem shall support the mandatory requirements of DoD IPv6 Standard Profiles for IPv6 Capable Products published in the DISR for the applicable equipment categories.

TAC-002300 [**Required**] The IP Modem shall support simultaneous, dual-stack, IPv4, and IPv6 packet processing.

TAC-002310 [**Required**] The IP Modem shall extract information from IPv6 packet headers and support transparent IPv6 packet forwarding for unicast and multicast services.

TAC-002320 [**Required**] The IP Modem shall support the following IP dynamic routing protocols for IPv6 unicast and multicast traffic:

a. OSPF, version 2 (OSPF v2) per RFC 2328.

b. BGP, version 4 (BGP-4), per RFC 4271.

c. Routing Information Protocol, next generation(ng) (IPv6) (RIPng), per RFC 2080.

TAC-002330 [**Required**] The IP Modem shall support DHCPv6 and DHCPv6 relay.

TAC-002340 [**Required**] The IP Modem shall support a local DNS cache for IPv6 addresses.

TAC-002350 [**Required**] The IP Modem shall support IPv6 Neighbor Discovery (ND).

A.9.3.5.2 Satellite Interface Requirements

TAC-002360 [**Required**] The IP Modem shall support Constant Coding and Modulation (CCM) and Adaptive Coding and Modulation (ACM) techniques compliant with EN 302 307.

TAC-002370 [**Required**] The IP Modem shall support Binary, Quadrature and Binary Phase Shift Keying (BPSK, QPSK, and 8PSK) modulation in the return channels. In addition, the IP Modem shall support Turbo Coding with a performance at least equivalent to that defined in EN 301 790. Implementation of Reed Solomon, Convolutional, and CRC Channel Coding is not required. The constellation for QPSK shall be as defined in ETSI EN 301 790 [2].

TAC-002380 [**Required**] The outbound/broadcast transmission rate shall be configurable for a minimum of 1 Mbps up to 45 Mbps.

TAC-002390 [**Required**] The IP Modem shall operate with earth terminals over one or any combination of C-, X-, Ku-, or Ka-band geosynchronous transponder satellite systems.

TAC-002400 [**Required**] The IP Modem shall accommodate Doppler effects of C-, X-, Ku-, or Ka-band geosynchronous satellites with orbital inclinations of up to seven (7) degrees.

TAC-002410 [**Required**] An IP Modem network shall operate on only one satellite at a time.

TAC-002420 [**Required**] An IP Modem network shall operate in X- and Ka-band simultaneously.

TAC-002430 [**Required**] The IP Modem shall support operation in a receive-only mode. In this mode of operation, the IP Modem shall operate without any communications to the distant end in both TRANSEC enabled or disabled modes. This mode shall require no transmission by the IP Modem nor any type of network log-on or authentication.

TAC-002440 [**Required**] The IP Modem shall use a dynamic MF-TDMA technique and shall support frequency hopping between carriers with different symbol rate, coding rate and modulation scheme. The burst payload size of all traffic time slots accessed by an IP modem in a logon session shall be the same.

A.9.3.5.2.1 Forward Link Modulation and Coding Rates

TAC-002450 [**Required**] The modulation and forward error correction (FEC) coding formats implemented in the forward channel shall be compliant with the requirements of EN 302 307 including the following:

a. QPSK modulation with FEC rates of 1/4, 1/3, 2/5, 1/2, 3/5, 2/3, 3/4, 4/5, 5/6, and 8/9.

b. 8PSK modulation with FEC rates of 3/5, 2/3, 3/4, 5/6, and 8/9.

c. 16APSK modulation with FEC rates of 2/3, 3/4, 4/5, 5/6, and 8/9.

A.9.3.5.2.2 DVB Compliance

TAC-002460 [**Required**] The IP Modem shall provide functionality and performance at least equivalent to the Minimum Compliance Requirements under the "MPEG2 DVB-S2" profile of ETSI EN 301 790, with the exception of specific exclusions as specified in the present document.

A.9.3.5.2.3 Transmission

TAC-002470 [**Required**] The outbound/broadcast transmission rate shall be configurable for a minimum of 1 Msps.

TAC-002480 [**Required**] The IP Modem forward link error performance shall be compliant with EN 302 307, Paragraph 6 with 0.5 dB of degradation for QPSK and 0.9 dB of degradation for higher order modes (in IF loop back mode, FECFRAME (16, 200 bits) and with 0.20 roll-off. This includes allowance for the difference in FECFRAME size.

TAC-002490 [**Required**] The IP Modem return link error performance shall be compliant with Table A.9-1, Turbo Code Es/No Performance (170-byte packet) at Quasi Error Free PER = 10-5 (IF loop, AWGN channel), in IF loopback mode and with 0.20 roll-off. This table provides a threshold Es/No specification for a range of spectral efficiencies, expressed as FEC payload bits per data-carrying symbol. Recognizing that each proposed Turbo codec may have configurable FEC rate options that vary slightly, each vendor shall support an FEC rate with a threshold Es/No matched with the appropriate range. A minimum of three configurable FEC rate options shall be supported that offer flexibility in the tradeoff between power and bandwidth.

Table A.9-1. Turbo Code Es/No Performance (170-byte packet) at Quasi Error Free PER = 10-5 (IF loop, AWGN channel)]

SPECTRAL EFFICIENCY (BITS/SYMBOL)	THRESHOLD ES/N0 (DB)
< 0.500	0.4
0.501 to 0.600	1.5
0.601 to 0.700	2.0
0.701 to 0.800	2.3

SPECTRAL EFFICIENCY (BITS/SYMBOL)	THRESHOLD ES/N0 (DB)
0.801 to 0.800	2.8
0.901 to 1.000	3.5
1.001 to 1.100	4.1
1.101 to 1.200	4.8
1.201 to 1.300	5.4
1.301 to 1.400	6.0
1.401 to 1.500	6.8
1.501 to 1.600	8.4
1.601 to 1.700	8.7
1.701 to 1.800	9.3
1.801 to 1.900	10.0
1.901 to 2.000	10.6
2.001 to 2.100	11.5
2.101 to 2.200	12.7

A.9.3.5.2.4 Variable Coding and Modulation (VCM)

The IP Modem control and management system shall provide Variable Coding and Modulation (VCM) techniques compliant with EN 302 307. For the Forward Link TDM broadcast, the DVB-S2 Modulator shall support Frame-to-Frame dynamic switching between Mod Codes to accommodate different size broadcast receivers on the same broadcast. The control interface for this switching shall provide for a means of traffic differentiation (such as by destination IP/multicast address) to allow external selection of modulation and code rate, and shall be open and documented.

TAC-002500 [**Required**] The IP Modem shall comply with the IF interface and frequency requirements specified in Table A.9-2, IF Interface Requirements, and Table A.9-3, IP Intermittent Frequency Requirements.

Table A.9-2. IF Interface Requirements

PARAMETER	REQUIREMENT
Input and output independence	Input and output parameters shall be independently settable
IF Frequency	L-Band.
IF Output Frequency Setability	1 kHz steps
Hub IF Output Frequency Stability (internal reference)	1 x 10E-8 per day
Hub IF Output Frequency Accuracy	1 x 10E-7 at 1 hr after internal reference startup
IP Modem IF Output Frequency Stability	6 x 1E-8 after achieving downstream NCR lock
IF Output Spectral Shape	As specified in Figure X.X.3.5-1

PARAMETER	REQUIREMENT
Spectral Inversion	Modulator output spectrum shall not be inverted
IF Output Power Level	At minimum, 0 to -25 dBm in <0.5dB increments
IF Output Impedance	50 ohms or 75 Ohms
IF Input Desired Carrier Power	-55 to -10 dBm
IF Input Impedance	50 ohms
IF Input Doppler Mitigation	As specified in Paragraph X.X.3.5.2.5
IF Output Spurious Emissions	IF Output Spurious Emissions shall be –less than -50 dBc for information rates >2048 kbps and less than -40 dBc for information rates ≤2048 kbps
IF Output Harmonics	IF Output Harmonics shall be less than or equal to -50 dBc
LEGEND:	
dB decibel	IF Intermediate Frequency
dBc decibel (referenced to carrier)	kHz Kilohertz
dBm decibel (referenced to milliwatts)	

Table A.9-3. IP Intermittent Frequency Requirements

CARRIER DEVICE	INTERMEDIATE FREQUENCY
Satellite	70 MHz, 950-2050
Terrestrial Microwave	250 MHz, 70 MHz or 75 MHz
FM Radio	262 kHz, 455 kHz, 1.6 MHz, 5.5 MHz, 10.7 MHz, 10.8 MHz, 11.2 MHz, 11.7 MHz, 11.8 MHz, 21.4 MHz, 75 MHz and 98 MHz
LEGEND:	
FM Frequency Modulation	kHz Kilohertz
IP Internet Protocol	MHz Megahertz

A.9.3.5.2.5 Doppler Performance

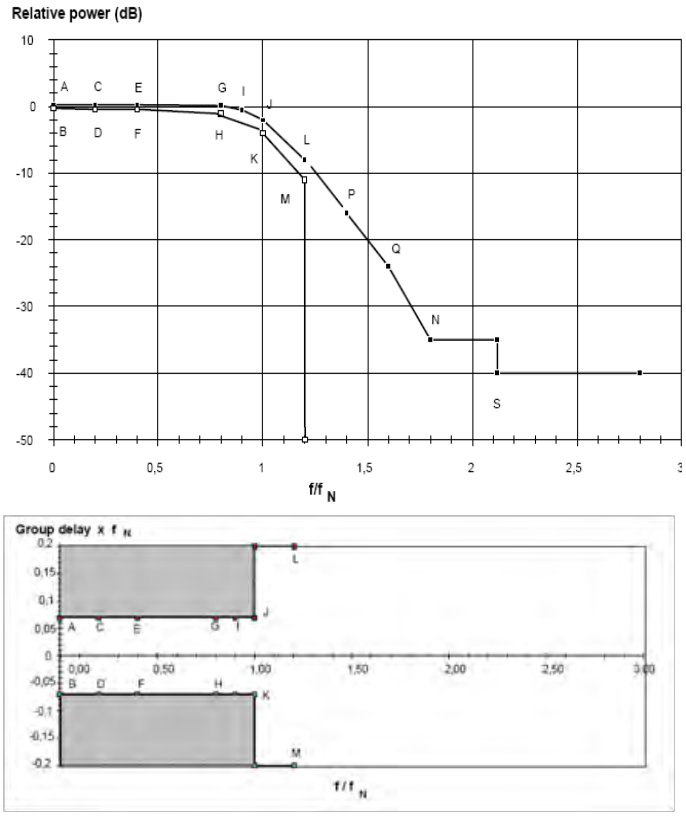
TAC-002510 [**Required**] The IP modem shall maintain its specified performance under all of the satellite Doppler conditions listed in Table A.9-4, Satellite Doppler Conditions, up to seven (7) degrees of orbital inclination:

Table A.9-4. Satellite Doppler Conditions

PARAMETER	C-BAND	X-BAND	KU-BAND	KA-BAND
Doppler Shift in Hz	± 2,475	± 3,535	± 6,045	± 11,810
Doppler Rate of Change in Hz/sec	± 226	± 270	± 490	± 1,046
Doppler Acceleration in Hz/sec^2	± 243	± 290	± 526	± 1,124
LEGEND:				
Hz Hertz			sec second	

A.9.3.5.2.6 Spectral Confinement

TAC-002520 [**Required**] The IP Modem modulator output signal spectral confinement, group delay, and demodulator input filter mask shall be as specified in the spectral density limit mask and group delay chart shown in Figure A.9-1, Modulator Signal Spectral Density Limit Mask and Group Delay.



POINT	FREQUENCY FOR □ = 0.35	RELATIVE POWER (DB)	GROUP DELAY
A	0.0 f_N	+0.25	+0.07 / f_N
B	0.0 f_N	-0.25	-0.07 / f_N
C	0.2 f_N	+0.25	+0.07 / f_N
D	0.2 f_N	-0.40	-0.07 / f_N
E	0.4 f_N	+0.25	+0.07 / f_N
F	0.4 f_N	-0.40	-0.07 / f_N
G	0.8 f_N	+ .15	+0.07 / f_N
H	0.8 f_N	-1.10	-0.07 / f_N
I	0.9 f_N	-0.50	+0.07 / f_N
J	1.0 f_N	-2.00	+0.07 / f_N
K	1.0 f_N	-4.00	-0.07 / f_N
L	1.2 f_N	-8.00	-
M	1.2 f_N	-11.00	-
N	1.8 f_N	-35.00	-
P	1.4 f_N	-16.00	-
Q	1.6 f_N	-24.00	-
S	2.12 f_N	-40.00	-

Legend:
dB decibel FN Frequency

Figure A.9-1. Modulator Signal Spectral Density Limit Mask and Group Delay

TAC-002530 [**Required**] IP Modem products shall transmit in a single or range of frequencies as listed in Figure A.9-1, Modulator Signal Spectral Density Limit Mask and Group Delay.

A.9.3.5.2.7 IP Encapsulation

TAC-002540 [**Required**] The IP Modem shall support the following IP characteristics:

a. The IP Modem shall provide a Single Transport Stream or a single generic stream for the forward link carrier.

b. The IP Modem shall provide encapsulation of IP packets on the forward link that is compliant with MPE (EN 301 192), GSE (TS 102 606) or equivalent.

A.9.3.5.2.8 IPv6

TAC-002550 [**Required**] The IP Modem shall support the mandatory requirements of DoD IPv6 Standard Profiles for IPv6 Capable Products published in the DISR for the applicable equipment categories.

TAC-002560 [**Required**] The IP Modem shall support simultaneous, dual-stack, IPv4 and IPv6 packet processing

TAC-002570 [**Required**] The IP Modem shall extract information from IPv6 packet headers and support transparent IPv6 packet forwarding for unicast and multicast services.

TAC-002580 [**Required**] The IP Modem shall support the following IP dynamic routing protocols for IPv6 unicast and multicast traffic.

a. Open Shortest Path First, Version 2 (OSPF v2) per RFC 2328.
b. Border Gateway Protocol version 4 (BGP-4), per RFC 4271.
c. Routing Information Protocol, next generation(ng) (IPv6) (RIPng) per RFC 2080.

TAC-002590 [**Required**] The IP Modem shall support DHCPv6 and DHCPv6 relay.

TAC-002600 [**Required**] The IP Modem shall support a local DNS cache for IPv6 addresses.

TAC-002610 [**Required**] The IP Modem shall support IPv6 Neighbor Discovery (ND).

A.9.3.6 Assured Service Requirements

A.9.3.6.1 Class of Service

The IP Modem shall manage communications resources to satisfy its traffic and QoS requirements. Resources shall be allocated using a per network QoS strategy. Higher priority traffic classes shall be allocated before lower priority traffic classes within the defined QoS policy.

TAC-002620 [**Required**] The IP Modem shall support Mechanism Message Authentication Code (MAC) Messages or equivalent as required by the non-optional requirements of EN 301 790.

TAC-002630 [**Conditional**] The IP Modem may comply with non-optional MAC Message requirements of EN 301 790 including the following methods:

- Mini-slot Method.
- Data Unit Labeling Method.

TAC-002640 [**Required**] The IP Modem shall be capable configuring VLAN IDs (VIDs). VIDs on an ingress port shall be configurable to any of the 4094 values (except 0 and 4095 are reserved). Each VLAN shall support independently routable IP address spaces.

TAC-002650 [**Required**] The IP modem shall be able to support up to 7 VLANs simultaneously.

TAC-002660 [**Required**] The IP Modem shall be capable supporting port-based VLANs, and VLANs using 802.1q tagged packets at the modem Ethernet interface.

A.9.3.6.2 QoS

IP Modem products shall support configurable traffic classification and QoS as follows:

TAC-002670 [**Required**] The IP Modem shall support traffic classification for the purpose of QoS assignment based on DSCP as defined in RFC 2474/2475, source IP address, destination IP address, destination port, and VLAN.

TAC-002680 [**Required**] For each traffic classification, the IP Modem shall support priority levels and weighted fair queuing with configurable parameters.

TAC-002690 [**Required**] The IP Modem shall be capable of accepting any packet tagged with a DSCP (0-63) on an ingress port and reassign that packet to any new DSCP value (0-63). Default DSCPs are provided in Table A.9-5.

Table A.9-5. Default DSCPs

	AGGREGATE SERVICE CLASS	GRANULAR SERVICE CLASS	DEFAULT DSCPS		
			BASE 2	BASE 10	BASE 16[3]
1	Control	Network Control	110 000-111 000	48-56	0xC0 – 0E0
2	Inelastic/Real Time	User Signaling[1]	101 000-101 111	40-47	0xA0 – 0xBC
		Circuit Emulation[1]			
		Short Messages[1]			
		Voice[2]			
		Video/VTC	100 000-100 111	32-39	0x80 – 0x9C
		Streaming	011 000-011 111	24-31	0x60 – 0x7C
3	Preferred Elastic	Interactive Transactions	010 000-010 111	16-32	0x40 – 0x5C
		File Transfers	001 000-001 111	8-15	0x20 – 0x3C
4	Elastic	Default	000 000-000 111	0-7	0x0 – 0x1C

Notes:
1. All user signaling (voice and video) may be grouped into this granular service class. User signaling, circuit emulation, and short messages may use the same DSCP.
2. Voice traffic must be differentiated with a different DSCP from user signaling, circuit emulation, and short messages.
3. DSCP Hexadecimal (Base 16) values assume last two bits of the 8 bit field to be 00.

Specific DSCPs for each precedence level are contained in UCR Section 6, Network Infrastructure End-to-End Performance Requirements.

Definitions of granular service classes are provided in UCR Section 6, Network infrastructure End-to-End Performance Requirements.

	AGGREGATE SERVICE CLASS	GRANULAR SERVICE CLASS	DEFAULT DSCPS		
			BASE 2	BASE 10	BASE 16[3]

LEGEND:

DSCP	Differentiated Services Code Point	VTC	Video Teleconferencing
UCR	Unified Capabilities Requirements		

TAC-002700 [**Required**] The QoS mechanism shall support at least four traffic classes: Control & Signaling; Real-time Streaming; Preferred Data; Best Effort.

TAC-002710 [**Required**] The IP Modem shall be capable of accepting any packet tagged with a DSCP (0-63) on an ingress port and assign that packet to a QoS behavior listed in UCR 2008, Section 5.3.1.3.6, Quality of Service Features.

TAC-002720 [**Required**] The IP Modem shall allow configuration and mapping of user traffic DSCPs to traffic classes for each network based on Per Hop Behavior (PHB).

TAC-002730 [**Required**] The modem shall be configurable so that the Control and Real Time traffic shall be treated as Priority Traffic and have a PHB served through a Priority Queuing mechanism.

TAC-002740 [**Required**] The Streaming and Preferred Data traffic shall be treated as higher service classes than Best Effort with a PHB serviced through a queuing mechanism that can guarantee delivery of this traffic up to a configured maximum.

TAC-002750 [**Required**] The IP Modem shall be configurable to allocate for each of the service classes:

a. A percent of the configured network information rate of the air interface or a percent of the minimum/maximum user information rate per remote.

b. To prevent starvation of the Best Effort and other class traffic queues, the IP Modem shall police Priority traffic and Preferred traffic such that it is not permitted to exceed its allocated rate.

TAC-002760 [**Required**] The IP Modem shall ensure that the DSCP values of IP datagrams appear the same on the terrestrial interface at the egress of the IP Modem network as they were at the ingress of the datagrams on the terrestrial interface of the IP Modem network.

TAC-002770 [**Required**] The Forward Link encapsulators shall have the capability to provide guaranteed bandwidth on the FL TDM per IP Input (Multicast destination Address, IP Unicast destination range, etc).

TAC-002780 [**Required**] The IP Modem shall support the following (as a minimum) Capacity Request categories, as defined by EN 301 790 for Return Channel via Satellite:

a. Absolute Volume Based Dynamic Capacity (AVBDC).

b. Free Capacity Assignment (FCA).

TAC-002790 [**Required**] The IP Modem may optionally support the following Capacity Request categories, as defined by EN 301 790 for Return Channel via Satellite:

a. Rate Based Dynamic Capacity (RBDC).

b. Committed Rate Assignment (CRA).

TAC-002800 [**Required**] The IP Modem shall provide configuration support to map resources at the Media Access Control (MAC) layer (capacity categories) from Layer 3 (PHBs, service classes or IP 5-tuple).

TAC-002810 [**Required**] The IP Modem must be able to support the prioritization of aggregate service classes described in Table A.9-6, Traffic Prioritizations. Traffic Prioritizations Prioritized service classes shall be queued according to UCR 2008, Section 7.2.1.6, Quality of Service Features.

Table A.9-6. Traffic Prioritizations

AGGREGATE SERVICE CLASS		GRANULAR SERVICE CLASS	PRIORITY
1	Control	Network Control	1
2	Inelastic/ Real-Time	User Signaling	2
		Circuit Emulation	2
		Short Messages	2
		Voice	3
		Video/VTC	4
		Streaming	5
3	Preferred Elastic	Interactive Transactions and OA&M	6
		File Transfers and OA&M	7
4	Elastic	Default	Best Effort
LEGEND:			
OA&M Operations, Administration, and Management VTC Video Teleconferencing			

TAC-002820 [**Conditional**] If provided, then the following CoS requirements apply:

a. The IP Modem shall be capable of accepting any frame tagged with a user priority (0-7) on an ingress port and assign that frame to a QoS behavior listed in UCR 2013, Section 7.2.1.6, Quality of Service Features.

b. The IP Modem shall be capable of accepting any frame tagged with a user priority (0-7) on an ingress port and reassign that frame to any new user priority value (0-7).

TAC-002830 [**Required**] IP Modem products may support the 3-bit user priority field of the IEEE 802.1Q 2-byte Tag Control Information (TCI) field (see Figure UCR 7.2-1, IEEE 802.1Q Tagged Frame for Ethernet, and UCR Figure 7.2-2, TCI Field Description). The default values are provided in Table 7.2-1 of the 802.1Q Default Values.

c. Provide a minimum of four (4) queues (see Figure 7.2-6).

d. Assign any "tagged" session to any of the queues.

e. Support Differentiated Services (DiffServ) per hop behaviors (PHBs) per RFCs 2474, 2494, 2597, 2598, and 3246 as listed in Figure 7.2-6

f. Support the following requirements:

(1) Weighted Fair Queuing (WFQ) IAW RFC 3662.

(2) Priority Queuing (PQ) IAW RFC 1046.

(3) Class-Based WFQ IAW RFC 3366.

g. All queues shall be capable of having a bandwidth (BW) assigned (i.e., queue 1: 200 kbps, queue 2: 500 kbps, etc.) or percentage of traffic (queue 1: 25 percent, queue 2: -25 percent, etc.).

A.9.3.6.3 QoS Performance and Delay

TAC-002840 [**Required**] The IP Total Delay (IPTD), Inter-Packet Delay Variation (IPDV) and IP Packet Loss Ratio (IPLR) for the IP Modem shall meet the performance parameters as specified in Table A.9-. These numbers are inclusive of encryption enabled and satellite link best case round-trip propagation delay of 472 ms. The system loading shall be configured such that the outbound channel is at least 50% utilized, and the inbound channel is at least 50% utilized. The measurements shall be taken while the system is in steady state. The IPTD is a combination of modem processing delay plus propagation delay. The IPTD is measured from the IP stream entering the IP Modem from the LAN interface to the IP stream exiting the paired IP Modem. IPDV is measured one-way from IP Modem to IP Modem. Packet Loss Ratio is the ratio of packets received to packets sent from the IP Modem. Performance thresholds are listed in Table A.9-7, Performance Thresholds for IP Modem Satellite Networks.

Table A.9-7. Performance Thresholds for IP Modem Satellite Networks

TRAFFIC CLASS	IP TOTAL DELAY	RMS JITTER	PACKET LOSS RATIO
Control & Signaling	300 ms	25 ms	<0.01%
Real Time	300 ms	25 ms	<0.015%
Preferred Data	375 ms	NS	<0.01%
Best Effort	NS	NS	NS
Note: Measured without congestion			

TRAFFIC CLASS	IP TOTAL DELAY	RMS JITTER	PACKET LOSS RATIO
LEGEND:			
ms Millisecond		VTC Video Teleconferencing	
NS Not Specified			

A.9.3.7 Transmission Security

TAC-002850 [**Conditional**] All information routed to the satellite (via the IF interface) must be protected with TRANSEC when interoperability compatibility exists with this standard.

A.9.3.8 Network Management

A.9.3.8.1 Network Management – IP Modem – Local Operator Functions and Interfaces

TAC-002860 [**Required**] At a minimum, the IP Modem shall provide means for a local (connecting from LAN interface) operator to execute the following:

- Provide an initial configuration when necessary.
- Upgrade the modem's software and firmware.
    a. Access a local web interface provided by the terminal to monitor performance parameters such as IP statistics, Tx/Rx signal power, latency, routing table information, faults, alarms and system logging information.
    b. Access a local web interface to provide TRANSEC initiation and management

The local web interface shall support operator functions using an external personal computer or laptop computer, hereafter termed the IP Modem Local Management Computer (LMC).

TAC-002870 [**Required**] The IP Modem shall connect to the LMC via an Ethernet or serial interface. The IP Modem shall be compatible with standard Secure Shell, Secure HTTP or SNMP and may also require the use of contractor-provided software.

TAC-002880 [**Required**] Front panel controls and indicators shall be provided, as necessary, to implement required TRANSEC Passphrase entry, loading of seed key and TRANSEC Bypass activation. Alternative solutions not requiring front panel controls to accomplish these same functions are acceptable.

A.9.3.9 Network Management – Remote Operator Functions and Interfaces

TAC-002890 [**Required**] The IP Modem shall provide a mechanism for the operator to execute all necessary NMS functions in a secure fashion utilizing the provided systems over-the-air

(satellite link) interface as well as supporting the local operator as discussed in 9.3.8.1 above. As a minimum, IP Modem shall support the following network management functions:

TAC-002900 [**Required**] The IP Modem products shall support the following network control and monitoring features via a secure protocol:

h. Remote update of IP Modem configuration.

i. Remote update of IP Modem software and firmware.

j. Remote status monitoring of critical IP Modem parameters.

TAC-002910 [**Required**] The IP Modem shall provide a separate logical communications network for exchange of network management and control information between the IP Modem and a centralized network management system.

TAC-002920 [**Required**] The IP Modem will be capable of performance management, including the ability to measure, report, analyze, and adjust the IP Modem performance including but not limited to throughput, bandwidth utilization, network utilization, availability, latency, and packet error rate (PER).

TAC-002930 [**Required**] The IP Modem shall be capable of performance management functionality per network and per QoS traffic class.

TAC-002940 [**Required**] The IP Modem shall calculate and report the Information/Traffic Throughput Rate, which is the actual user traffic traversing the IP Modem network, for both outbound and inbound links by taking into consideration overhead factors.

TAC-002950 [**Required**] The IP Modem will provide fault management capabilities, including the ability to detect, log, isolate, and respond to fault conditions at the IP modem.

TAC-002960 [**Required**] The IP Modem will have the ability to perform security key distribution and to control access of the IP Modem to network resources and protect against hackers, unauthorized users, and physical or electronic sabotage.

TAC-002970 [**Required**] The IP Modem shall allow network administrators to control what each individual authorized user can (and cannot) do with the system.

TAC-002980 [**Required**] The IP Modem shall have the ability to control and monitor Network TRANSEC functions, including key management.

A.9.3.9.1 Demand Assigned Multiple Access (DAMA)

TAC-002990 [**Required**] The IP Modem shall support DAMA for MF-TDMA channel access.

TAC-003000 [**Required**] The IP Modem shall support a DAMA signaling protocol for communications between IP Modems. At a minimum, the DAMA signaling protocol shall

provide efficient control and management information exchanges to enable the following functions:

a. IP Modem entry to the network.

b. Communications resource request and allocation, including priority and QoS traffic.

c. IP Modem exit from the network.

d. IP Modem status polling and reporting.

e. IP Modem remote configuration.

A.9.3.9.2 Network Management System Functions

TAC-003010 [**Required**] The IP Modem shall provide a mechanism for the operator to execute all necessary functions for the IP Modem at the terminal/site. As a minimum, IP Modem shall support the following network management functions:

f. Performance management, including the ability to measure, report, analyze, and adjust the IP Modem performance including but not limited to throughput, bandwidth utilization, network utilization, availability, and latency. Performance management functionality shall be available per network and per QoS traffic class. The IP Modem shall calculate and report the Information/Traffic Throughput Rate which is the actual user traffic traversing the IP Modem network for both outbound and inbound links by taking into consideration overhead factors.

g. Fault management, including the ability to detect, log, isolate, and respond to fault conditions at the IP Modem.

A.9.3.10 Remote Control and Network Management

TAC-003020 [**Required**] The IP Modem software and standard Microsoft Windows features (Secure HTTP and Secure Shell), Linux or Unix shall provide management functions necessary to remotely manage the IP Modem. The IP Modem shall support SNMPv1 and SNMPv2, at a minimum.

a. The IP Modem interface shall be used by the IP Modem to send aggregate performance notifications.

b. The IP Modem shall support SNMP network discovery by allowing IP Modem to collect status' of other IP Modems in the network.

A.9.3.11 Hardware Requirements

A.9.3.11.1 Hardware

TAC-003030 [**Required**] The IP Modem hardware components shall meet the requirements outlined in Table A.9-8, Hardware Requirements.

Table A.9-8. Hardware Requirements

PARAMETER		REQUIREMENT
a.	Packaging	Chassis-type components shall be mountable in a standard 19-inch rack
b.	Cooling	Shall not require external forced air cooling. The IP modem may provide its own forced air cooling.
c.	Electro-Magnetic Interference (EMI)	FCC Rules Part 15 (47CFR15, Sections 47CFR15.107 and 47CFR15.109 for Class B devices
d.	EMC Susceptibility	FCC Rules Part 15 for Class B devices
e.	Reliability	MTBF ≥ 40,000 hours in a Ground Fixed Environment using Telcordia SR-332 prediction
f.	Maintainability	MTTR ≤ 15 min at organizational level
g.	System Availability	0.9999
h.	AC Prime Power	Selectable 100-240V at 50-60Hz
i.	High Temperature, Operating (Sea Level)	60ºC (140ºF)
j.	High Temperature, Non-operating	60ºC (140ºF)
k.	Low Temperature, Operating	-30ºC (-22ºF)
l.	Low Temperature, Non-operating	-40ºC (-40ºF)
m.	Humidity, Operating	≤ 92 %, non-condensing
n.	Humidity, Transportation and Storage	100 %, non-condensing
o.	Internal Frequency Reference	Operable without external standard while meeting frequency stability requirements
p.	External Frequency Reference Input Interface	10 MHz from site frequency standard. Frequency reference should not be required for operation.
q.	10 MHz or 50 MHz (configurable) Frequency Reference Output Interface (-5 to +5 dBm at input port)	For associated VSAT block up converter and LNB
r.	24 VDC (4-5A max current) Power Output Interface	For associated VSAT block up converter
s.	13 and 18 VDC (-500mA max current) Power Output Interface, Switchable	For associated VSAT LNB
t.	Control Interface	Open AMIP v 1.7 for mobility
u.	Built In Diagnostics	As required to support MTTR

PARAMETER		REQUIREMENT	
LEGEND:			
A	Amp	mA	Milliamp
C	Celsius	MHz	Megahertz
dBM	Decibel (referenced in milliwatts)	MTBF	Mean Time Between Failures
EMI	Electromagnetic Interference	MTTR	Mean Time To Recover
F	Fahrenheit	SNMP	Simple Network Management Protocol
FCC	Federal Communications Commission	V	Volt
Hz	Hertz	VSAT	Very Small Aperture Terminal
LNB	Low-Noise Block Converter	VDC	Volts Direct Current

A.9.3.11.2 IP Modem Front Panel

The IP Modem shall allow the operator to execute the following functions using the front panel:

TAC-003040 [**Required**] The IP Modem front panel shall be equipped with a Key Fill Connector compatible with the AN/PYQ-10 Simple Key Loader (SKL) and capable of supporting the Seedkey loading functions specified in Paragraph C.5 of the Security Addendum. This Key Fill Connector interface shall be configured as specified in NSA Drawing ON241774. Alternatively, the IP modem may provide for secure over the air key distribution for TRANSEC without the need for an external key fill.

TAC-003050 [**Required**] The IP Modem front panel shall be equipped with the necessary controls and indicators to implement a TRANSEC Bypass, if the host network allows non TRANSEC terminals. Control of the TRANSEC bypass may alternatively be done through the front panel or through the Local Management Computer.

TAC-003060 [**Required**] If the IP modem requires a passphrase, the IP Modem front panel shall include a keypad and alphanumeric display for TRANSEC Passphrase entry. Alternately, passphrase entry may be done through the Local Management Computer.

TAC-003070 [**Required**] The IP Modem front panel shall be equipped with other controls and indicators for operation and maintenance functions required by the contractor's design including but not limited to power-on indicator, receive lock indicator, and logged on indicator.

A.9.3.11.3 Rear Panel

TAC-003080 [**Required**] The IP Modem chassis rear panel, as a minimum, shall include the following rear panel connectors and other features.

a. AC power.

b. Grounding stud.

c. IF input (if not included in the front panel).

d. IF output (if not included in the front panel).

e. Ethernet network interface for user traffic (if not included in the front panel).

f. Ethernet or serial interface compatible with standard personal/laptop computer (if not included in the front panel).

A.9.3.11.4 Human Engineering

TAC-003090 [**Required**] IP Modem equipment shall comply with the following Human Engineering requirements:

Front panel controls, displays, marking, coding, labeling, and arrangement schemes shall be uniform for common functions. The allocation of operational and maintenance functions to personnel and equipment shall be consistent with required safety, reliability, personnel skill levels, functional precision, and time constraints necessary for mission-effective IP Modem performance.

a. All front panel controls, displays, indicators, and associated labels shall be legible and easily visible in rooms with a general lighting level of 10 foot-candles without any aid over a ±30 degree viewing angle in the normal operating configuration.

b. The AC power on/off switches on the IP Modem rack(s) and chassis front panels shall be protected with a guard to prevent accidental activation.

A.9.3.11.5 Materials

1. Insofar as possible, nonflammable material shall be used.
2. Parts and materials that are not nutrients for fungus and are resistant to moisture shall be used in the IP Modem equipment whenever possible. Where use of fungi-nutrient materials is essential to the design, the materials shall be treated with fungicide agent.
3. The materials listed below shall not be used in the IP Modem equipment without written consent from the procuring agency:
   a. Asbestos: asbestos compounds and asbestos filled compounds.
   b. Cadmium.
   c. Carcinogens.
   d. Chlorofluorocarbons (CFCs), that is, Freon.
   e. Lithium and lithium compounds (except commercially-available batteries).
   f. Magnesium or magnesium alloys.
   g. Mercury or its compounds and amalgams.
   h. Polycarbonate Biphenyl (PCB).

i. Polyvinyl Chloride (PVC), except when used as component leads and cable insulation or jackets in NDIs.

j. Zinc or zinc alloys unless otherwise specified.

A.9.3.11.6 Nameplates and Product Marking

TAC-003100 [**Required**] A permanent nameplate that displays the information specified in the Statement of Work shall be affixed to the IP Modem equipment front panel(s).

TAC-003110 [**Required**] All IP Modem hardware components shall comply with the Unique Identification (UID) requirements of MIL-STD-130L.

A.9.3.11.7 Safety

TAC-003120 [**Required**] The IP Modem system shall be designed so that under all operating conditions specified herein (installation, operation, and maintenance) and under a likely fault condition (including human error), it protects against the risk of electric shock and other hazards.

k. Equipment shall meet the applicable requirements of the NFPA 70-93.

l. Equipment leakage current to ground shall not exceed 3.6 ma when tested in accordance with ANSI C101.1.

A.9.3.12 Software Requirements

A.9.3.12.1 Reprogrammability

TAC-003130 [**Required**] The IP Modem shall be able to receive software/firmware upgrades through unicast or multicast distribution over the air, or through a local Ethernet connection. The modem shall also be reconfigurable over the air.

A.9.3.12.2 IP Modem Options

TAC-003140 [**Required**] The IP Modem shall be equipped to enable optional capabilities to be implemented relying on software/firmware upgrades as much as possible.

A.9.3.12.3 Local Management Computer (LMC) Software

TAC-003150 [**Required**] The IP Modem application software necessary to provide functionality shall be supplied on a CD-ROM and be capable of operating on any commercial personal computer or laptop computer running Microsoft Windows or LINUX operating systems, unless the application is a standard web browser.

TAC-003160 [**Required**] Password authentication and connection encryption are required for the LMC to access the IP modem.

A.9.3.13 Information Assurance Requirements

TAC-003170 [**Required**] IP Modem products shall meet the security protocol requirements listed in UCR 2013, Section 4, Information Assurance Requirements, or FIPS 140-2.

TAC-003180 [**Required**] All user communications traffic routed to the IP Modem network interface will be either externally encrypted by HAIPE, or unencrypted SBU or lower traffic, and considered SBU.

A.9.3.14 Product Certification and Requirements Summary

TAC-003190 [**Required**] The contractor will be responsible for obtaining a series of certifications required by the Government prior to receiving a Unified Capabilities Interoperability certification. Certifications are required in the following areas.

m. Compliance with MILSATCOM criteria for operation on DSCS, GBS, and WGS.

n. Compliance with DVB-S2 standard (with TRANSEC bypassed).

o. NIST compliance with FIPS 140-2, Level 2 for TRANSEC.

p. Compliance with Information Assurance requirements specified in Section A.9.3.13, Information Assurance Requirements.

TAC-003200 [**Required**] Table A.9-9, is taken from Section7.2.3 of the UCR and summarizes product requirements and provides references to the governing documents.

Table A.9-9. Core, Distribution, and Access Product Requirements Summary

RQMTS	FEATURES	REFERENCES	APPLICABILITY
Physical Ports	Serial Port	EIA/TIA	R
	100Base T UTP	IEEE 802.3i	C
	100Base –FX	IEEE 802.3u	R
	1000Base-T UTP	IEEE 802.3u	C
	1000Base X Fiber	IEEE 802.3z	C
	10GBase-X	IEEE 802.3ae	C
Port Parameters	Auto-Negotiation	IEEE 802.3	R
	Force Mode	IEEE 802.3	R
	Flow Control	IEEE 802.3x	R
	Filtering	RFC 1812	R
	Link Aggregation	IEEE 802.3ad	C
	Spanning Tree Protocol	IEEE 802.1D	R
	Multiple Spanning Tree Protocol	IEEE 802.1s	C
	Rapid Reconfiguration of Spanning Tree	IEEE 802.1w	C
	Port Based Access Control	IEEE 802.1x 1	R

RQMTS	FEATURES	REFERENCES	APPLICABILITY
Traffic Prioritization	CoS Traffic Classes	IEEE 802.1D/Q	C
	DSCP	RFC 2474	R
VLANs	Port based	IEEE 802.1Q	R
	MAC based	IEEE 802.1Q	C
	Protocol based	IEEE 802.1Q	R
IPv4 Protocols	IPv4 requirements are contained within the DISR on-line RTS profiles for Core, Distribution, and Access products	DISR	R
IPv6 Protocols	See IPv6 profiles contained in the DISR	DISR	R
QoS	DiffServ PHBs	RFCs 3246, 2597	R
	Minimum 4 traffic queues	DoD CoS/QoS WG	R
	FIFO	RFC 3670	C
	WFQ	RFC 3662	R
	CQ	RFC 3670	C
	PQ	RFC 1046	C
	CB-WFQ	RFC 3366	C
Security	Security requirements are contained in the IA portion of the document		R

Notes:
1. Only between end-user and product; not trunks.
2. One of these queuing mechanisms is required to implement EF PHB.

LEGEND:

C	Conditional	IPv6	Internet Protocol version 6
CB-WFQ	Class-Based Weighted Fair Queuing	MAC	Media Access Control
CoS	Class of Service	PHB	Per-Hop Behavior
CQ	Custom Queuing	PQ	Priority Queuing
DiffServ	Differentiated Services	R	Required
DISR	DoD IT Standards Registry	RFC	Request for Comment
DoD	Department of Defense	RMON	Remote Monitoring
EF	Expedited Forwarding	RTS	Real-Time Services
EIA	Electronic Industries Alliance	TIA	Telecommunications Industry Association
FIFO	First-in First-out	UTP	Unshielded Twisted Pair
IEEE	Institute of Electrical and Electronics Engineers	VLAN	Virtual Local Area Network
IPv4	Internet Protocol version 4	WFQ	Weighted Fair Queuing

APPENDIX B
UNIQUE CLASSIFIED UNIFIED CAPABILITY

B.1 PURPOSE AND SCOPE

This section describes technical requirements that are unique to providing classified Unified Capabilities (UC). Classified requirements consist of the Sensitive but Unclassified (SBU) requirements with modifications as described in this section. This issue of the Unified Capabilities Requirements (UCR) specifies technical requirements for assured interoperability and Information Assurance of the following set of UC:

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

More specifically, meeting the requirements specified in this section will allow classified UC products to be tested and placed on the UC Approved Products List (APL).

The current Classified Voice and Video over Internet protocol (IP) (CVVoIP) system is a single security level network operating over the Defense Information Systems Network (DISN) SECRET Aggregation Routers (ARs) that include secure voice capabilities that interface with the Defense RED Switch Network (DRSN) at selected locations. The CVVoIP system described is not intended to replace the DRSN and its many unique features.

The contents of this section are arranged as follows:

- Section B.1, Purpose and Scope, provides the purpose of this section and provides a list of major policies that are unique to the multilevel secure voice services provided by the DRSN and to the single security level DISN Voice and Video over IP (VVoIP) services.
- Section B.2, General Requirements Overview, provides a summary of the CVVoIP requirements that drive the CVVoIP design.
- Section B.3, Migration to AS-SIP Signaling for DISN CVVoIP, addresses the Voice over Secure IP (VoSIP) migration to a multivendor IP-based, assured, secure CVVoIP system.
- Section B.4, Initial CVVoIP Technical Design, addresses the CVVoIP IP technical design.
- Section B.5, Modifications to the SBU Assured Services Requirements To Include CVVoIP-Unique Requirements, describes the modifications to the SBU Assured Services (AS) requirements as necessary to include CVVoIP-unique requirements. Topics discussed include voice End Instrument (EI), Session Controller (SC) requirements, network-level Softswitch (SS), Media Gateway (MG), Signaling Gateway (SG), Session Border Controller (SBC), addressing schema, Network Management (NM), voice quality, Wide Area Network (WAN) requirements, and the Information Assurance requirements.

- Section B.6, Classified AS-SIP-Unique Requirements, defines the modifications to the SBU UC Session Initiation Protocol (SIP) requirements as necessary for classified AS.
- Section B.7, DRSN Switches and Peripheral Devices, discusses special construction requirements that include Protected Distribution System (PDS) cabling, encryption of facilities leaving a secure enclave, and TEMPEST.
- Section B.8, Physical Construction Unique Requirements, discusses the special construction requirements for classified elements within a secure enclave.
- Section B.9, UC Secure Preset Conference, describes the requirements that will enable SBU voice subscribers equipped with a National Security Agency (NSA) Type I encryption device to conference in the secure mode.

B.1.1 Policy and Requirements Documents for DRSN and CVVoIP

All the policies identified in Section 3, Policy, apply to CVVoIP. Table B.1-1, Major Policy and Requirements Drivers for Defense Information Systems Network (DISN) CVVoIP Services, lists the major policy and requirements documents that are unique to Multi-Level Security (MLS) voice services provided by the DRSN and to single security level DISN CVVoIP services.

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

TITLE	DATE OR VERSION
Joint Requirements Oversight Council (JROC), JROC Memorandum (JROCM) 202-02, "Global Information Grid (GIG) Mission Area Initial Capabilities Document (MA ICD)" 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	22 November 2002
Department of Defense Directive (oODD) 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

TITLE	DATE OR VERSION
"Operational Requirements Document (ORD) for Secure Voice Requirements," J-6A 01665-92	17 November 1992
National Security Telecommunications and Information Systems Security (NSTISS) Instruction (NSTISSI) No. 4010, "Keying Material Management (U)," For Official Use Only (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)," SECRET/Not Releasable to Foreign Nationals (S/NF)	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"	

B.2 GENERAL REQUIREMENTS OVERVIEW

A high-level summary of the requirements for CVVoIP are provided by a combination of the documents referenced in Table B.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 Command and Control (C2) communications service offering. These performance attributes have been proven in real world operations stretching from OPERATION 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 the following:

- Multilevel secure service.
- Rapid, high-quality, secure communications and conferencing capabilities for senior leaders and warfighters.
- Assured services.
- Information Assurance.
- End-to-End (E2E) interoperability.
- Network Operations (NetOps).

One of the key C2 functions of the DRSN is to provide rapid, flexible, and secure conferencing. As a result, a number of unique non-commercial off-the-shelf (COTS) MLS operator console features have been developed in response to the Combatant Commands' (COCOMs') command center requirements. These unique features, which are part of the way those command centers conduct their business, will not be required for CVVoIP.

B.2.1 Assured Services

The CVVoIP system shall provide AS features as described in Section 2, Session Control Products.

B.2.2 Multilevel Secure Voice Services

The CVVoIP services are provided using the SECRET-level Secure IP Router Network (SIPRNet) as the IP transport infrastructure. The CVVoIP services use the Confidential Access Level (CAL) parameter within the Assured Services Session Initiation Protocol (AS-SIP) signaling protocol to identify the security level of a session. The security level indicated by the CAL parameter is transmitted to the DRSN via the CVVoIP-DRSN Gateway as described in Section B.5.4, DRSN to CVVoIP Media Gateway With Signaling Interworking.

B.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 E2E voice quality requirements for the IP-based environment of CVVoIP are based on Mean Opinion Score (MOS) measurements as defined in Section B.5.8, Voice Quality. The objective of the DRSN subset of secure voice 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. For the DRSN subset of CVVoIP, this is defined as receiving a score of at least 90 on the diagnostic rhyme test (DRT) and a score of at least 60 on the diagnostic acceptability measure (DAM). The DRT measures intelligibility, and the DAM measures quality.

B.2.4 C2 Requirements

This section provides a summary of the system-wide C2 requirements for classified services. The term "system" as used in this section refers to the combination of the DRSN and CVVoIP environments. Once IP technology matures to the necessary level, the full complement of C2 requirements may be provided by the CVVoIP system.

For the near-term, the following requirements will be met by a combination of the CVVoIP and the current suite of DRSN switches:

- MLS Voice:
  - Variable security access level (applicable to DRSN only, CVVoIP is fixed at SECRET).
  - Authentication.
  - Low probability of misconnect.
  - High crosstalk isolation.
  - TEMPEST/Electromagnetic Interference (EMI) compliance.
- Integrated RED-BLACK instruments (DRSN only):
  - Instruments located in a Sensitive Compartmented Information Facility (SCIF) must meet the Committee on National Security Systems (CNSS) 5000-series instructions and procedures (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:
  - Nonblocking components.
  - Transport bandwidth.
  - Resilient routing.
  - Multilevel Precedence and Preemption (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.
- Interoperability:
  - Legacy devices (secure voice radios, instruments, and other terminal types (DRSN only)).
  - Dissimilar devices [e.g., between Military Strategic, Tactical, and Relay (MILSTAR) and Secure Terminal Equipment (STE) terminals (DRSN only)].
  - Media conversion.
  - Protocol conversion.
  - Speakers, recorders.
  - Other networks, such as MILSTAR.SECN, Defense Satellite Communications System (DSCS)/Early Pentagon Capability (EPC), Homeland Security, FBI, and Department of State (DRSN only).

B.2.5 Key CVVoIP Voice Services Features

The key CVVoIP voice services features and attributes are shown in Table B.2-1, Key CVVoIP Voice Service Features.

Table B.2-1. Key CVVoIP Voice Service Features

FEATURE NAME	FEATURE FUNCTIONAL PURPOSE
Automatic Number Identification (ANI)	Provides caller ID to both users
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 an instrument. Any IP EI must be DISABLED at all times when not under the physical control of the authorized user
COTS Features	Call forward, call waiting, call hold

B.2.6 General Security Features

The DRSN RED Switches, classified SCs, 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 TOP SECRET security level.

However, CVVoIP users and classified SCs are to be configured only at the SECRET level until an MLS operation for IP-based technology is mature.

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.

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 a CVVoIP system must be approved or implemented as defined by the SIPRNet Connection Approval Process. The DRSN RED Switches and CVVoIP SCs, must interconnect with other RED Switches and/or peripheral devices (to include, but not limited to, Deployed secure voice switches or enclaves, radio interfaces, audio systems, voice announcers, and multimedia and/or secure voice over data capabilities) through encrypted ISTs or by means of a PDS. Other secure systems must interconnect to the DRSN using Defense Information Systems Agency (DISA)-established interface criteria and encryption devices or a PDS.

B.2.7 Special Security Features

Currently, the following special security features are 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.

- 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 before the call is 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 [i.e., SECRET (S), TOP SECRET (TS), or TS/Sensitive Compartmented Information (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. The CVVoIP instruments will be fixed at the SECRET level and display the calling telephone number via AS-SIP signaling.
- Security Access Level. The SAL is a user classmark assigned to each instrument, line key, and trunk, and provides security authentication of the calling and called party. The SALs are assigned to each instrument, line key, and trunk based on 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.

- Automatic Security Authentication (ASA). The ASA ensures DRSN calls are set up in accordance with (IAW) security and access authorization criteria defined for each user and/or DRSN switch interface. The 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 on a highest common denominator scheme. For example, a connection between a user classmarked with a Variable SAL (VSAL) (see paragraph 3b) of SECRET calling a user classmarked with a VSAL of TOP SECRET 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 Fixed SAL (FSAL) (see paragraph 3a) 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.
  - Fixed Security Access Level. The FSAL emphasizes call security over call completion. A user selects an FSAL classmarked 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 classmarked with the same SAL (e.g., TOP SECRET), 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 unavailable 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. The CVVoIP instruments will be fixed at the SECRET level.
  - Variable Security Access Level. The 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 unequal. Calls are established automatically 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. The CVVoIP instruments will be fixed at the SECRET level.

- 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 DAA, through the DISA DRSN Information Systems Security Manager. Before removal, the user must justify the action, develop procedures for maintaining the secure integrity of the instrument, and have written approval IAW DRSN security guidelines.

B.2.8 Network Security

- The DRSN RED Switches, CVVoIP SCs, and Tier0 SSs must be located in RED enclaves. The DRSN RED Switches at locations that have subscriber terminals authorized to process TS/SCI must be located in SCIFs. The DRSN RED Switches and CVVoIP SCs will provide the following:
  - In-the-clear calling within each RED enclave by means of PDSs and protected Assured Services Local Area Networks (ASLANs).
  - Cryptographically protected calling between RED enclaves supported by DRSN RED Switches and CVVoIP SCs.
  - DRSN RED Switches, and CVVoIP SCs interface to external cryptographic equipment for all other calling.
- The NSA-approved encryption equipment provides Communications Security (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 Telecommunications Security (TSEC)/KG-84 family of equipment (including KIV-7) provides Transmission Security (TRANSEC) to ISTs to locations (including quarters) receiving DRSN service via Digital Phone Adapter (DPA), Digital Trunk Adapter (DTA), 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.
- The DRSN and 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 or limited exclusion area within the quarters and must comply with requirements set forth in the security guides for DRSN and VoSIP/CVVoIP.

B.2.9 Network Interfaces

A key feature of the DRSN is its ability to interface and interoperate with a variety of Department of Defense (DoD) and commercial networks. The CVVoIP system interfaces to the DRSN through a gateway. (See Section B.5.4, DRSN to CVVoIP Media Gateway With Signaling Interworking.)

B.2.10 CVVoIP 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 must follow the SIPRNet Connection Approval Process. The Joint Interoperability Test Command (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. The 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 effects 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.

B.2.11 DRSN and CVVoIP Network Management

DISA establishes DRSN management systems and procedures to ensure responsive, secure, interoperable, survivable, and cost-effective service. The DRSN is under the management control of the Director, DISA Systems Security Manager (SSM), on behalf of the U.S. Strategic Command (USSTRATCOM), and is responsive to the Chairman of the Joint Chiefs of Staff (CJCS), the COCOMs, the Military Departments (MILDEPs), and Defense agencies and activities.

- DISA must possess read-access capabilities and limited or 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.
- DISA must maintain a Configuration Management (CM) database of all switch configurations (continental United States [CONUS] and outside CONUS [OCONUS]) and provide access to agencies, activities, and MILDEPs as authorized by the Office of the Secretary of Defense (OSD); the Director, DISA; and the Joint Staff.
- 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 SCs) 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 Operations and Maintenance (O&M) activities before implementing DRSN and Tier0 switch network-level database changes and/or network controls.
- During emergencies, DISA has the authority to use direct write capabilities to implement switch database revisions required for operation and management of the DRSN and CVVoIP system.

- DISA will take necessary action to establish capabilities and procedures necessary to sustain the DRSN and CVVoIP if a failure of the GNSC/TNC occurs and to reconstitute a major DRSN nodal element if a catastrophic failure occurs.

B.2.12 Conferencing Requirements

The CVVoIP services will not provide the full conferencing features inherent with the DRSN, but CVVoIP users must be able to join and participate in conferences set up by external conference systems and the DRSN. The SC must support use of the CAL/SAL functionality as part of conferencing. The CVVoIP SC must be capable of providing a minimum of 5 simultaneous preset conferences with a minimum of 25 participants (local and external). Each preset pattern must be able to coexist with other conferences as independent conferences. Expanded requirements for secure preset and meet-me conferences based on SBU voice subscribers equipped with NSA Type I encryption devices are provided in Section B.9, UC Secure Preset Conference.

B.2.13 CVVoIP Equipment Certification and Testing Policy

Interoperability and Information Assurance testing of CVVoIP equipment will be executed in accordance with DoDI 8100.04.

B.3 MIGRATION TO AS-SIP SIGNALING FOR DISN CVVOIP

The core system must be able to support both H.323 and AS-SIP until a migration to all AS-SIP is completed.

B.4 INITIAL CVVOIP TECHNICAL DESIGN

Figure B.4-1, Overview of Initial CVVoIP Assured Services Design, illustrates the CVVoIP technical design for assured classified services at a single security level. The red text illustrates the significant changes introduced to achieve E2E CVVoIP with assured service. The design is similar to the one that is used by the SBU VVoIP with the following significant differences:

- The SECRET Provider Edge (PE) (S-PE) Routers, the SECRET Customer Edge (CE) (S-CE) Routers, and the SECRET Aggregation Routers (S-ARs) versus the U-PE, U-CE, and U-ARs will be used.
- A High Assurance IP Encryptor (HAIPE) will be used with the S-PE Router.
- The AS-SIP protocol version used for CVVoIP is a modification of the SBU version (See Section B.6, Classified AS-SIP-Unique Requirements).
- The bearer stream will use the Real-Time Transport Protocol (RTP) rather than Secure Real-Time Transport Protocol (SRTP). This is acceptable since all CVVoIP enclaves are protected by encryption devices.

- The use SBCs are not required. For CVVoIP the UC signaling and bearer traffic go through existing SIPRNet data firewalls; these data firewalls have been configured with port ranges to allow UC traffic to pass.

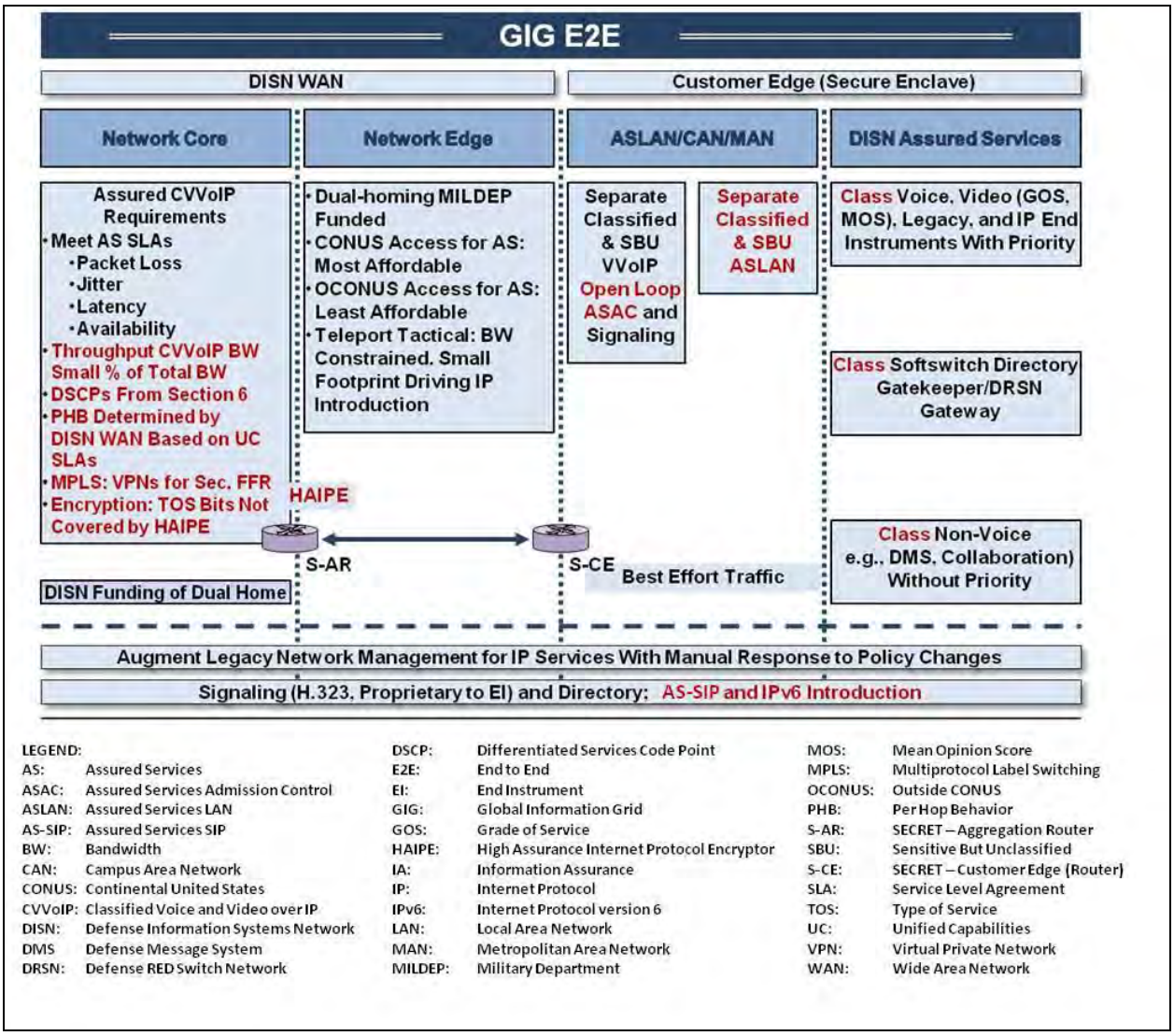


Figure B.4-1. Overview of Initial CVVoIP Assured Services Design

The classified SS (referred to as Tier0 SSs) is pure IP without a Time Division Multiplexing (TDM) signaling capability, except they provide a unique media and signaling interface to the DRSN.

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

In this timeframe, 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 the 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. Users will be encouraged to convert to IP video services when AS-SIP with the full H.323 feature set is available. Nevertheless, until NSA develops an IP replacement for the KIV, multilevel secure services will have to be over the DSN ISDN circuit-switched services.

B.4.1 Signaling Design

The signaling design has to provide both backward and forward technology capabilities. Thus, Client Access Server (CAS) and PRI in the DRSN has to interoperate with H.323 signaling in the current CVVoIP network 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 is depicted in Figure B.4-2, DISN CVVoIP Hybrid Signaling Design.

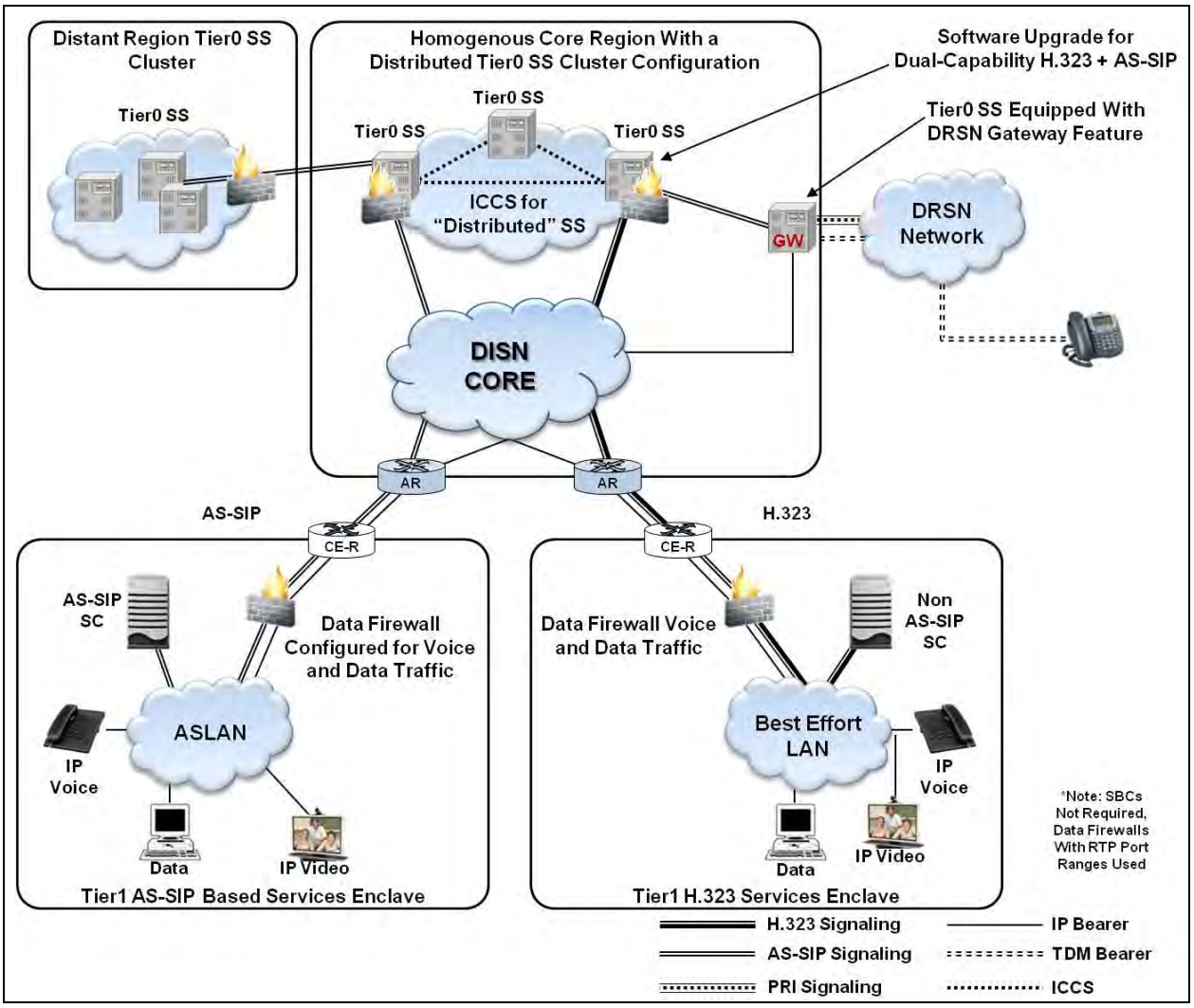


Figure B.4-2. DISN CVVoIP Hybrid Signaling Design

The hybrid signaling design is constructed as a two-tier hierarchy consisting of a "local" level and a "backbone" level. At the local level, SCs are located in secure enclaves and represent the level of the signaling hierarchy closest to the EIs. The local level is based on a multivendor assortment of SCs. The backbone, or Tier0 signaling, level is a robust, homogeneous design based on current vendor-unique geographic cluster arrangements of Tier0 SS. 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 to AS-SIP based CVVoIP there will be segments using H.323 signaling also. Signaling interoperability between H.323 and AS-SIP will be achieved by an APL product called a Dual-Signaling Softswitch (DSSS). (See Section B.5.3, Network-Level Softswitches.)

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 SCs as well as a few, select Tier0 SSs provide "Managed Services" to a limited set of EIs and, therefore, a Tier0 SS may have an SC function associated with it also.

Every SC 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 by Intra-Cluster Communication Signaling (ICCS) links, and they 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 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.

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

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

Originating SC --- Tier0 SS 1 ---------- Tier0 SS 2 --- Destination SC

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

Originating SC --- Tier0 SS --- Destination SC

The access link between the CE Router and the AR is resource constrained and the SC 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) where the Tier0 SS intervenes by blocking session

requests or preempting session requests and active sessions when the Tier0 SS determines that the SC has exceeded its provisioned threshold for voice traffic or video traffic.

B.4.2 Bearer Design

The CVVoIP local service enclaves and core locations are protected by encryption devices and data firewalls with ports open to accommodate voice, video, and data traffic. As a result, bearer design for the CVVoIP system will use the Real Time Protocol (RTP). SBCs are currently not employed within CVVoIP system, but may be installed as an option at certain local service enclaves and at Tier0 core locations.

B.5 MODIFICATIONS TO THE SBU ASSURED SERVICES REQUIREMENTS TO INCLUDE CVVOIP-UNIQUE REQUIREMENTS

Section 2, Session Control Products, addresses the functions, methods, protocols, and associated technical parameters for the EI, SC, SS, SBC, and NM components of the DISN VVoIP System. AS-SIP 2013, Section 4, SIP Requirements for AS-SIP Signaling Appliances and AS-SIP EIs, provides the complete requirements for AS-SIP, including both the SBU and unique classified requirements.

This section 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.

B.5.1 Voice End Instrument

CLA-000010 [**Required: Voice EI**] Voice Instruments require two-factor authentication [This may be achieved by using a Common Access Card (CAC)-enabled instrument or other security means].

CLA-000020 [**Required: Voice EI**] Voice instruments must display the security level (CAL) of the call.

B.5.2 Classified SC Requirements

B.5.2.1 SBU SC Requirements Not Applicable to Classified SC

The following SC requirements defined in Section 2.10, Session Controller, do not apply to the classified SC:

1. MG, SG for SS7 (the classified SCs do not interface to external networks).
2. Public safety features [e.g., Public Safety Announcement Bulletin (PSAB), E911 access].

B.5.2.2 Classified SC Unique Requirements

The following general requirements are unique to classified SCs:

- Located in secure enclave.
- PDS cabling per DRSN requirements.
- Dynamic Host Configuration Protocol (DHCP) not allowed, strict control of EI assignments using static IP addresses.
- Use the classified version of AS-SIP signaling, including sending CAL/SAL display information to the end instrument.
- Expanded conferencing features to include minimum of five simultaneous presets with a minimum of 25 participants (local and external). Each preset conference pattern must be able to coexist with other conferences as independent conferences. The conferencing capability must support the CAL/SAL functionality.
- Automatic Security Authentication (ASA) with a mix of fixed and variable SAL.

B.5.3 Network-Level Softswitches

Section 2.11, Network-Level Softswitches, describes the network-level SSs used in the SBU network. The CVVoIP system uses a unique backbone SS referred to as a Tier0 SS. During the CVVoIP transition period, the Tier0 SS will be augmented to provide a dual-signaling capability to provide interoperability between H.323 and AS-SIP-based SCs. When augmented, the Tier0 SS will become an APL product referred to as a DSSS. Figure B.5-1, DSSS Reference Model, provides the functional reference model for the DSSS.

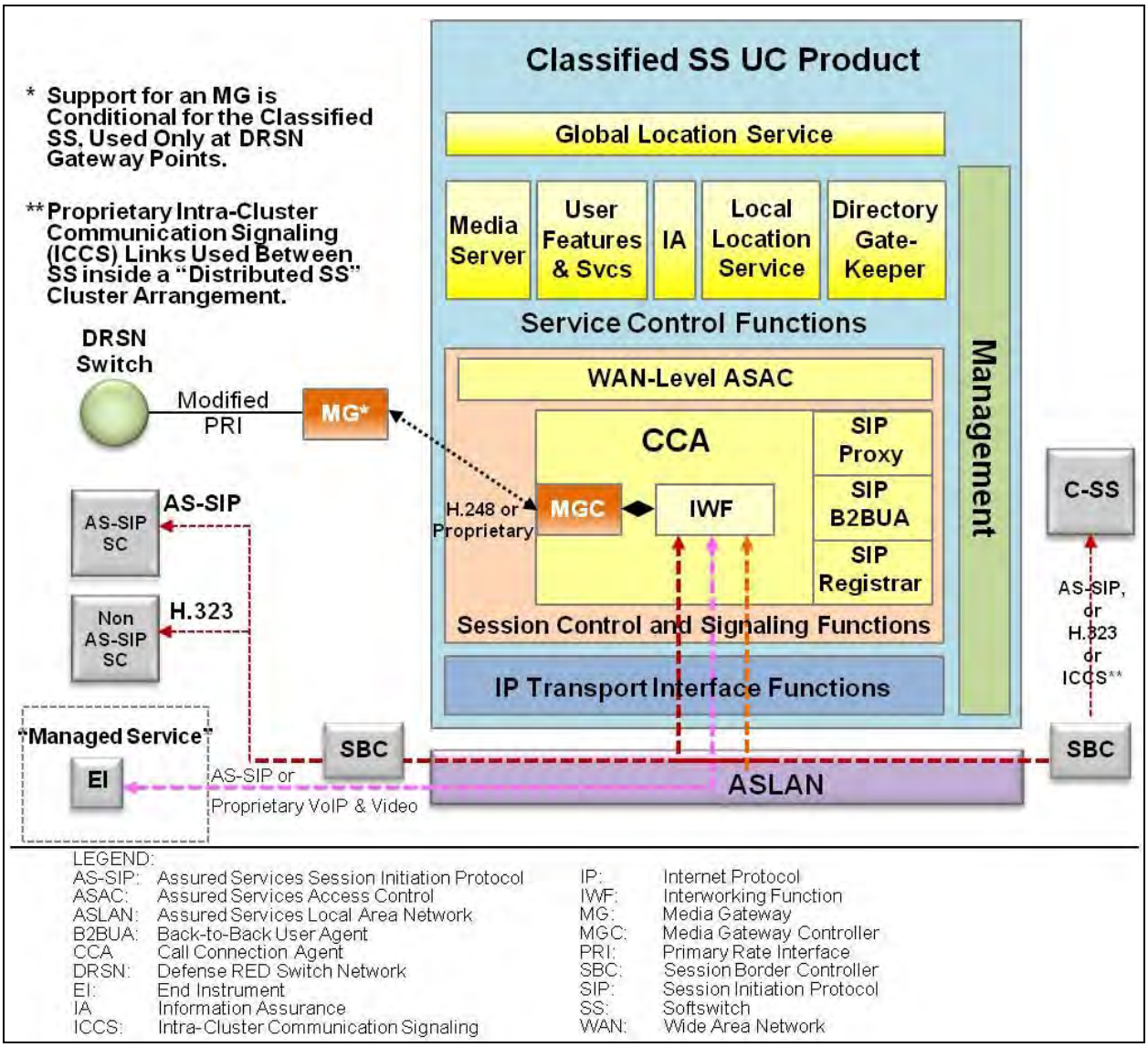


Figure B.5-1. DSSS Reference Model

CLA-000030 [**Required: Tier0 SS, DSSS**] The product must provide both H.323 Directory/Gatekeeper functionality and AS-SIP as well as interworking between the two signaling methods. (This is a transitional requirement until CCVoIP becomes all AS-SIP-based).

CLA-000040 [**Required: Tier0 SS, DSSS**] Managed Services is the term used to describe the situation where a limited number of subscribers are served on a remote basis from either an SC or the SC function of a Tier0 SS. The subscribers are located in a remote secure enclave and provided secure (encrypted) access to the SC.

CLA-000050 [**Required: Tier0 SS, DSSS**] Numbering plan/addressing compatibility with DRSN, Tactical Global Block Numbering Plan (GBNP), and SIPRNet IP addressing schema.

CLA-000060 [**Optional: Tier0 SS, DSSS**] There are no TDM capabilities except as noted for the MG function at selected locations.

CLA-000070 [**Not Required: Tier0 SS, DSSS**] Public safety features (e.g., PSAB, E911 access) are not required.

B.5.4 DRSN to CVVoIP Media Gateway With Signaling Interworking

B.5.4.1 General

As the Classified Voice and Video over Internet Protocol (CVVoIP) service evolves, the classified IP telephony component (CVoIP) will coexist with the Defense RED Switch Network (DRSN) for an unspecified period, as the DRSN will continue to serve as the foundation of a DoD multilevel secure C2 voice capability. During this period of coexistence, the requirement exists to provide interoperability and transparency of features and capabilities between the DRSN domain and the CVoIP domain. The bridge between these domains is a Media Gateway and Signaling Interworking function. This "bridge" is based on the use of an ISDN Primary Rate (PRI) user-network interface in which the interface structure is composed of multiple B channels, one D-channel and a User-User Information Element (UUIE) on the DRSN side of the "bridge" and an IP signaling protocol on the CVVoIP side of the "bridge." This "bridge" provides, among other things, a methodology and capability for the interworking and interoperability of SALs used in the DRSN Domain and Confidential Access Levels (CALs) used in the CVVoIP domain. The required Media Gateway and Signaling Interworking function for the CVVoIP is exclusively instantiated as a function of and at the DISA Tier0 Softswitch infrastructure. This section establishes the CVVoIP Media Gateway and signaling Interworking requirements between the DRSN domain and the CVVoIP domain.

It is assumed that the reader has some familiarity with the function and operation of SALs used in the DRSN domain and CALs used in the CVVoIP. The reader's attention is further directed to the CVVoIP "CAL General Requirements" established by and in AS-SIP 2013, Section 4.9.2, Presence of CAL Header in INVITE Requests, 200 Responses, 418 Responses, and in Section B.2.7, Special Security Features, for CVVoIP signaling appliances.

B.5.4.2 DRSN Signaling Protocol

A base assumption for the DRSN/MG interface is that the Classified Voice over IP (VoIP) (CVoIP) network side is configured as homogenous with respect to the DISA-defined SAL methodology. Adjudication, changes to the call SAL and call clearing as a result of mismatch are contained within DRSN.

CLA-000080 [**Required: MG**] The DRSN Signaling Protocol interface is an ISDN user-network interface in which the interface structure is composed of multiple B channels and one D-channel. The bit rate of the D-channel in this structure is 64 Kbps. When a 1544-Kbps Primary Rate Interface (PRI) is provided, the interface structure is 23B+1D. Requirements for this feature

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

CLA-000090 [**Required: MG**] The MG shall support the option to operate in accordance to the 4ESS Primary Rate specification: AT&T TR41459. Physical layer specifications previously defined apply for the 4ESS variant.

CLA-000100 [**Required: MG**] Requirements for ISDN SAL service shall be in accordance with ANSI Standards T1.621-1992 User-to-User Signaling Supplementary Service.

CLA-000110 [**Required: MG**] ISDN PRI Setup Message shall contain the User-User Information Element, as shown in Table B.5-1, ISDN PRI User-User Information Element (Setup/Connect).

Table B.5-1. ISDN PRI User-User Information Element (Setup/Connect)

Bit:	8	7	6	5	4	3	2	1
	User-User Information							
Octet 1:	0	1	1	1	1	1	1	0
	Element Identifier							
2	Length of User-User Contents							
3	0	0	0	0	0	0	0	0
	User-Specific Protocol							
4	0	1	0	1	0	1	0	1
5	0	0	0	0	0	0	0	1
7	0	1	0	1	1	1	0	1
	SAL Protocol Identifier							
8	Length of SAL Message							
9	Message Type ID							
10	Precedence Level							
11	0/1	Security Access Level Designation						
	V/F							
12	0	0	0	0	0	0	0	0
	0	0	0	0	1	0	1	0
13	0	0	0	0	1	0	1	0
	User-Specific Protocol							
14–29	Caller ID							
Octet 4-7: (Static Definition) MG ingress: no processing								

MG egress: must be populated with the information indicated in Table B.5-1
Octet 9: Message Type ID Bits 8 7 6 5 4 3 2 1 0 0 0 0 1 0 1 0 (Call – Sent with SETUP message) 0 0 0 0 0 0 1 0 (Answer – Sent with CONNECT message) MG ingress: reject call if value other than in Table B.5-1, or misaligned with the indicated PRI message MG egress: set appropriately to PRI message
Octet 10: Precedence Level Bits: 8 7 6 5 4 3 2 1 0 0 0 0 0 0 0 0 (No precedence) 0 0 0 0 0 0 0 1 (Routine – lowest) 0 0 0 0 0 0 1 0 (Priority) 0 0 0 0 0 0 1 1 (Immediate) 0 0 0 0 0 1 0 0 (Flash) 0 0 0 0 0 1 0 1 (Flash Override) 0 0 0 0 0 1 1 0 (Flash Override Override – highest) 1 1 1 1 1 1 1 1 (Not Used)
Octet 11: Security Access Level – SAL Bit 8: Set to 0 for Variable Security Access Level, set to 1 for Fixed Security Access Level Bits 7 6 5 4 3 2 1: Security Access Level (SAL) value. Valid values – 2 thru 99.
Octet 12: (Static Definition) MG ingress: no processing MG egress: must be populated with the value indicated in Table B.5-1.
Octet 13: (User Specific Protocol) This octet is not applicable to UC. MG ingress: no processing MG egress: must be populated with the value indicated in Table B.5-1.
Octet 14-29: Caller ID (optional, if text is provided it must comply with the following instructions, otherwise should be left null) The remaining octets allow the passing of Caller ID information between switch nodes. Octet 14 is the left most character and octet 29 is the right most character. The information from this field is used for end instruments with display capabilities to display the Caller ID of the calling party. Valid values: A-Z a-z 0-9 !@#$%^&*()-_+={}[]<>

CLA-000120 [**Required: MG**] The Setup Message User-User Information Element shall comply with population and processing guidance in Table B.5-1 and the table notes.

CLA-000130 [**Required: MG**] ISDN PRI Connect Message shall contain the User-User Information Element, as shown in Table B.5-1.

CLA-000140 [**Required: MG**] The Connect Message User-User Information Element shall comply with population and processing guidance in Table B.5-1 and the table notes.

CLA-000150 [**Required: DRSN and IP Signaling Appliance**] The Signaling Appliance shall contain a SAL/CAL Adjudication Map Approved by DISA for the adjudication and verification of SAL/CAL for calls and sessions

CLA-000160 [**Required: DRSN and IP Signaling Appliance**] The received SAL/CAL value shall be verified (per the DISA Adjudication Map) against the SAL/CAL configured for the MG interface and the call rejected with cause code 54 ("Incoming calls barred within Closed User Group") in the event of incompatibility.

CLA-000170 [**Required: DRSN and IP Signaling Appliance**] The SAL/CAL Adjudication Map shall be protected from unauthorized access.

CLA-000180 [**Required: DRSN and IP signaling Appliance**] Modifications to the SAL/CAL Adjudication Map shall be audited events.

CLA-000190 [**Required: DRSN and IP Signaling Appliance**] The DRSN/IP signaling appliance shall perform SAL/CAL adjudication (per the DISA Adjudication Map) between the SAL/CAL presented by the MG signaling and the EI(s) and update the MG SAL/CAL when adjudication results in a SAL/CAL adjustment.

CLA-000200 [**Required: DRSN and IP Signaling Appliance**] For ingress signaling containing SAL/CAL data, the text value corresponding to the numeric value shall be delivered to the EI (for display).

CLA-000210 [**Required: EI**] The latest SAL text received from the Signaling Appliance shall be continuously displayed on the EI for the duration of the call.

CLA-000220 [**Required: MG**] The MG shall support the User Information Message containing the User-User Information Element (from the DRSN signaling appliance) as shown in Table B.5-2, ISDN PRI UUIE (User Information for SAL), for the signaling of SAL level change during a connection.

Table B.5-2. ISDN PRI UUIE (User Information for SAL)

Bit:	8	7	6	5	4	3	2	1
	User-User Information							
Octet 1:	0	1	1	1	1	1	1	0
	Element Identifier							
2	Length of User-User Contents							
3	0	0	0	0	0	0	0	0
	User-Specific Protocol							
4	0	0	0	0	1	1	1	0
	Operation							
5	0	0	0	0	0	1	1	1
	SAL Change							

6	Sale Numeric Value 2–99
7	Fixed/Variable SAL
Octet 4: (Static Definition) MG ingress: No processing MG egress: must be populated with the information indicated in Table B.5-2.	
Octet 5: Operation Type Bits 8 7 6 5 4 3 2 1 0 0 0 0 0 1 1 1 (SAL Change)	
Octet 6: Security Access Level - SAL Bits 8 7 6 5 4 3 2 1 Security Access Level (SAL) value. Valid values - 2 thru 99.	
Octet 7: Fixed/Variable SAL Bits 8 7 6 5 4 3 2 1 0 0 0 0 0 0 0 1 (Fixed SAL) 0 0 0 0 0 0 1 0 (Variable SAL)	

CLA-000230 [**Required: MG**] The User-User Information Element in the User Information Message for SAL change signaling processing shall comply with the processing guidance in Table B.5-2 and the table notes.

CLA-000240 [**Optional: MG**] The MG shall support User Information Message containing the User-to-User Information Element (from the DRSN signaling appliance) as shown in Table B.5-3, ISDN PRI UUIE (User Information for Caller ID), for the signaling of Caller ID change during a connection.

Table B.5-3. ISDN PRI UUIE (User Information for Caller ID)

Bit:	8	7	6	5	4	3	2	1
	User-User Information							
Octet 1:	0	1	1	1	1	1	1	0
	Element Identifier							
2	Length of User-User Contents							
3	0	0	0	0	0	0	0	0
	User-Specific Protocol							
4	0	0	0	0	1	0	1	1
	Operation							
5	0	0	0	0	0	0	0	0
	User-Specific Protocol							
6–21	Caller ID							
Octet 4: (Static Definition) MG ingress: No processing								

MG egress: must be populated with the information indicated in Table B.5-3.
Octet 5: (Static Definition) MG ingress: no processing MG egress: must be populated with the value indicated in Table B.5-3.
Octet 6-21: Caller ID The remaining octets allow the passing of Caller ID information between switch nodes. Octet 6 is the left most character and octet 21 is the right most character. The information from this field is used for end instruments with display capabilities to display the Caller ID of the calling party. Valid values – A-Z a-z 0-9 !@#$%^&*()-_+={}[]<>

CLA-000250 [**Optional: MG**] The User-User Information Element in the User Information Message for Caller ID change signaling processing shall comply with the processing guidance in Table B.5-3 and the table notes.

CLA-000260 [**Required: DRSN and IP Signaling Appliance**] The Signaling Appliance shall contain a mapping for numeric SAL/CAL values and their corresponding, DISA assigned, text.

CLA-000270 [**Required: DRSN and IP Signaling Appliance**] The SAL/CAL numeric-text mapping data shall be protected from unauthorized access.

CLA-000280 [**Required: DRSN and IP Signaling Appliance**] Modifications to the SAL/CAL numeric-text mapping shall be audited events.

CLA-000290 [**Required: MG**] The MG shall contain a DISA approved mapping to translate numeric SAL values to CAL values and vice versa.

CLA-000300 [**Required: MG**] The MG shall convert all received numeric SAL values to their corresponding numeric CAL value on signaling transmission.

CLA-000310 [**Required: MG**] The MG shall convert all received numeric CAL values to their corresponding numeric SAL value on signaling transmission.

CLA-000320 [**Required: MG**] The SAL/CAL numeric mapping data shall be protected from unauthorized access.

CLA-000330 [**Required: MG**] Modifications to the SAL/CAL numeric mapping shall be audited events.

B.5.4.3 Call Scenarios

The following call scenarios across the gateway are illustrated in the subsequent sections:

- Basic Calls:
  - MG to DRSN.
  - DRSN to MG, no SAL adjustment required on answer.
  - DRSN to MG, SAL adjustment required on answer.

  - Transfer from Secure VoIP EI, after connection, to a local phone.
- SAL Violation:
  - SAL violation on MG SETUP (pre-ring).
  - SAL violation on MG incoming call, DRSN user answer.
  - SAL violation after answer due to DRSN party change.
- Changes during call: SAL change during call due to DRSN party change.

B.5.4.3.1 Basic Call Scenarios

NOTE: All SAL adjudication is performed in the DRSN or IP Signaling Appliances. All privileges of acceptance, rejection, and adjustment of offered SALs will be contained within these signaling appliances. The primary obligation of the MG (with respect to SALs) is to translate (as may be required) numeric values from the IP domain (CAL) to the DRSN domain (SAL).

Figure B.5-2, Illustration of a Basic MG to DRSN Call I, illustrates a MG to DRSN Call.

NOTE: For MG to DRSN calls, the assigned SAL/CALs applied in determining the end-to-end SAL/CAL include the DRSN trunk SAL and any CAL assigned to the IP side of the MG.

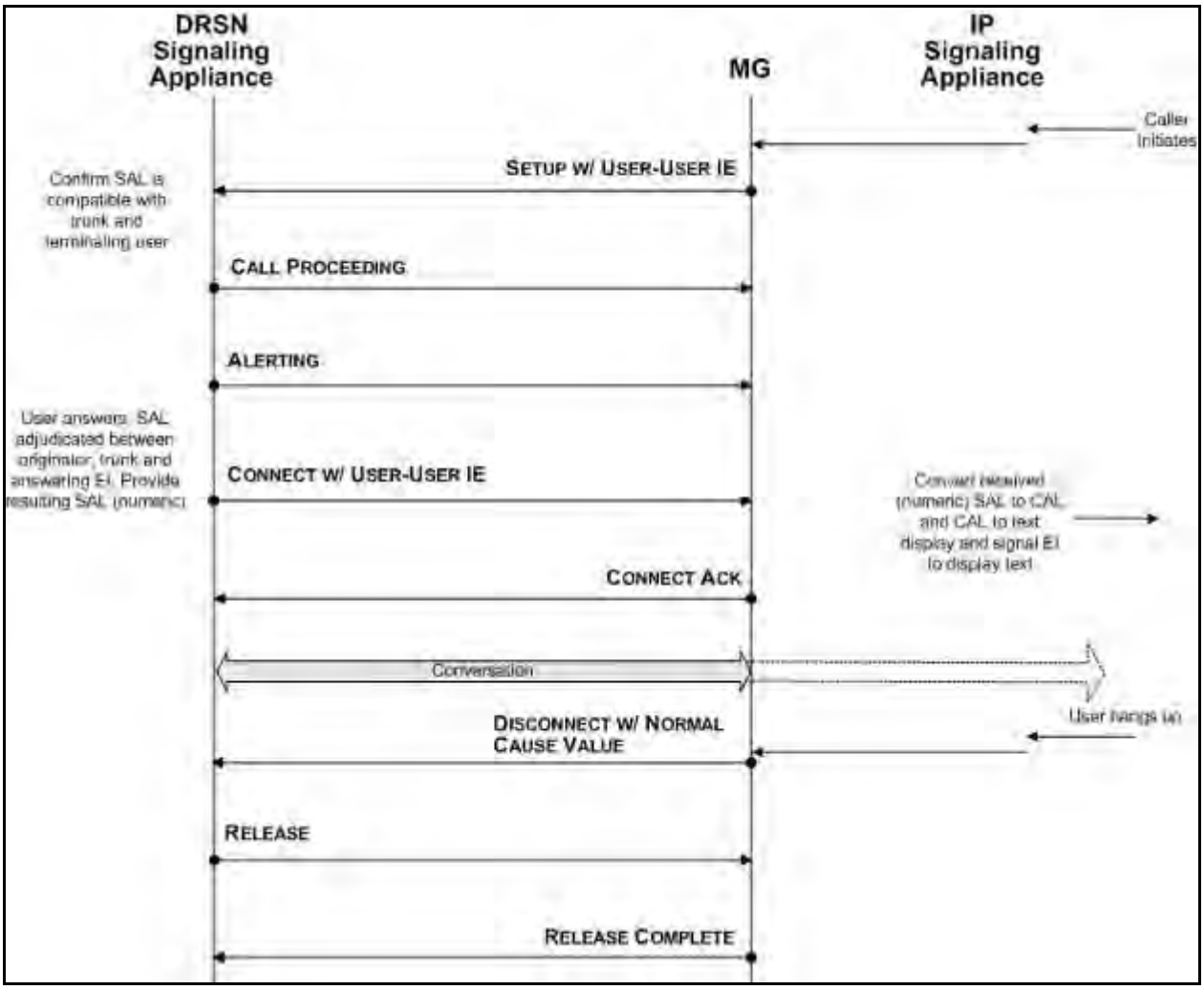


Figure B.5-2. Illustration of a Basic MG to DRSN Call I

Figure B.5-3, Illustration of a Basic DRSN to MG Call, With No SAL Adjustment, illustrates a DRSN to MG, with no SAL adjustment.

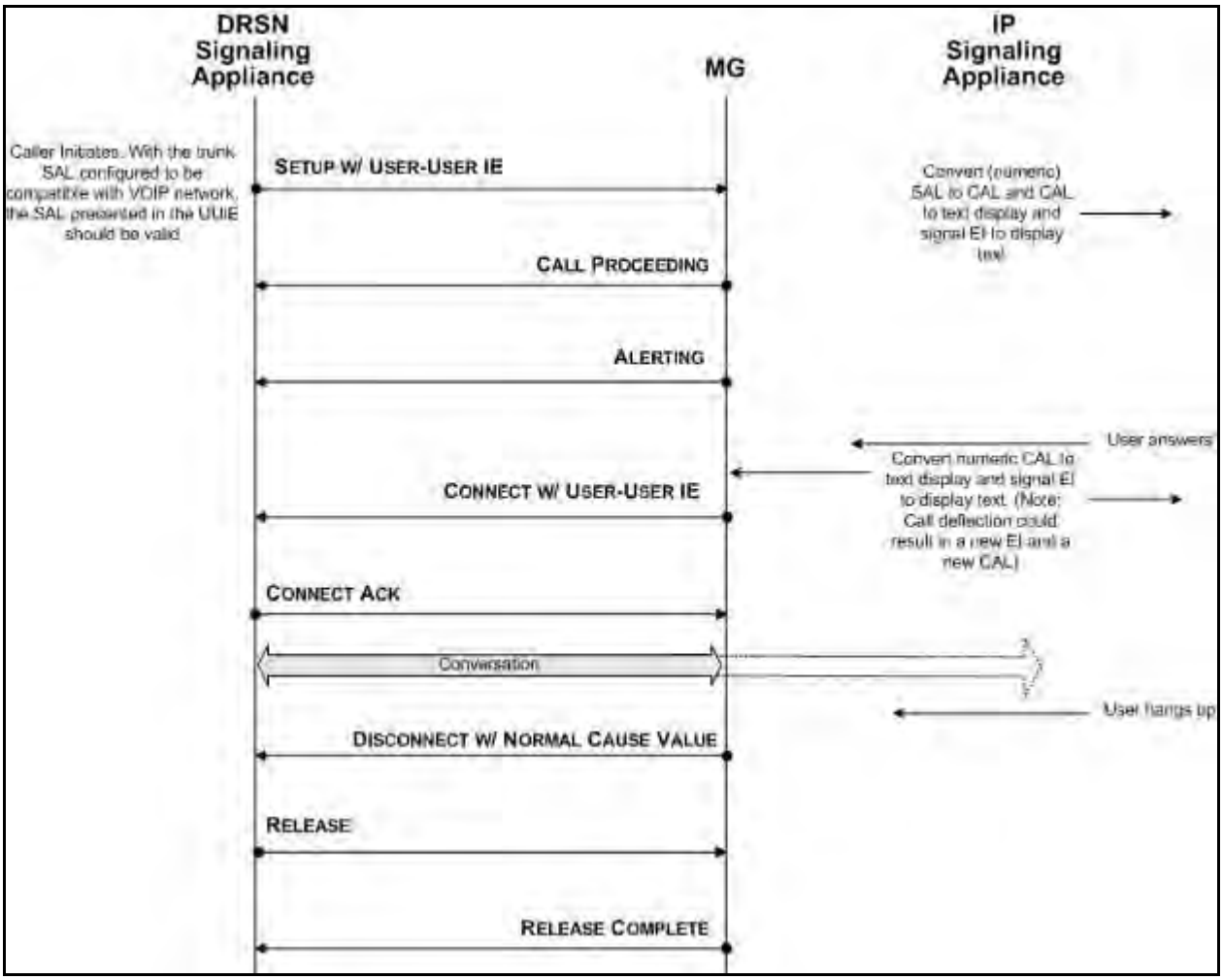


Figure B.5-3. Illustration of a Basic DRSN to MG Call, With No SAL Adjustment

Figure B.5-4, Illustration of a Basic DRSN to MG Call, With SAL Adjustment Required, illustrates a basic DRSN to MG, with SAL adjustment required.

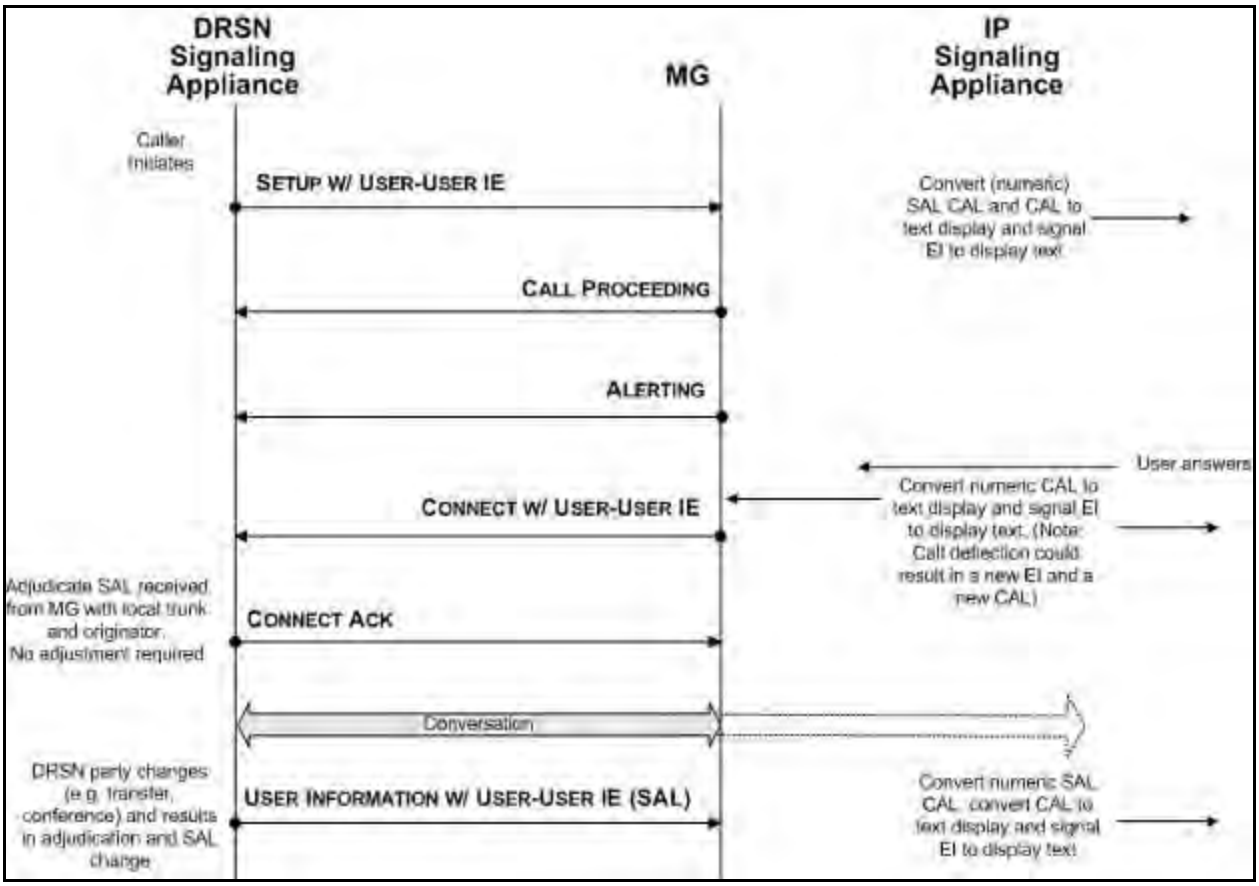


Figure B.5-4. Illustration of a Basic DRSN to MG Call, With SAL Adjustment Required

This scenario will be valid if IP communities assign a variety of "caveats" within a security domain. Such an event might result in local adjudication or when a CONNECT with a SAL variation is received.

Figure B.5-5, Illustration of Transfer Invoked From VoIP EI to a Local VoIP EI With Different Security Domain Caveat, illustrates Transfer invoked from VoIP EI to a local VoIP EI with different security domain caveat.

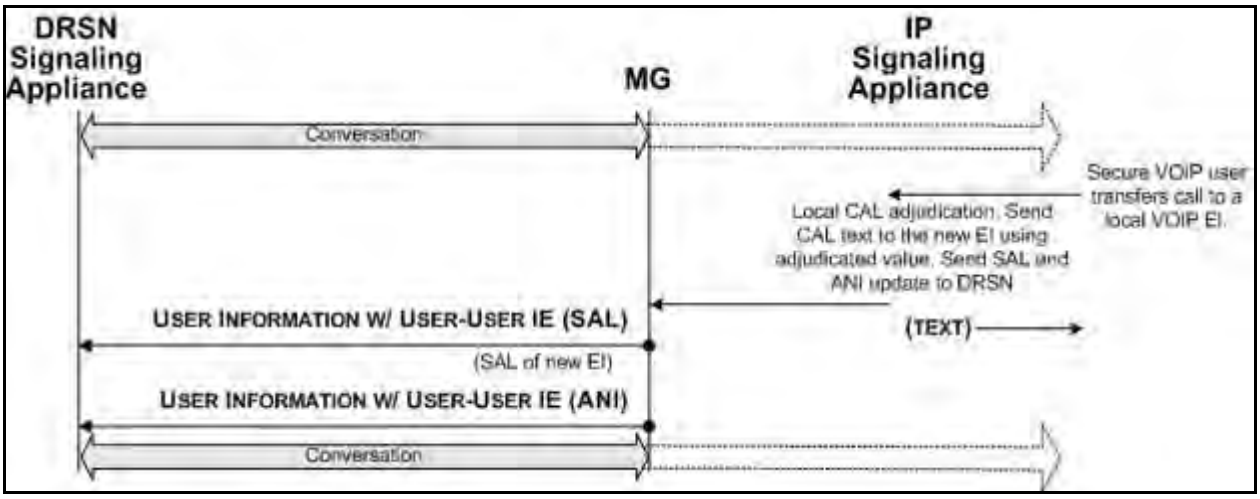


Figure B.5-5. Illustration of Transfer Invoked From VoIP EI to a Local VoIP EI With Different Security Domain Caveat

B.5.4.3.2 SAL Violation Scenarios

Figure B.5-6, Illustration of SAL Violation on MG SETUP (pre-ring), illustrates SAL violation on MG SETUP (pre-ring). The SAL provided on the MG SETUP was either incompatible with the trunk SAL (indicating misconfiguration) or was incompatible with the destination EI SAL.

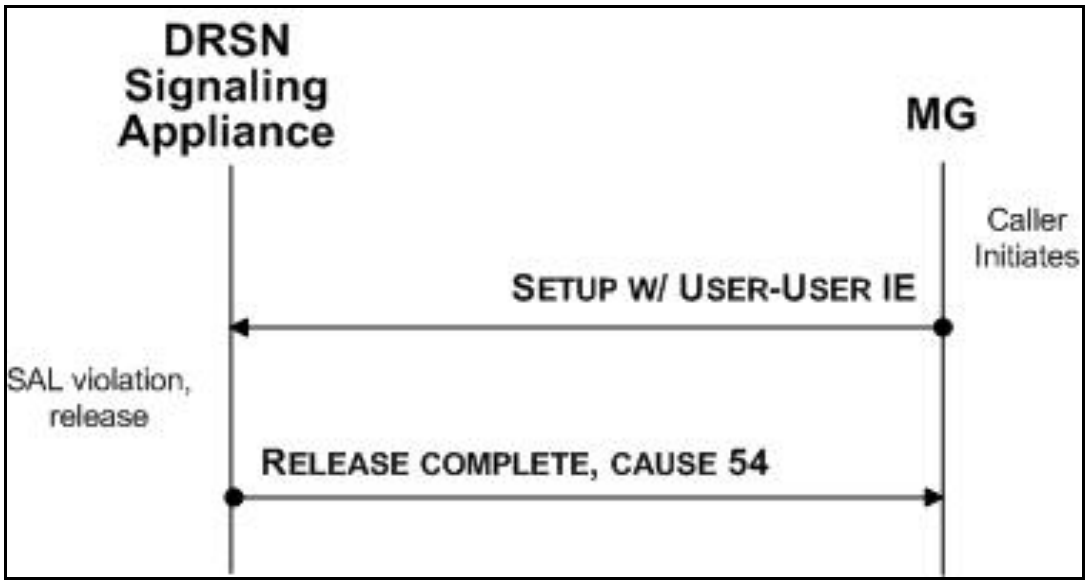


Figure B.5-6. Illustration of SAL Violation on MG SETUP (pre-ring)

Figure B.5-7, Illustration of SAL Violation on an MG Incoming Call, DRSN User Answer, illustrates SAL violation on a MG incoming call, DRSN user answer. The call was originally allowed to proceed since the originator, trunk and termination party SALs were compatible. Some party other than the original destination (e.g., Station Hunt Group, Call Pickup) answered the call and resulted in a violation.

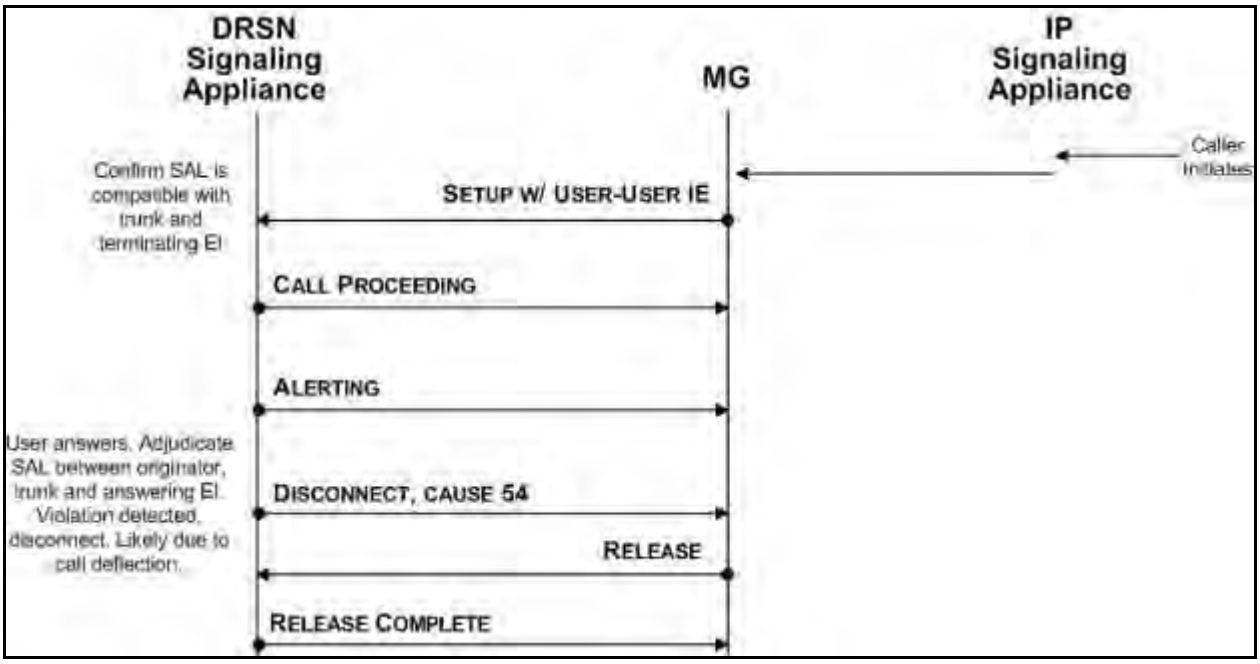


Figure B.5-7. Illustration of SAL Violation on an MG Incoming Call, DRSN User Answer

Figure B.5-8, Illustration of SAL Violation After Stable Call Resulting From DRSN Party Change, illustrates a SAL violation after a stable call because of a DRSN party change. The DRSN party performed an action that involved the addition of a new SAL into the conversation, resulting in a SAL violation.

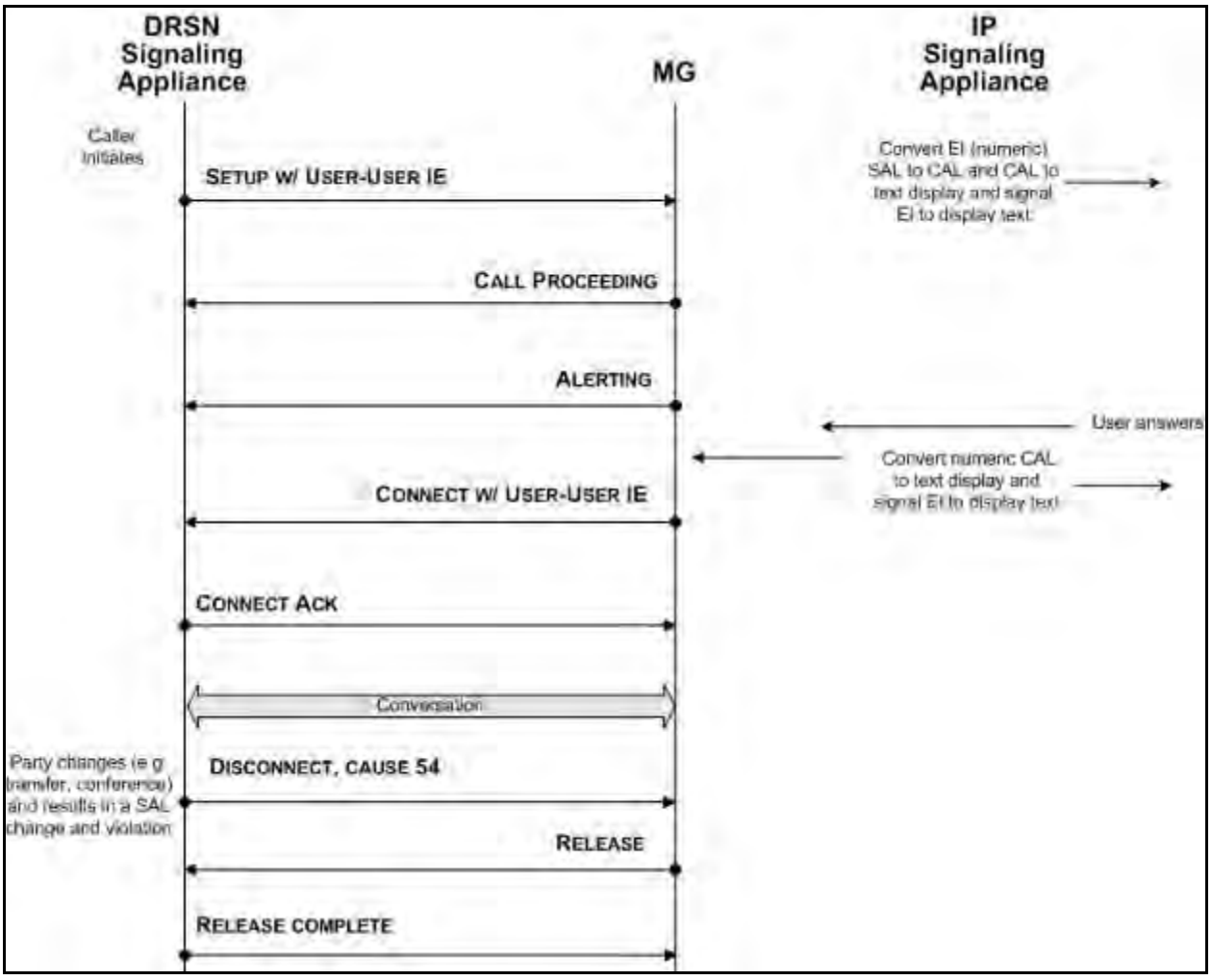


Figure B.5-8. Illustration of SAL Violation After Stable Call Resulting From DRSN Party Change

B.5.4.3.3 Changes During Call

Figure B.5-9, Illustration of a SAL Change During Call Resulting From DRSN Party Change, illustrates a SAL change during call because of DRSN party change. A DRSN party has performed an action that results in a new party and SAL becoming involved in the conversation.

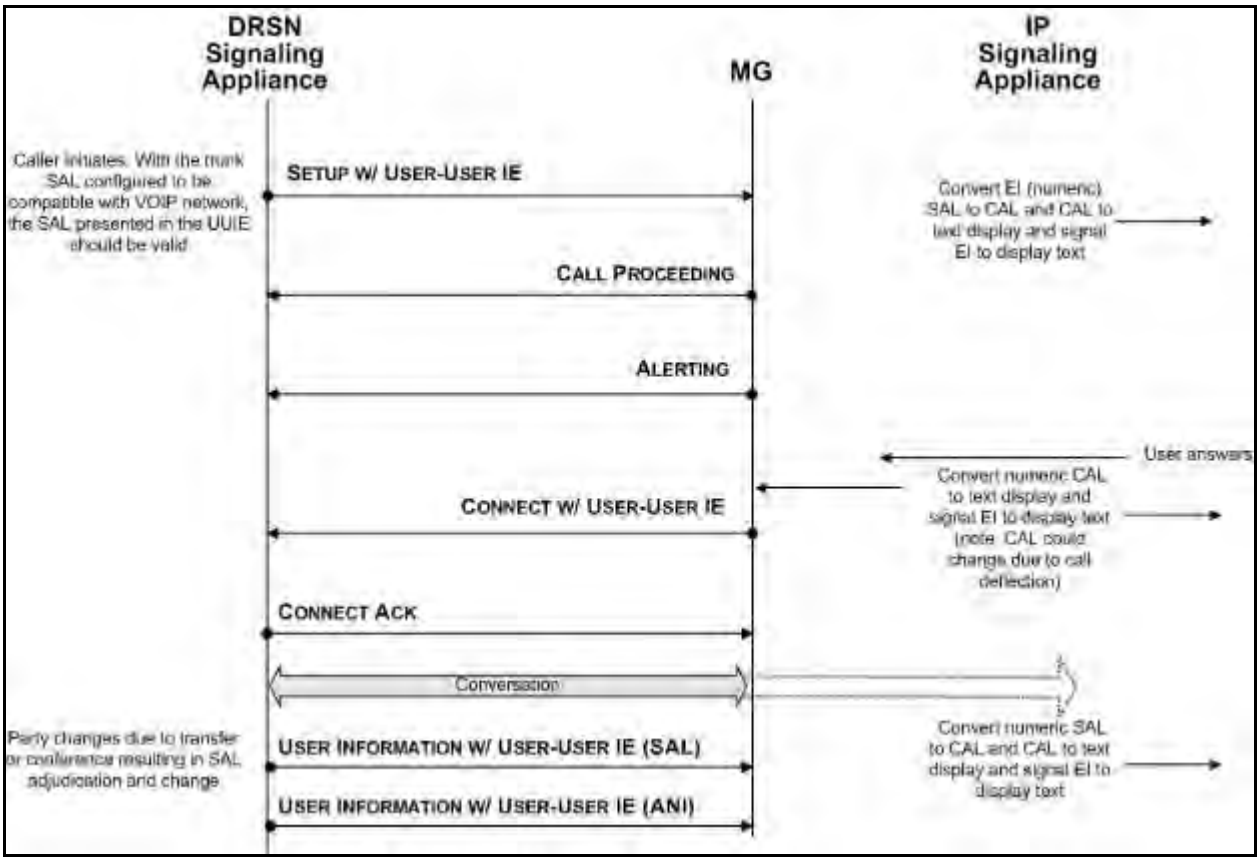


Figure B.5-9. Illustration of a SAL Change During Call Resulting From DRSN Party Change

B.5.5 Session Boundary Controller

All requirements for the SBC specified in Section 2, Session Control Products, apply to the CVVoIP system. The use SBCs are optional within the CVVoIP.

- Where used, the SBC must be dedicated to CVVoIP services and not shared with SBU services.

B.5.6 Addressing Schema for SC

The following additional requirements are unique to the classified SCs:

CLA-000340 [**Required: SC**] The classified SCs must have a DRSN and CVVoIP (as established by VoSIP) numbering plan capability.

CLA-000350 [**Required: SC**] The classified SCs must have interoperability with the Tactical GBNP.

CLA-000360 [**Required: SC**] The classified SCs must have SIPRNet IP addressing schema.

B.5.7 Network Management

All requirements specified in Section 2.17, Management of Network Appliances, for NM apply to the classified SC, SBC, and Tier0 SS.

The following unique features are required for classified:

CLA-000370 [**Required: SC**] The SC shall generate an alarm message indicating that a registered CVVoIP EI has been unplugged.

CLA-000380 [**Required: SC**] The SC shall generate an alarm message indicating that a registered CVVoIP EI that was previously unplugged has been plugged back in.

B.5.8 Voice Quality

CLA-000390 [**Required**] Because intelligibility of voice communications is critical to C2, the voice service quality rating, on at least 95 percent of the voice sessions, will have a MOS IAW the following scenarios:

a. Fixed-to-Fixed – 4.0.

b. Fixed-to-Deployable – 3.6.

c. Deployable-to-Deployable – 3.2.

CLA-000400 [**Required**] The method used for obtaining the MOS shall be in accordance with the DoD Information Technology Standards Registry (DISR) mandated standard International Telecommunications Union – Telecommunication (ITU-T), P.800, "Methods for Subjective determination of Transmission," August 1996.

NOTE: The current method used is the E-Model for Fixed-to-Fixed scenarios and P.862 for Deployable scenarios.

The measurement of voice quality shall conform to the requirements found in Section 2.19.3.1.1, Quality of Service.

B.5.9 Call Setup Time

The following call setup times apply to the classified VVoIP network:

- For SC intraenclave calls, the average delay should be no more than 1 second. For the 95 percent of calls, the delay should not exceed 1.5 seconds during normal traffic conditions.
- For interenclave and worldwide calls within the classified environment, average delay should not exceed 6 seconds, with 95 percent of calls not to exceed 8 seconds during normal traffic conditions.

B.5.10 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.

CLA-000410 [**Optional**] If the classified Edge system appliance supporting VVoIP uses an Ethernet interface for connecting to the Local Area Network (LAN), then its Network Interface Card (NIC) MTU size shall be set to 1280 bytes.

NOTE: This will allow for overhead associated with encryptors or Virtual Private Networks (VPNs).

CLA-000420 [**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 Differentiated Services Code Point (DSCP) discriminators exist between ROUTINE and above ROUTINE VVoIP sessions across the encryption boundaries (i.e., HAIPE).

Figure B.5-10, Addition of Encryption Within the Network Infrastructure, illustrates where encryption elements fit within the current network design.

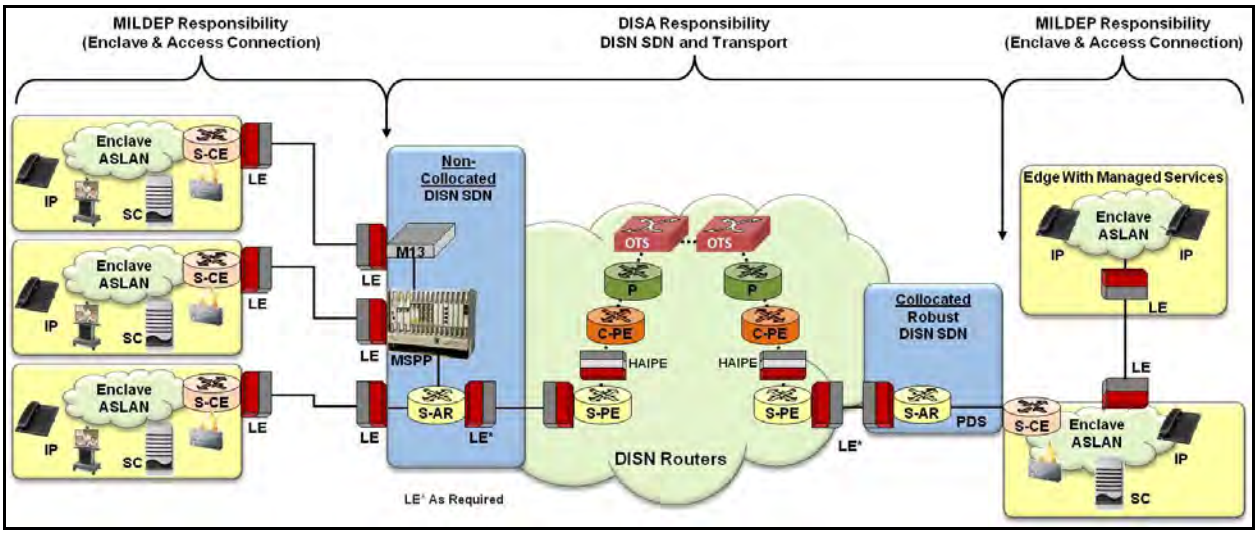


Figure B.5-10. Addition of Encryption Within the Network Infrastructure

B.5.11 Unique Information Assurance Requirements for CVVoIP

All Information Assurance requirements are specified in Section 4, Information Assurance. In addition, the following requirements are unique to the CVVoIP services:

CLA-000430 [**Required: EI**] The product shall be capable of being enabled or disabled using two-or three-factor authentication.

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

CLA-000440 [**Required: EI**] If the product supports an enable or disable code, the enable code shall be unique for that facility.

CLA-000450 [**Required: EI**] If the product supports an enable or disable code, the code shall be able to be modified by an authorized authority.

CLA-000460 [**Required: EI**] If the product supports an enable or a disable code, the product shall have a configurable code aging parameter, and the default shall be 90 days.

CLA-000470 [**Optional: SC, EI**] The product shall be capable of using three-factor authentication to include Public Key Infrastructure (PKI) certificates and biometric mechanisms for authenticating user credentials to the SC via the EI.

NOTE: The SC is responsible for the authentication decisions. The method for authenticating users with their PKI certificate is a vendor decision because of the immaturity of the current standards. Vendors may choose to implement user authentication using PKI certificates as described in Request for Comments (RFCs) 3261 or 3893.

CLA-000480 [**Required: E**I] The product shall be capable of meeting the DoD Public Key Enabled (PKE) requirements for PKI-based authentication.

NOTE: Public Key Infrastructure is required for EIs, whereas in the SBU it is optional. In summary, the EI is required to support PKI and all the PKI requirements apply.

CLA-000490 [**Optional: Tier0 SS, DSSS, SC, MG, BC**] The product 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.

CLA-000500 [**Required: Tier0 SS, DSSS, SC, MG, BC**] If the product supports classified users, the system shall be capable of ensuring that all unused network access device connections or physical ports are secured appropriately from unauthorized use by one of the following methods listed in preferential order:

d. Ports are disabled (i.e., shut down).

e. Ports are assigned to an unused Virtual LAN (VLAN), as applicable.

f. A MAC-based port security is used on active ports.

g. Port authentication is used by using 802.1X.

h. A VLAN Management Policy Server (VMPS) is used.

CLA-000510 [**Required: Tier0 SS, DSSS, SC, 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:

i. Invalid user authentication attempt.

j. Unauthorized attempts to access system resources.

k. Changes made in a user's security profile and attributes.

l. Changes made in security profiles and attributes associated with an interface or port.

m. Changes made in access rights associated with resources (i.e., privileges required of a user and an interface or port to access).

n. Changes made in system security configuration.

o. Creation and modification of the system resources performed via standard operations and maintenance procedures.

p. Disabling a user profile.

q. Events associated with privileged users.

CLA-000520 [**Optional**] If the system contains resources that are deemed mission critical (e.g., a risk analysis classifies it critical), then the system should log any events associated with access to those mission-critical resources:

r. Successful login attempts.

s. Failed logon attempts to include the following:

(1) Failed logon attempt because of an excessive number of logon attempts.

(2) Failed logon attempt because of blocking or blacklisting of a user ID.

(3) Failed logon attempt because of blocking or blacklisting of a terminal.

(4) Failed logon attempt because of blocking or blacklisting an access port.

t. Logouts.

u. Remote system access.

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

CLA-000530 [**Required: Tier0 SS, DSSS, SC, MG, BC, R, LS**] The security log event record shall be capable of including at least the following information:

v. Date and time of the event (both start and stop).

w. User ID including associated terminal, port, network address, or communication device.

x. Event type.

y. Names of resources accessed.

z. Success or failure of the event.

aa. Origin of the request (e.g., terminal ID).

NOTE: Only the last item is an addition for the CVVoIP (origin of the request).

CLA-000540 [**Required: Tier0 SS, DSSS, SC, MG, BC, R, LS**] The product shall be capable of supporting an out-of-band (OOB) or direct connection method for product device management.

CLA-000550 [**Optional: Tier0 SS, DSSS, SC, MG, BC, R, LS**] If the product 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.

CLA-000560 [**Optional: R**] If the product uses an OOB management method, the product shall be capable of limiting management connections to authorized source IP addresses.

CLA-000570 [**Optional: R**] If the product uses an OOB management method, the product shall be capable of maintaining a separation between the management and production networks.

NOTE: This requires physically separate networks.

CLA-000580 [**Optional: Tier0 SS, DSSS, SC, MG, BC, R, LS**] If the product uses an OOB management method, it shall be capable of ensuring system management access using the following four security restrictions:

a. Role-based authenticated access control.

b. Strong two-factor authentication (e.g., Secure ID).

c. Encryption of management and logon sessions.

d. Auditing of security-related events.

CLA-000590 [**Optional: Tier0 SS, DSSS, SC, MG, BC, R, LS**] If the product uses in-band management, it shall be capable of restricting the sessions to a limited number of authorized IP addresses.

B.6 CLASSIFIED AS-SIP-UNIQUE REQUIREMENTS

AS-SIP 2013, Section 4, SIP Requirements for AS-SIP Signaling Appliances and AS-SIP EIs, provides all the AS-SIP requirements, including those that apply to classified only. 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.

B.6.1 Classified Signaling Environment

The classified signaling environment is unique in that it will use a mix of 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 a 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 Section B.4.1, Signaling Design. The design is also depicted in Figure B.6-1, DISN CVVoIP Hybrid Signaling Design.

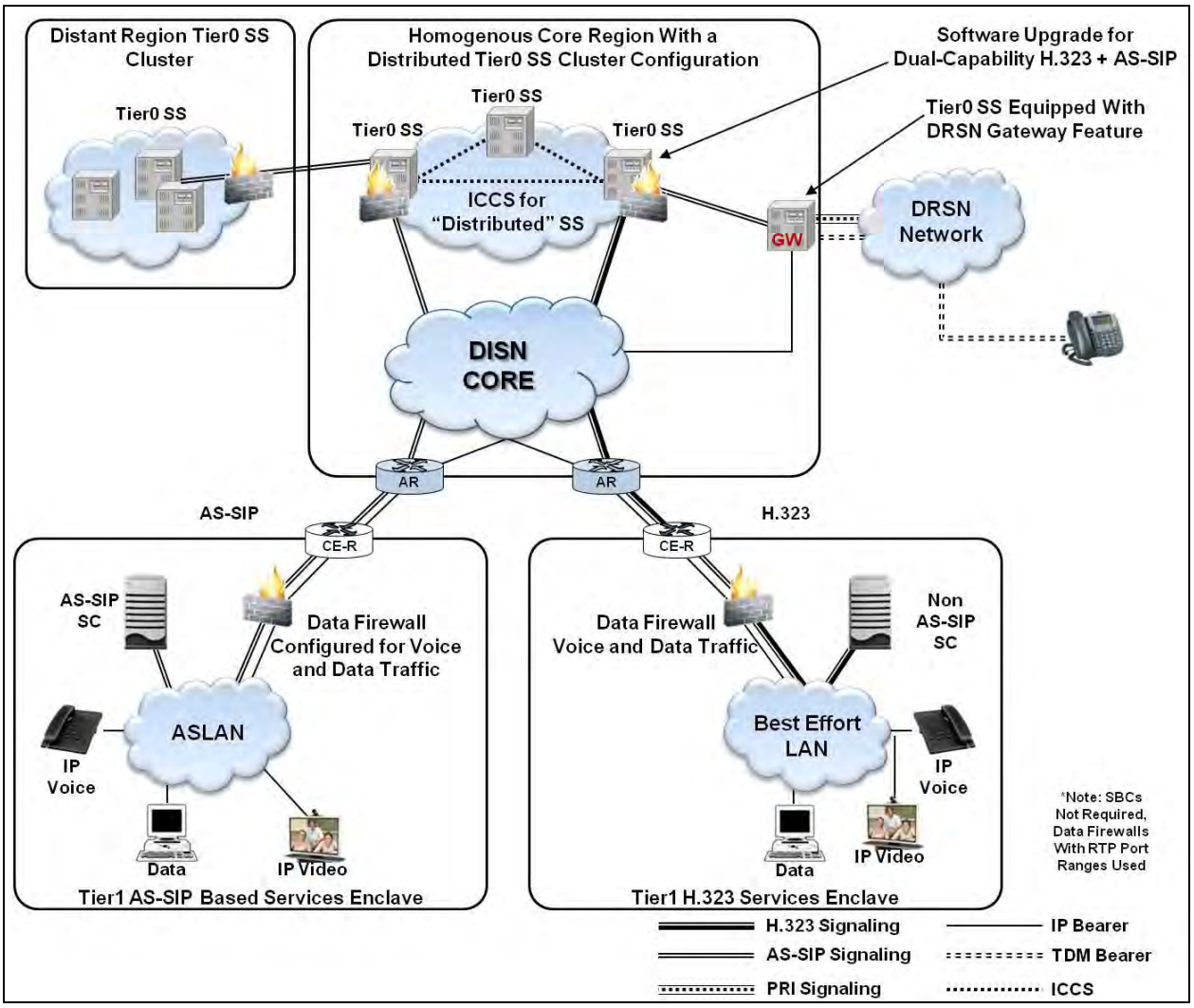


Figure B.6-1. DISN CVVoIP Hybrid Signaling Design

To simplify the signaling path description, the term Tier0 SS from here on refers to a geographic clustered Tier0 SS. (NOTE: During a transition period, H.323 and AS-SIP will coexist at certain locations.) All session (call) signaling messages received by an SC from local EIs and intended for a destination outside the secure service enclave are sent by the SC 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 SC or to a Tier0 SS located in a different geographic area; this Tier0 SS then, in turn, forwards the message to the distant-end SC. Similarly, all session (call) signaling messages sent from a remote location and intended for IP EIs associated with a given SC will be routed to the Tier0 SS assigned to the destination SC and the Tier0 SS will forward the AS-SIP signaling messages to the destination SC.

B.6.1.1 IP Signaling Path Reference Cases

Based on the top-level signaling design depicted in Section B.6.1, Classified Signaling Environment, the signaling paths that must be supported to provide the classified VVoIP services are identified in Figure B.6-2, IP Signaling Path Reference Illustration, and Table B.6-1, Reference Case: IP-to-IP Calls Over an IP Backbone.

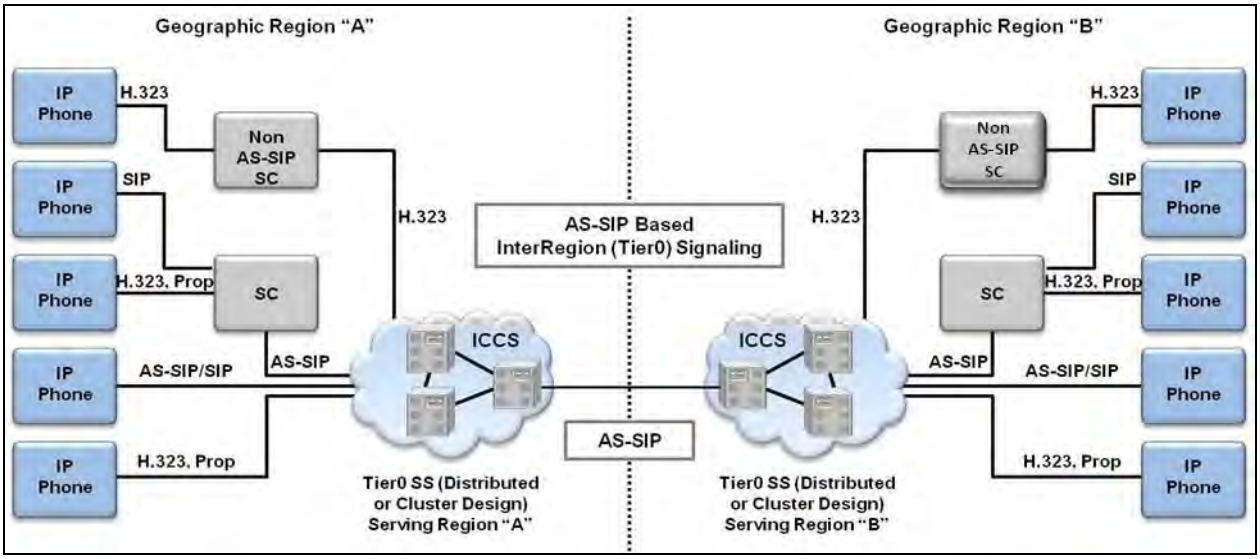


Figure B.6-2. IP Signaling Path Reference Illustration

Table B.6-1. Reference Case: IP-to-IP Calls Over an IP Backbone

REF. CASE	ORIGINATOR PHONE	ORIGINATOR SIGNALING	NETWORK SIGNALING AND CALL PATH							TERMINATOR SIGNALING	TERMINATOR PHONE
1A	IP phone	SIP	SC	AS-SIP	Tier0 SS	AS-SIP	Tier0 SS	AS-SIP	SC	SIP	IP phone
1B	IP phone	SIP	SC	AS-SIP	Tier0 SS	AS-SIP	Tier0 SS	AS-SIP	SC	H323, Prop.	IP phone
1C	IP phone	SIP	SC	AS-SIP	Tier0 SS	AS-SIP	Tier0 SS			SIP	IP phone
1D	IP phone	SIP	SC	AS-SIP	Tier0 SS	AS-SIP	Tier0 SS			H323, Prop.	IP phone
1E	IP phone	H323, Prop.	SC	AS-SIP	Tier0 SS	AS-SIP	Tier0 SS	AS-SIP	SC	SIP	IP phone
1F	IP phone	H323, Prop.	SC	AS-SIP	Tier0 SS	AS-SIP	Tier0 SS	AS-SIP	SC	H323, Prop.	IP phone
1G	IP phone	H323, Prop.	SC	AS-SIP	Tier0 SS	AS-SIP	Tier0 SS			SIP	IP phone
1H	IP phone	H323, Prop.	SC	AS-SIP	Tier0 SS	AS-SIP	Tier0 SS			H323, Prop.	IP phone
1I	IP phone	SIP			Tier0 SS	AS-SIP	Tier0 SS	AS-SIP	SC	SIP	IP phone
1J	IP phone	SIP			Tier0 SS	AS-SIP	Tier0 SS	AS-SIP	SC	H323, Prop.	IP phone

REF. CASE	ORIGINATOR PHONE	ORIGINATOR SIGNALING	NETWORK SIGNALING AND CALL PATH							TERMINATOR SIGNALING	TERMINATOR 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	SC	SIP	IP phone
1N	IP phone	H323, Prop.			Tier0 SS	AS-SIP	Tier0 SS	AS-SIP	SC	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	SC	AS-SIP	Tier0 SS	AS-SIP			SC	SIP	IP phone
2B	IP phone	SIP	SC	AS-SIP	Tier0 SS	AS-SIP			SC	H323, Prop.	IP phone
2C	IP phone	SIP	SC	AS-SIP	Tier0 SS					SIP	IP phone
2D	IP phone	SIP	SC	AS-SIP	Tier0 SS					H323, Prop.	IP phone
2E	IP phone	H323, Prop.	SC	AS-SIP	Tier0 SS	AS-SIP			SC	SIP	IP phone
2F	IP phone	H323, Prop.	SC	AS-SIP	Tier0 SS	AS-SIP			SC	H323, Prop.	IP phone
2G	IP phone	H323, Prop.	SC	AS-SIP	Tier0 SS					SIP	IP phone
2H	IP phone	H323, Prop.	SC	AS-SIP	Tier0 SS					H323, Prop.	IP phone
2I	IP phone	SIP			Tier0 SS	AS-SIP			SC	SIP	IP phone
2J	IP phone	SIP			Tier0 SS	AS-SIP			SC	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			SC	SIP	IP phone
2N	IP phone	H323, Prop.			Tier0 SS	AS-SIP			SC	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

B.6.2 Differences Between SBU and Classified AS-SIP Requirements

AS-SIP 2013, Section 4, SIP Requirements for AS-SIP Signaling Appliances and AS-SIP EIs, defines both SBU and classified requirements. The classified-specific requirements are defined in AS-SIP 2013, Sections 4.3.1.4 and 4.3.1.5 (Route Header Requirements); AS-SIP 2013, Section 4.3.2, (Proxy Require header), AS-SIP 2013 Section 4.4.1 requirement number AS-SIP 001480, (418 response); AS-SIP 2013, Section 4.5.2 (SIP Preconditions); AS-SIP, Section 4.7 (CAL Requirements); and AS-SIP 2013, Section 6.1.1.5 (Precedence Levels). In addition, sections specifying “domain name,” “namespace,” and/or domain subfields define “uc” as Required for the SBU environment, and “cuc” as Required for the classified environment.

The following sections describe additional differences between the SBU and classified AS-SIP requirements.

B.6.2.1 Nomenclature

The classified environment uses the term Tier0 SS (Tier0 SS) while AS-SIP 2013, Section 4, SIP Requirements for AS-SIP Signaling Appliances and AS-SIP EIs, uses the term SS to denote the SBU environment.

The classified environment uses "cuc" as the network domain name, while the SBU environment uses "uc" as the network domain name.

NOTE: Reference cases 2A through 2P (see Table B.6-1, Reference Case: IP-to-IP Calls Over an IP Backbone) represent the call paths when the same Tier0 SS serves both the calling party calling party's SC (or the calling party's EI directly) and the called party's SC (or the called party's EI directly). Reference cases are not shown for non-AS-SIP SCs.

B.6.2.2 Route Header Requirements

The Route header requirements for SCs and SSs are predicated on the SBU network design in which SBCs are required at each enclave having at least one AS-SIP signaling appliance.

The current CVVoIP network design defines SBCs as optional; therefore, it is anticipated that during the transition toward full implementation of AS-SIP within the classified network there will be instances where SBCs may or may not be present at all locations encountered on an E2E AS-SIP call. Therefore, the classified requirements must include specifications for the various permutations of Route headers for the situations where an SBC is present at a Tier0 SS or at an SC, or at both. If there is not an SBC at either location and there are no intermediary AS-SIP signaling appliances between an SC and its Tier0 SS, then there may not be a need for a Route header. (See AS-SIP 2013, Sections 4.3.1.4 and 4.3.1.5)

B.6.2.3 Proxy Require

In adherence with the enumerated RFCs, the AS-SIP EIs MUST be capable of generating, receiving, and processing SIP header fields as defined in AS-SIP 2013, Section 4.3.2:

The "Proxy-Require" must be generated for the classified network only.

B.6.2.4 418 Response

AS-SIP 2013, Section 4.4.1, requirement AS-SIP 00148 states (NOTE: This paragraph applies to classified only), "The SCs MUST support the generating of a 418 (Incompatible CAL) response code upon receipt of an INVITE 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 [User Agent Server] UAS or to the access-level supported for the routing domain that failed resolution at an intermediate Tier0 SS."

B.6.2.5 SIP Preconditions

AS-SIP 2013, Section 4.5.2, states that implementation of preconditions is conditional for the classified network. [RFC 3312]

B.6.2.6 CAL Requirements

AS-SIP 2013, Section 4.9, defines CAL requirements. The purpose of the CAL header is to convey the classification level for a telephony or video session between the parties to the session.

B.6.2.7 Precedence Levels

AS-SIP 2013, Section 6.1.1.5, defines precedence level requirements for the classified network. The classified adds a FLASH OVERRIDE-OVERRIDE (FOO) precedence level.

B.6.2.8 SIP URI Mapping of Telephone Number

AS-SIP 2013, Section 4.6, SIP URI and Mapping of Telephone Number Into SIP URI, describes the SIP Uniform Resource Identifier (URI) and telephone number mapping requirements. The following modifications apply to the classified version of AS-SIP:

- Instead of uc.mil, use cuc.mil in the host name for classified SIP URIs.
- Instead of uc.mil, use cuc.mil with the phone-context parameter.
- The SBU Requirements [SIP-46170] and [SIP-46180] apply to interworking of telephone numbers on the Public Switched Telephone Network (PSTN) and they are conditional in the classified specification.
- The 3-digit 911 and 411 numbers are conditional in the classified specification. There is no current requirement to support access to 911 services in the classified network.

B.6.2.9 64 Kbps Transparent Calls (Clear Channel)

There are no requirements for clear channel service within the classified environment; therefore, the SBU AS-SIP requirements defined in Section 4.7, 64 Kbps Transparent Calls (Clear Channel), do not apply.

B.6.2.10 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 requirements defined in Section 4.8, Transport of Route Code Information over AS-SIP, do not apply.

B.6.2.11 Classified VoIP Information Signals

Table 6.1-4, UC Information Signals (from Section 4, SIP Requirements for AS-SIP Signaling Appliances and AS-SIP EIs), has been expanded for the classified environment to include secure dial tone, line busy tone, and reorder tone requirements as outlined in DRSN documentation. Table B.6-2, CVVoIP Information Signals, is the expanded version.

Table B.6-2. CVVoIP Information Signals

SIGNAL	FREQUENCIES (HZ)	SINGLE TONE LEVEL	COMPOSITE LEVEL	INTERRUPT RATE	TONE ON	TONE 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 Tone	440 + 620 (Mixed)	-19 dBm0	-16 dBmo	Continuous	Steady on	
Call Waiting (Precedence Call)	440	-13 dBm0		Continuous at 6 IPM	100 ± 20 ms Three Bursts	9700 ms
Conference Disconnect Tone	852 and 1336 (Alternated at 100 ms Intervals)	-24 dBm0		Steady on	2000 ms (per occurrence)	
Override Tone	440			Continuous at 6 IPM	2000 ms (followed by) 500 ms on and 7500 ms off	
Camp On	440	-13 dBm0			Single burst 0.75 to 1 sec	
LEGEND Hz: Hertz IPM: Impulse Per Minute ms: Millisecond sec: Second						

B.6.2.12 Policing of Call Count Thresholds

Section 7, SS 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.

B.7 DRSN SWITCHES AND PERIPHERAL DEVICES

Requirements for DRSN switches and peripheral devices are not included in the UCR. Specifications for these products are available on a need-to-know basis from the DISA NS DRSN Single Service Manager.

B.8 PHYSICAL CONSTRUCTION UNIQUE REQUIREMENTS

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

- All cabling must follow PDS guidelines.
- Cabling or interfaces leaving a secure enclave must be encrypted.
- Equipment must comply with TEMPEST requirements.

B.9 UC SECURE PRESET CONFERENCE

This section provides descriptions of network configuration requirements that will enable SBU voice subscribers equipped with an NSA Type I encryption device to conference in the secure mode.

B.9.1 Introduction

The DoD voice community has a need to communicate in a secure mode with multiple subscribers and to communicate transparently with other DoD secure voice networks.

The DoD SBU voice network is the DSN that is a part of the DoD Unified Communications. The DSN provides the capability for SBU communications between its subscribers as a standard feature. The DSN also provides the capability for unique subscribers to communicate in a secure mode using various encryption devices. The UC SBU voice currently is not equipped with the capability for any subscriber type to communicate simultaneously with multiple subscribers on a secure mode either on a preset or meet-me basis and, it is not equipped to communicate transparently with other secure networks (i.e., VoSIP, DRSN).

The DoD established the need for the UC SBU voice subscribers to communicate with multiple subscribers in a secure mode that will enhance the current UC SBU voice subscriber feature that

allows voice communications beyond the SBU classification based on the NSA accreditation level of the device used for the UC SBU voice session.

Current capabilities of the UC SBU voice for subscriber communications with multiple subscribers will have to be expanded to implement a secure mode feature of the existing capabilities. This section describes and outlines the necessary enhancements needed to comply with the DoD mandate for UC SBU voice secure communications that will allow communications above the SBU classification.

B.9.2 Feature Requirements

A UC SBU voice secure interface(s) will provide the capability for UC SBU voice subscribers equipped with an NSA Type I encryption device to communicate in the following ways:

- In the secure mode with multiple subscribers who are equipped with interoperable NSA devices on a preset Directory Number (DN) assigned to the originator to initiate the session.
- With multiple subscribers equipped with interoperable NSA devices on a "meet-me" basis.
- To another network subscriber that uses interoperable NSA devices.

To reduce the risk of new development for such a feature, it is recommended that such an interface operates at the 56 Kbps rate via a standard Telcordia Technologies GR-506-CORE 2W loop and that optional interface(s) can use a single DS0 off an ISDN PRI also, using the ANSI T1.619a protocol. The interface is fully automated and transparent to the subscriber and meets the DoD standards for secure communications that use NSA Type I devices.

The following description expands the current UCR requirements for conferencing and adds the UC SBU Voice Secure Gateway Interface. The conferencing features are expanded to include a "SECURE" environment for the UC SBU voice subscribers who are equipped with an NSA Type I encryption device to conduct a secure preset conference session and to conduct a "random" secure conference session using the "meet-me" conference bridge.

The UC SBU Voice Secure Gateway allows for a UC SBU voice subscriber equipped with an NSA Type I encryption device to communicate with a secure system subscriber equipped with the compatible encryption device provided that the secure system has a direct DS0 or DS1 (PRI) interface. These additional features provide the means for the current UC SBU voice subscribers who are equipped with an NSA Type I encryption device to conduct secure sessions up to the classification allowed by the NSA Type I encryption device.

The current secure interface for typical applications is depicted in Figure B.9-1, Examples of Current Secure Interface Arrangements, and Figure B.9-2, Additional Examples of Current Secure Interface Arrangements. These interfaces are not vendor unique and are shown as typical implementations of these requirements, and are not intended to be the only implementation that satisfies the requirements.

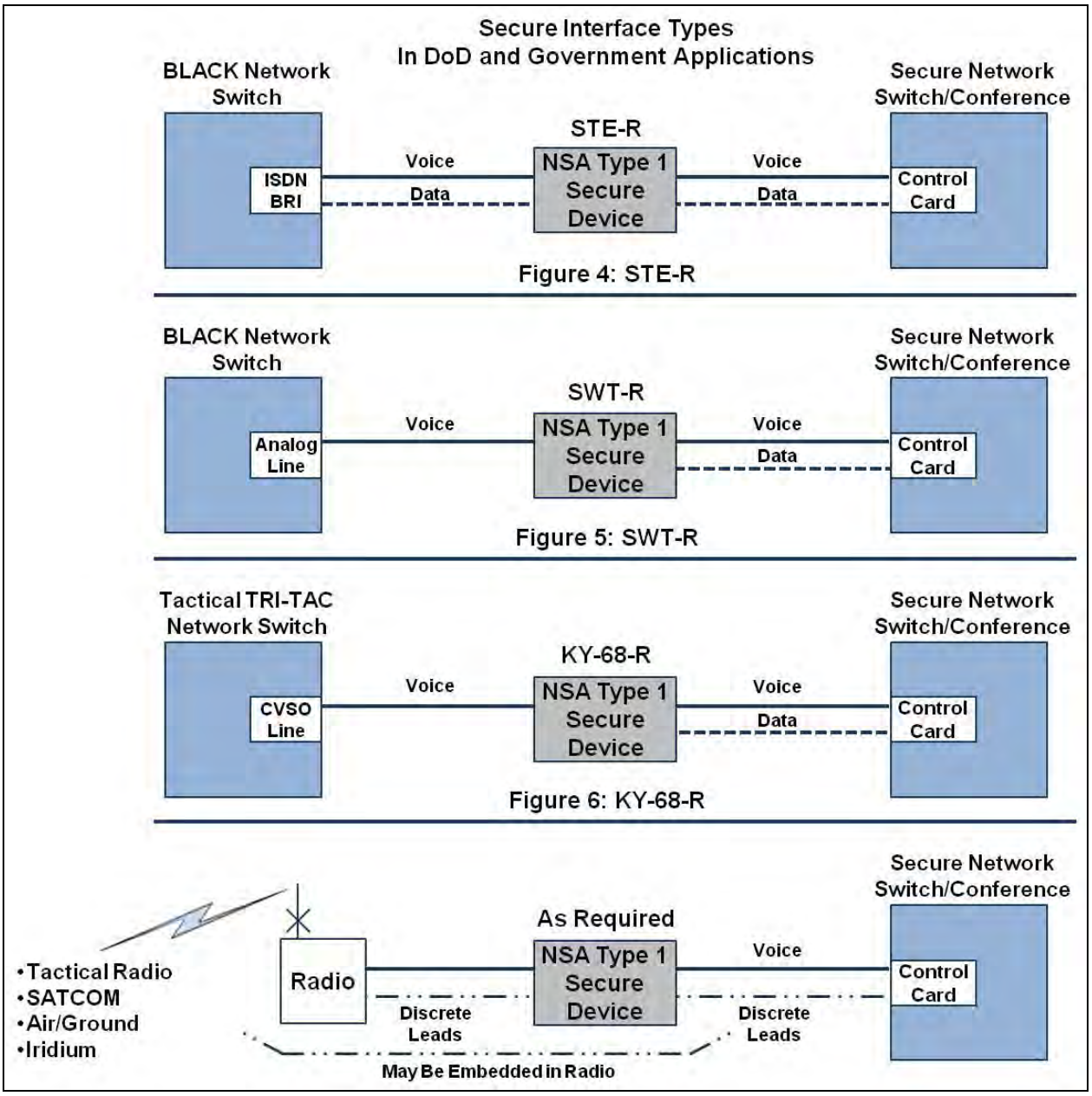


Figure B.9-1. Examples of Current Secure Interface Arrangements

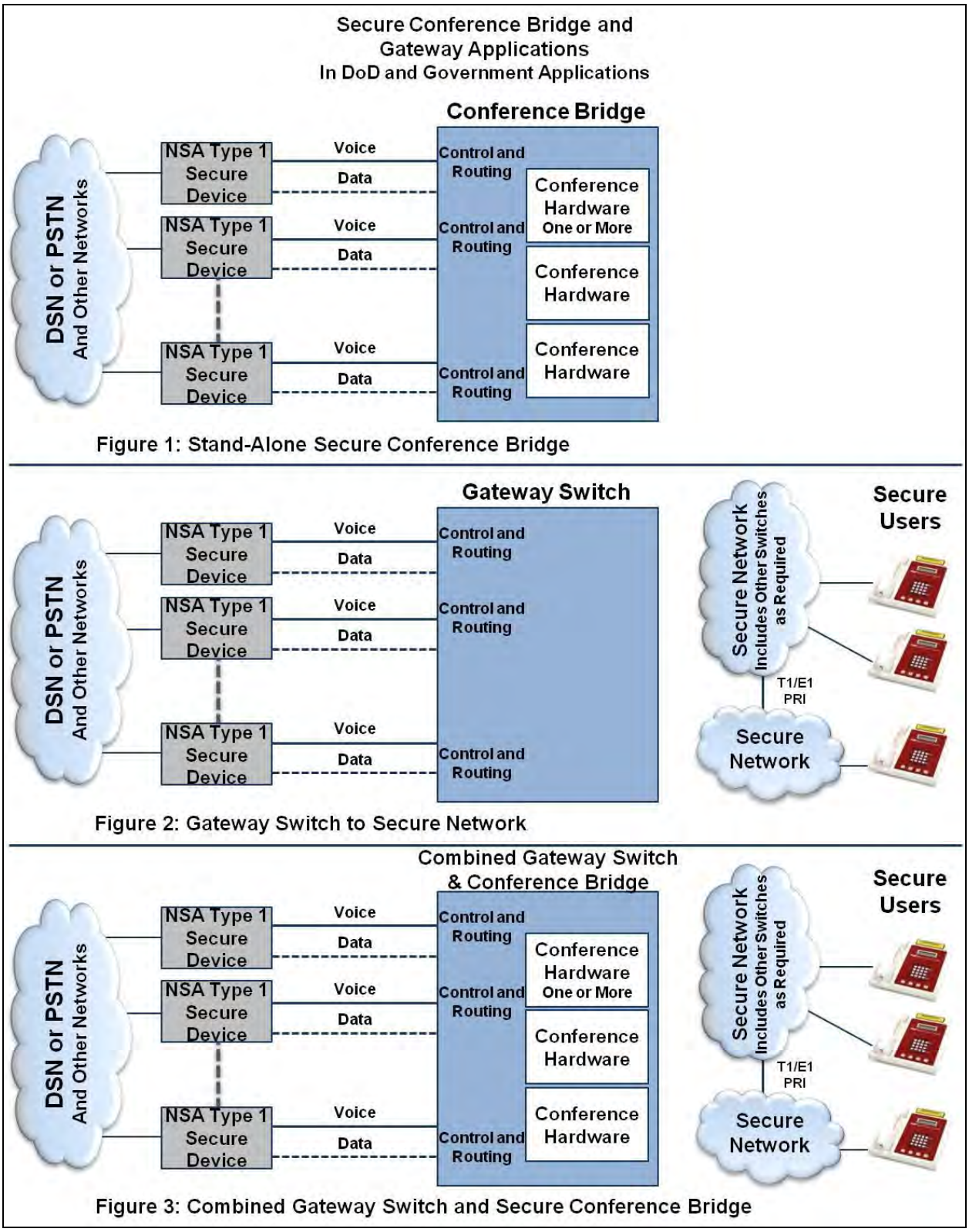


Figure B.9-2. Additional Examples of Current Secure Interface Arrangements

B.9.3 UC SBU Voice Secure Conference Features

(Features listed in this section are in addition to the features listed in, Section 3.4, UC Audio and Video Conference System Requirements).

(Network system interface with secure preset and meet-me conference bridges that allows UC SBU voice users with an NSA Type I encryption device to originate or participate in conference sessions across the UC voice multi-networks.)

B.9.3.1 Feature Description

The secure conference bridge system (preset or meet-me) is equipped with individual ports with automated supervision and control interfaces that conform to standard telephony two-wire loop (DS0 minimum rate of 56 Kbps) (IAW Telcordia Technologies GR-506-CORE). The system is equipped with an automated "ON-HOOK" and "OFF-HOOK" type function and can be any one of the specified GR-506-CORE two-wire signaling types. The port interface provides for automated supervision and control of the incoming and outgoing signaling that conforms to the line signaling, specified in Telcordia Technologies GR-506-CORE, for Dual Tone Multifrequency (DTMF) for originating a call. Call origination can be from the conferee participant port only of the preset bridge. Meet-me bridge ports do not have an originating feature. Calls that are originated to or from the preset bridge are always secure via control and supervision of the NSA Type I encryption device used. Calls terminating to a meet-me bridge port are equipped with an NSA Type I encryption device that ensures only encrypted sessions will be able to communicate, and non-encrypted sessions are not allowed to be cut-through into the bridge.

Preset and meet-me bridges are equipped with an optional ISDN DS1 interface user-network interface where the interface structure is composed of multiple B-channels and one D-channel. The bit rate of the D-channel in this structure is 64 Kbps. When a 1544-Kbps PRI is provided, the interface structure is 23B+1D.

Requirements for this feature shall be IAW Telcordia Technologies SR-NWT-002120, SR-NWT-002343, and TR-NWT-001268. The UC SBU voice user-to-network signaling physical layer specification for the PRI operating at 1.544 Mbps shall be ANSI T1.408 and ANSI T1.619a.

The PRI provides for automated supervision and control of the incoming and outgoing signaling that conforms to the line signaling specified in Telcordia Technologies GR-506-CORE for DTMF for originating a call via the control of the selected D-channel of the PRI. Call origination can be from either input of the interface. Calls that are originated to or from the gateway are always secure via control and supervision of the NSA Type I encryption device used. The NSA Type I PRI channelized encryption device ensures that only encrypted sessions will be able to communicate, and non-encrypted sessions are not allowed to be cut-through on the talk-path of the session.

B.9.4 UC Preset Conference Bridge Requirements

The bridge shall provide the following capabilities (see the notional diagram in Figure B.9-3, Secure Preset Conference Capability):

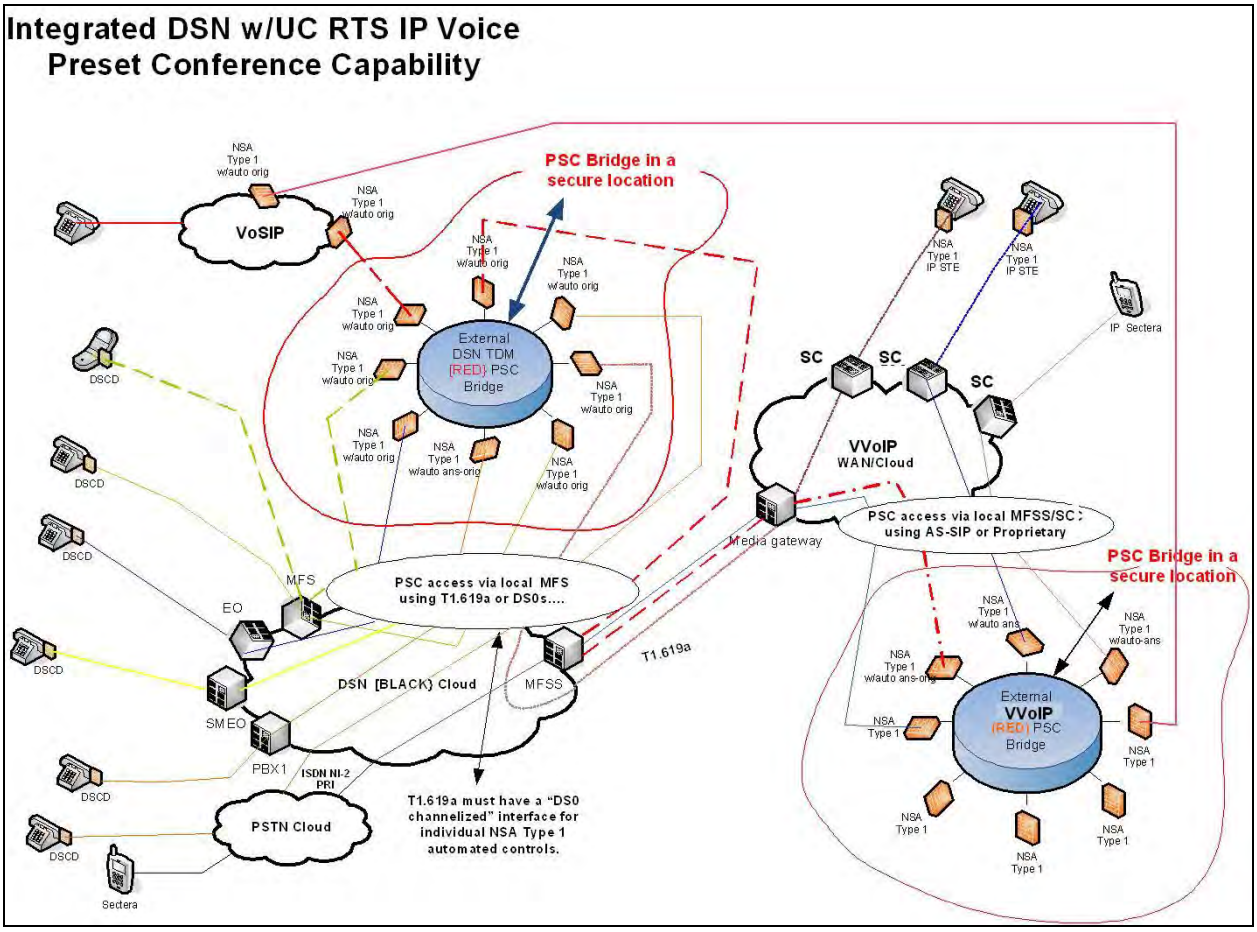


Figure B.9-3. Secure Preset Conference Capability

1. All bridge port access shall be via an NSA Type I-approved device that interoperates with the caller or called party's NSA-compatible device for encryption and supervisory control of the bridge ports IAW the features listed in this document (i.e., VoSIP, VVoIP, and Tactical WAN access must be via the NSA-compatible device).
2. Each bridge shall be equipped with a unique preset conference originator port (i.e., the port that starts the conference) and preset conference participant ports (i.e., the ports that dial the DN of the participant) that establish a conference up to the maximum number of participants as specified previously.
3. The bridge shall be programmable to establish an originating preset conference based on the conference ID that accessed the conference originating port of the bridge.
4. Conference ID shall be based on the originator's calling ID and the originator's dialed code.

5. A conference dialed code shall be able to establish a preset conference consisting of the maximum number of participants (see Section 3.4) and shall use multiple bridge ports when required for the conference.
6. Conference bridge ports shall be limited to the maximum number of participants (see Section 3.4) based on the number of cascaded bridges required to connect the required quantity of participants.
7. The bridge shall provide a feature for the conference originator to selectively release (terminate) a participant. Such a feature must be interoperable with bridges that are cascaded.
8. The bridge shall provide a feature for the conference originator to selectively recall a participant. Such a feature must be interoperable across bridges that are cascaded.
9. The bridge shall provide a feature for the conference originator to selectively add on a participant. Such a feature must be interoperable with bridges that are cascaded.
10. The bridge shall provide a feature for the conference originator (when the originator is equipped with an alphanumeric display) to be informed of a participant's status (i.e., answer, disconnect). Such a feature must be interoperable with bridges that are cascaded.
11. The bridge shall be programmable for a minimum of a 100 preset conference dialed codes.
12. Bridge ports shall comply with Telcordia Technologies GR-507-CORE, Section 7.5 (inclusive), specifications that allow for remote or distant access to the bridge.
13. Bridge ports (conference originator and participant) shall be via DS0 allocations that may be via a T1.619a DS1 interface.
14. Each DS0 port access (originating and terminating) to the bridge shall be encrypted via an NSA Type I device.
15. Each bridge DS0 port (originating and terminating ports) shall interface with an NSA Type I encryption device that provides a fully automated supervision (answer and cut-through) control (this supervision control either can be before the actual bridge DS0 port interface to the DSN switch port or after the DS0 port interface to the bridge itself) that will permit the NSA Type I encryption device to encrypt the two-way conversation and allow the cut-through of the DS0 port into the bridge when the NSA device acknowledges and confirms that the connected line is cryptographically synchronized.
16. Each bridge DS0 port interface can be activated and put in-service only when it is connected serially with a NSA Type I encryption device (either automated provisioning or manual provisioning is allowed to provide the control).

B.9.5 UC Secure Meet-Me Conference Bridge Requirements

In addition to the requirements stated in Section 3.4, the bridge shall have the following capabilities (see Figure B.9-4, Secure Meet-Me Conference Arrangement, for a notional diagram):

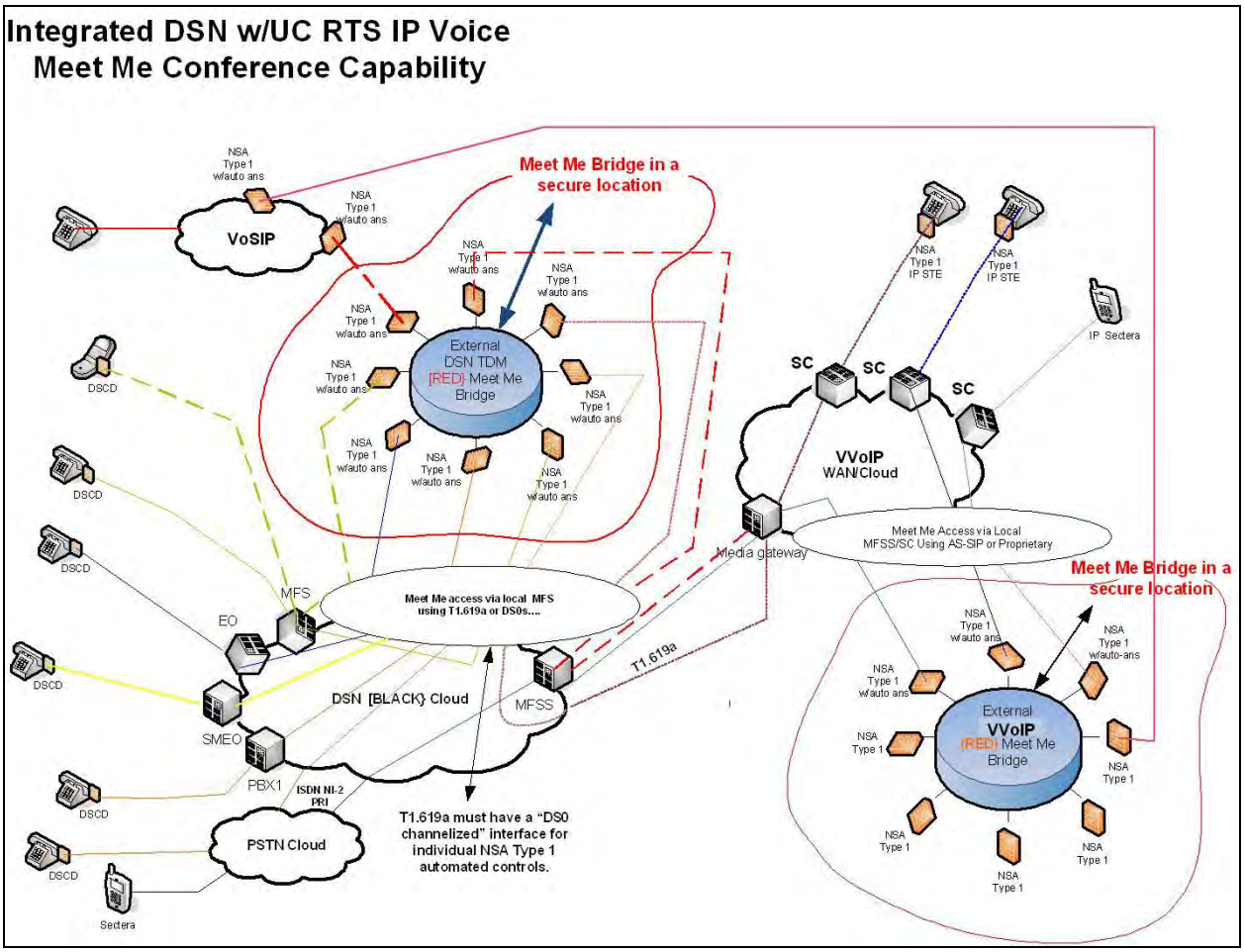


Figure B.9-4. Secure Meet-Me Conference Arrangement

1. All bridge port access shall be via an NSA Type I-approved device that interoperates with the caller or called party's NSA-compatible device for encryption and supervisory control of the bridge ports IAW the features listed in this document (i.e., VoSIP, VVoIP, and Deployed WAN access must be via the NSA-compatible device).
2. Bridge ports shall comply with Telcordia Technologies GR-507-CORE, Section 7.5 (inclusive), specifications that allow for remote or distant access to the bridge.
3. Each bridge shall be programmable to a specific number of participants.
4. Each bridge shall be configurable to cascade with other bridge(s) to expand the number of participants up to 100 participants. Cascading of bridges shall be via an NSA Type I encryption device.
5. Each bridge port access shall be assigned a unique DSN DN.
6. Each port access (originating and terminating) to the bridge shall be encrypted via an NSA Type I device.

7. Each bridge DS0 port (originating and terminating ports) shall interface with an NSA Type I encryption device that provides a fully automated supervision (answer and cut-through) control (this supervision control either can be before the actual bridge DS0 port interface to the DSN switch port or after the DS0 port interface to the bridge itself) that will permit the NSA Type I encryption device to encrypt the two-way conversation and allow the cut-through of the DS0 port into the bridge when the NSA device acknowledges and confirms that the connected line is cryptographically synchronized.
8. Each bridge DS0 port interface can be activated and put in-service only when it is connected serially with an NSA Type I encryption device (either automated provisioning or manual provisioning is allowed to provide the control).

B.9.6 UC Secure Network Gateway Requirements

(Network system interface that allows secure sessions across the UC multinetworks that are equipped with NSA Type I encryption devices.)

B.9.6.1 Feature Description

The gateway provides for UC SBU access to a secure classified system at the DS0 (minimum bit rate of 56 Kbps) or DS1 (PRI) bit rate using NSA Type I encryption devices. The DS0 interface uses a standard telephony 2-wire loop (IAW Telcordia Technologies GR-506-CORE) equipped with automated "ON-HOOK" and "OFF-HOOK" type function, and can be any one of the specified Telcordia Technologies GR-506-CORE two-wire signaling types. The DS1 interface uses an NI-2 PRI T1.619a protocol that uses "channelized DS0" NSA Type I encryption devices and is equipped with an automated D-channel-type signaling interface that controls the cut-through of the selected DS0 channel or session.

The DS0 interface provides for automated supervision and control of the incoming and outgoing signaling that conforms to the line signaling specified in Telcordia Technologies GR-506-CORE for DTMF for originating a call. Call origination can be from either input of the interface. Calls that are originated to or from the gateway are always secure via control and supervision of the NSA Type I encryption device used. The NSA Type I encryption device ensures that only encrypted sessions will be able to communicate, and non-encrypted sessions are not allowed to be cut-through on the talk path of the session.

The DS1 interface is an ISDN primary access interface and is an ISDN user-network interface in which the interface structure is composed of multiple B-channels and one D-channel. The bit rate of the D-channel in this structure is 64 Kbps. When a 1544-Kbps PRI is provided, the interface structure is 23B+1D.

Requirements for this feature shall be IAW Telcordia Technologies SR-NWT-002120, SR-NWT 002343, and TR-NWT-001268. The DSN user-to-network signaling physical layer specification for the PRI operating at 1.544 Mbps shall be ANSI T1.408 and ANSI T1.619a.

The PRI interface provides for automated supervision and control of the incoming and outgoing signaling that conforms to the line signaling specified in Telcordia Technologies GR-506-CORE for DTMF for originating a call via the control of the selected D-channel of the PRI. Call origination can be from either input of the interface. Calls that are originated to or from the gateway are always secure via control and supervision of the NSA Type I encryption device used. The NSA Type I PRI channelized encryption device ensures that only encrypted sessions will be able to communicate, and non-encrypted sessions are not allowed to be cut-through on the talk path of the session.

The UC Network Gateway shall have the following capabilities (see Figure B.9-5, Notional Diagram Illustrating Secure Network Gateway, for a notional diagram):

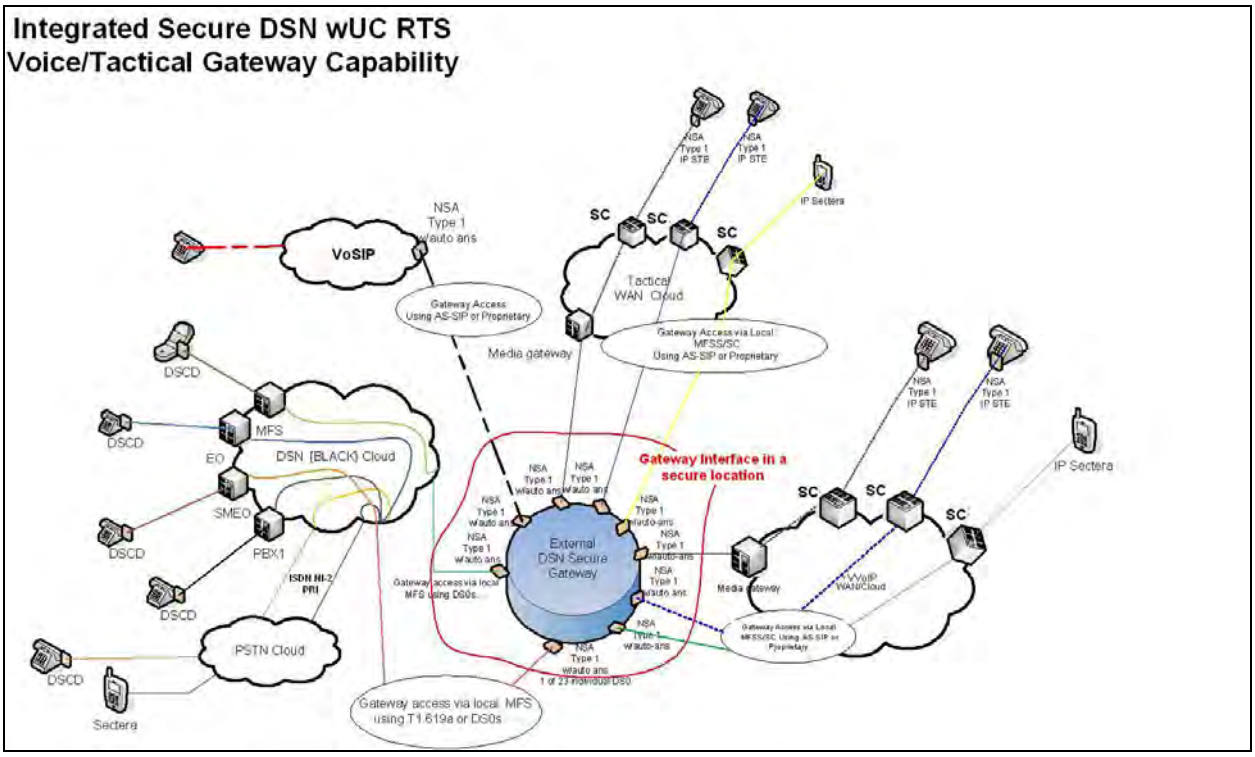


Figure B.9-5. Notional Diagram Illustrating Secure Network Gateway

1. All gateway interface port access shall be via an NSA Type I-approved device that interoperates with the caller or called party's NSA-compatible device for encryption and supervisory control of the bridge ports IAW the features listed in this document (i.e., VoSIP, VVoIP, and Tactical WAN access must be via the NSA-compatible device).
2. Each network secure gateway DS0 port (originating and terminating ports) shall interface with an NSA Type I encryption device that provides a fully automated supervision (answer and cut-through) control (this supervision control either can be before the actual gateway DS0 port interface to the DSN switch port or after the DS0 port interface to the gateway itself) that will permit the NSA Type I encryption device to encrypt the two-way

conversation and allow the cut-through of the DS0 port into the gateway when the NSA device acknowledges and confirms that the connected line is cryptographically synchronized.

3. The gateway interface shall operate at the DS0 (minimum bit rate of 56 Kbps) or DS1 (PRI) bit rate using NSA Type I encryption devices.
4. The DS0 interface shall comply with the standard telephony two-wire loop IAW Telcordia Technologies GR-506-CORE, GR-513-CORE, GR-1089-CORE, and ANSI T1.401-1993. The interface shall be equipped with an automated "ON-HOOK" and "OFF-HOOK" type function and can be any one of the specified GR-506-CORE two-wire signaling types.
5. Each DSN outgoing gateway interface shall be equipped with a unique DSN DN where the DN can provide a single port or multiple port access to the gateway device or system.
6. Each gateway port interface shall be equipped with the capability to provide automated supervision and control of the DSN outgoing connection that is interfaced with an NSA Type I encryption device. Such a control shall only allow cut-through of the session when the NSA Type I encryption device is synchronized cryptographically with the DSN's originator NSA Type I device.
7. Each gateway port interface shall be equipped with the capability to provide automated supervision and control of the non-DSN incoming connection to the DSN switch that is interfaced with an NSA Type I encryption device. Such a control shall only allow cut-through of the session when the NSA Type I encryption device is synchronized cryptographically with the DSN's terminator NSA Type I device.
8. Gateway ports shall comply with Telcordia Technologies GR-507-CORE, Section 7.5 (inclusive), specifications that allow for remote or distant access to the gateway.
9. Gateway ports (originator and terminator) shall be via DS0 allocations that may be via a T1.619a DS1 interface.
10. Each DS0 port access (originating and terminating) to the gateway that uses a T1.619a interface shall be encrypted via an NSA Type I device.
11. The DS1 interface shall be an ISDN primary access interface and is an ISDN user-network interface in which the interface structure is composed of multiple B-channels and one D-channel. The bit rate of the D-channel in this structure is 64 Kbps. When a 1544-Kbps PRI is provided, the interface structure is 23B+1D. Requirements for this feature shall be IAW Telcordia Technologies SR-NWT-002120, SR-NWT 002343, and TR-NWT-001268. The DSN user-to-network signaling physical layer specification for the PRI operating at 1.544 Mbps shall be ANSI T1.408 and ANSI T1.619a.
12. The PRI interface shall provide an automated supervision and control of the incoming and outgoing signaling that conforms to the line signaling specified in Telcordia Technologies GR-506-CORE for DTMF for originating a call via the control of the selected D-channel of the PRI. Call origination can be from either input of the interface. Calls that are originated to or from the gateway shall be "secure" via control and supervision of the NSA Type I

encryption device used. The NSA Type I PRI channelized encryption device ensures that only encrypted sessions will be able to communicate, and non-encrypted sessions are not allowed to be cut through on the talk path of the session.

13. Each gateway DS0 port interface can only be activated and put in-service when it is connected serially with an NSA Type I encryption device (either automated provisioning or manual provisioning is allowed to provide the control).

APPENDIX C
GLOSSARY OF ABBREVIATIONS AND ACRONYMS

Following are the acronyms used in the UCR 2013 document.

ACRONYM	DEFINITION
µs	Microsecond
1XRTT	One Times Radio Transmission Technology
3G	Third Generation
3GPP	Third-Generation Partnership Project
3G-SDI	3-Gbps Serial Digital Interface
3GSM	Third Global System for Mobile
4CIF	Four Times Common Intermediate Format
4G	Fourth Generation
A/V	Audio Visual
AAA	Authentication, Authorization, and Accounting
AAdmin	Audit Administrator
AAG	Access Aggregation
AAL5	Asynchronous Transfer Mode Adaptation Layer 5
ABNF	Augmented Backus Naur Form
ACA	Audio Compression Algorithm
ACD	Automatic Call Distribution
ACK	Acknowledgement
ACL	Access Control List
ACTA	Administrative Council for Terminal Attachments
ADC	Analog-to-Digital Converter
ADIMSS	Advanced DSN Integrated Management Support System
ADM	Add-Drop Multiplexing
ADN	Area Distribution Node
AEI	Assured Services Session Initiation Protocol Video End Instrument
AEI	Audio End Instrument
AES	Advanced Encryption Standard
AF	Assured Forwarding
AGF	Aggregate Grooming Function
AH	Authentication Header
AIA	Authority Information Access
AIS	Alarm Indication Signal
AIS	Automated Information System

ACRONYM	DEFINITION
ALG	Application Layer Gateway
ALI	Automatic Location Identification
AMI	Alternate Mark Inversion
AMSL	Above Mean Sea Level
ANAT	Alternative Network Address Type
ANI	Automatic Number Identification
ANS	Answer Message
ANSI	American National Standards Institute
AP	Association Path
API	Application Programming Interface
APL	Approved Products List
APS	Automatic Protection Switching
AR	Aggregation Router
ARP	Address Resolution Protocol
AS	Autonomous System
AS-SIP	Assured Services Session Initiation Protocol
ASA	Automatic Security Authentication
ASAC	Assured Services Access Control
ASF	Assured Services Features
ASLAN	Assured Services Local Area Network
AS-NE	Assured Services Network Element
Async	Asynchronous
ATA	Analog Terminal Adapter
ATB	All Trunk Busy
ATM	Asynchronous Transfer Mode
ATQA	Attendant Queue Announcement
AU-4	Administrative Unit 4
AVSC	Available Link Session Capacity
AVT	Audio and Video Transport
B/P/C/S	Base/Post/Camp/Station
B2BUA	Back-to-Back User Agent
B3ZS	Bipolar With Three Zero Substitution
B8ZS	Bipolar With Eight Zero Substitution
BC	Border Controller
BCE	Bridged Call Exclusion
BE	Best Effort

ACRONYM	DEFINITION
BER	Basic Encoding Rule
BER	Bit Error Rate
BFCP	Binary Floor Control Protocol
BGMP	Border Gateway Multicast Protocol
BGP	Border Gateway Protocol
BITS	Building Integrated Timing Supply
BLSR	Bidirectional Line Switched Ring
BLV	Busy Line Verification
BNEA	Busy Not Equipped Announcement
BOOTP	Bootstrap Protocol
BPA	Blocked Precedence Announcement
BPON	Broadband Passive Optical Network
BRI	Basic Rate Interface
BSC	Base Station Controller
BSI	British Standards Institution
BSR	Bootstrap Router
BW	Bandwidth
C&A	Certification and Accreditation
C/RD	Confidential Restricted Distribution
C2	Command and Control
C4	Command, Control, Communications, and Computers
CA	Certification Authority
CAC	Call Admission Control
CAC	Common Access Card
CAdmin	Cryptographic Administrator
CAG	Channel Access Grooming
CAL	Category Assurance List
CAN	Campus Area Network
CANF	Cancel From
CANT	Cancel to
CAP	Common Alerting Protocol
CAPWAP	Control and Provisioning of Wireless Access Points
CAS	Client Access Server
CC	Country Code
CC/S/A	Combatant Command/Station/Agency
CCA	Call Connection Agent

ACRONYM	DEFINITION
CCA-ID	Call Connection Agent Identifier
CCAT	Contiguous Concatenation
CCMP	Counter With Cipher Blocking Chaining – Message Authentication Code Protocol
CCS	Common Channel Signaling
CCS7	Common Channel Signaling 7
CDMA	Code Division Multiple Access
CDMI	Cloud Data Management Interface
CDP	Certificate Revocation List Distribution Point
CDR	Call Detail Record
CE	Customer Edge
CEE	Converged Enhanced Ethernet
CE-R	Customer Edge Router
CES	Circuit Emulation Service
CF	Call Forwarding
CFBL	Call Forwarding Busy Line
CFDA	Call Forwarding – Don t Answer
CFI	Canonical Format Indicator
CFR	Code of Federal Regulations
CFV	Call Forwarding Variable
CGA	Carrier Group Alarms
CIDR	Classless Inter-Domain Routing
CIO	Chief Information Officer
CIT	Craft Input Terminal
CivPDS	Civilian Personnel Data System
CJCS	Chairman of the Joint Chiefs of Staff
CJCSM	Chairman of the Joint Chiefs of Staff Manual
CLI	Command Line Interface
CM	Configuration Management
CNA	Converged Network Adapter
CND	Calling Number Delivery
CNSS	Committee on National Security Systems
CO	Central Office
COCOM	Combatant Command
COIN	Community of Interest Network
COMSEC	Communications Security
CONUS	Continental United States

ACRONYM	DEFINITION
COOP	Continuity of Operations
CORBA	Common Object Request Broker Architecture
CoS	Class of Service
COT	Continuity Testing
COTS	Commercial off-the-Shelf
CP	Collaboration Product
CPE	Customer Premises Equipment
C-PE	Classified Customer Edge Router
CPN	Calling Party Number
CQ	Custom Queuing
CRC	Cyclical Redundancy Check
CRD	Capabilities Requirement Document
CRL	Certificate Revocation List
CS	Circuit Switched
CSFB	Circuit Switched Fallback
CSPF	Constrained Shortest Path First
CTCP	Compound Transmission Control Protocol
CTL	Certificate Trust List
CTU	Conferencing Terminal Unit
CUI	Common User Interface
CV	Code Violation
CVoIP	Classified Voice over Internet Protocol
CVSD	Continuously Variable Slope Delta
CVVoIP	Classified Voice and Video over Internet Protocol
CW	Call Waiting
CY	Calendar Year
DA	Destination Address
DAC	Digital-to-Analog Converter
DAD	Duplicate Address Detection
DAM	Diagnostic Acceptability Measure
DASAC	Dynamic Assured Services Admission Control
DATMS	Defense Information Systems Network Asynchronous Transfer Mode Services
DB	Database
DBA	Database Administrator
DBMS	Database Management System
DCA	Defense Communications Agency

ACRONYM	DEFINITION
DCB	Data Center Bridging
DCBX	Data Center Bridging Exchange
DCC	Destination Code Control
DCE	Data Communications Equipment
DCID	Director of Central Intelligence Directive
DCN	Data Communications Network
DCO	Defense Connection Online
DCP	Designated Called Party
DCT	Discrete Cosine Transform
DCVX	Deployable Cellular Voice Exchange
DDWG	Digital Display Working Group
DEE	DoD Enterprise Email
DEMUX	Demultiplexer
DEROS	Date Eligible for Return From Overseas
DES-CBC	Data Encryption Standard – Cipher Block Chaining
DF	Dual Frequency
DFSU	Dual Frequency Signaling Unit
DHCP	Dynamic Host Configuration Protocol
DIA	Defense Intelligence Agency
DIACAP	Department of Defense Information Assurance Certification and Accreditation Process
DIAM	Defense Intelligence Agency Manual
DiffServ	Differentiated Services; also DS
DISA	Defense Information Systems Agency
DISN	Defense Information Systems Network
DISR	Department of Defense Information Technology Standards Registry
DIT	Directory Information Tree
DIU	Digital Interface Unit
DL	Dual-Link
DLAN	Deployable Local Area Network
DLoS	Direct Line of Sight
DMDC	Defense Manpower Data Center
DMSC	Deployed Mobile Switching Center
DN	Directory Number
DN	Distinguished Name
DNA	Defense Nuclear Agency
D-NE	Deployable Network Element

ACRONYM	DEFINITION
DNIS	Dialed Number Identification Service
DNS	Domain Name Service
DoD	Department of Defense
DoDAF	Department of Defense Architecture Framework
DoDD	Department of Defense Directive
DoDI	Department of Defense Instruction
DoS	Denial of Service
DP	Dial Pulse
DR	Disaster Recovery
DRSN	Defense RED Switch Network
DRT	Diagnostic Rhyme Test
DS	Differentiated Services; also DiffServ
DS0	Digital Signal Level 0
DS1	Digital Signal Level 1
DSC	Data Storage Controller
DSC	Deployed Session Controller
DSCD	Department of Defense Secure Communications Device
DSCP	Differentiated Services Code Point
DSCS	Defense Satellite Communications System
DSL	Digital Subscriber Line
DSLAM	Digital Subscriber Line Access Multiplexer
DSN	Defense Switched Network
DSP	Digital Signal Processing
DSS	Defense Information Systems Network Subscription Service
DSSS	Dual Signaling Softswitch
DTA	Digital Trunk Adapter
DTE	Data Terminal Equipment
DTE	Data Terminating Equipment
DTM	Digital Trunk Module
DTMF	Dual Tone Multifrequency
DTR	Deployed Tactical Radio
DUI	Duration of Unscheduled Interruption
DVI	Digital Visual Interface
DVR	Digital Video Recorder/Recording
DVS	Defense Information Systems Network Video Services
DVX	Digital Voice Exchange

ACRONYM	DEFINITION
DVX-C	Deployed Voice Exchange Commercial
DWDM	Dense Wavelength Division Multiplexing
DWT	Discrete Wavelet Transform
E&M	Ear and Mouth
E2E	End-to-End
E911	Enhanced Emergency Service
EAP	Extensible Authentication Protocol
EASF	Enterprise Applications and Services Forest
EBER	Excessive Basic Encoding Rule
eBGP	External Border Gateway Protocol
EC	Echo Canceller
ECA	External Certification Authority
ECN	Explicit Congestion Notification
ECU	Electronic Control Unit
EDC	Electronic Dispersion Compensation
EDID	Extended Display Identification Data
EDS	Enterprise Directory Services
ED-SDI	Enhanced Definition Serial Digital Interface
EF	Expedited Forwarding
EFEC	Enhanced Forward Error Correction
EFMCu	Ethernet in the First Mile Over Copper
EI	End Instrument
EIA	Electronic Industries Alliance
EIR	Equipment Identity Register
EISC	End Instrument Session Capacity
EKMS	Electronic Key Management System
EKTS	Electronic Key Telephone System
ELIN	Emergency Location Identification Number
EMC	Electromagnetic Compatibility
EMI	Electromagnetic Interference
eMLPP	Enhanced Multilevel Precedence and Preemption
EMPT	Electromagnetic Pulse Testing
EMS	Element Management System
EMSS	Enhanced Mobile Satellite System
ENUM	Electronic Numbering
EO	End Office

ACRONYM	DEFINITION
EOL	End of Life
EPC	Early Pentagon Capability
EPON	Ethernet Passive Optical Network
ERL	Emergency Response Location
ertPS	Extended Real-Time Polling Service
ES	Errored Seconds
ESA	Enterprise Services Area
ESC	Enterprise Session Controller
ESCON	Enterprise Services Connectivity
ESD	Electrostatic Discharge
ESF	Extended Super Frame
ESP	Encapsulating Security Payload
ET	End Terminal
ETS	Enhanced Transmission Selection
ETSI	European Telecommunications Standards Institute
EUB	End User Building
EUR	Europe
EVDO	Evolution – Data Optimized; also EV-DO
EWS	Exchange Web Services
EXP	Experimental
F	FLASH
F1SC	Failover Type 1 Session Controller
F2SC	Failover Type 2 Session Controller
FA	Forwarding Adjacency
FAS	Facility Associated Signaling
FC	Fibre Channel
FCAPS	Fault, Configuration, Accounting, Performance, and Security
FCC	Federal Communications Commission
FCoE	Fibre Channel Over Ethernet
FCP	Fibre Channel Protocol
FDCC	Federal Desktop Core Configuration
FDL	Facility Data Link
FDM	Frequency Division Multiplexing
FE	Fast Ethernet
FEAC	Far End Alarm and Control
FEBE	Far End Block Error

ACRONYM	DEFINITION
FEC	Forward Error Correction
FECC	Far End Camera Control
FEOOF	Far End out of Frame
FIB	Forwarding Information Base
FICON	Fiber Connectivity
FIFO	First-in First-out
FIPS	Federal Information Processing Standard
FIR	Full Intra Request
FNBDT	Future Narrowband Digital Terminal
F-NE	Fixed Network Element
FO	FLASH OVERRIDE
FOC	Full Operating Capability
FOO	Flash Override Override
FOUO	For Official Use Only
FQDN	Fully Qualified Domain Name
FSAL	Fixed Security Access Level
FSD	Functional Specifications Document
FSO	Field Security Office
FTP	File Transfer Protocol
FTR	Federal Telecommunications Recommendation
FW	Firewall
FX	Foreign Exchange
GAL	Global Address List
GAP	Generic Address Parameter
GbE	Gigabit Ethernet
GBNP	Global Block Numbering Plan
GCCS-J	Global Command and Control Systems – Joint
GETS	Government Emergency Telecommunications Service
GFP	Generic Framing Procedure
GIG	Global Information Grid
GIG-BE	Gigabit Bandwidth Expansion
GIS	Geographical Information System
GK	Gatekeeper
GMPLS	Generalized Multiprotocol Label Switching
GMT	Greenwich Mean Time
GNE	Gateway Network Element

ACRONYM	DEFINITION
GNS	Global Name Space
GOS	Grade of Service
GPON	Gigabit Passive Optical Network
GPRS	General Packet Radio System
GPS	Global Positioning System
GR	Generic Requirement
GRE	Generic Routing Encapsulation
GSM	Global System for Mobile
GSR	Generic System Requirement
GTP	Generic Test Plan
GUI	Graphical User Interface
GW	Gateway
HAIPE	High Assurance Internet Protocol Encryptor
HBSS	Host-Based Security System
HDB-3	High Density Bipolar 3 Code
HDCP	High-Bandwidth Digital Content Protection
HDLC	High-Level Data Link Control
HDMI	High Definition Multimedia Interface
HD-SDI	High Definition Serial Digital Interface
HEMP	High Altitude Electromagnetic Pulse
HLR	Home Location Register
HMAC	Hash-Based Message Authentication Code
HR	Hybrid Routing
HSPD	Homeland Security Presidential Directive
HTML	Hypertext Markup Language
HTTP	Hypertext Transfer Protocol
HTTPS	Hypertext Transfer Protocol Secure
Hz	Hertz
I/O	Input/Output
I/P	IMMEDIATE/PRIORITY
I3MP	Installation Information Infrastructure Modernization Program
IA	Information Assurance
IAD	Integrated Access Device
IANA	Internet Assigned Numbers Authority
IAP	Internet Access Point
IAS	Integrated Access Switch

ACRONYM	DEFINITION
IAT	Information Assurance Tool
IAVA	Information Assurance and Vulnerability Assessment
IAW	In Accordance With
IBGP	Internal
iBGP	Internal Neighbors Internal Border Gateway Protocol
ICA	Isolated Code Announcement
ICCS	Intra-Cluster Communication Signaling
ICD	Initial Capabilities Document
ICMP	Internet Control Message Protocol
IDMI	Identity Synchronization Service Machine Interface
IDP	Integrated Data Protection
IDS	Intrusion Detection System
IdSS	Identity Synchronization Service
Ie	Equipment Impairment Factor
IEC	International Electrotechnical Commission
IEEE	Institute of Electrical and Electronics Engineers
IETF	Internet Engineering Task Force
IF	Interface
IF-MAP	Interface – Metadata Access Point
IGMPv3	Internet Group Management Protocol Version 3
IKE	Internet Key Exchange
ILMI	Integrated Local Management Interface
IMS	Internet Protocol Multimedia Subsystem
IMT	International Mobile Telecommunications
INCITS	International Committee for Information Technology Standards
INE	In-Line Network Encryptor
INTSERV	Integrated Services
IP	Internet Protocol
IPB	Internet Protocol Budget
IPC	Internet Protocol Count
IPCP	Internet Protocol Control Protocol
IPDR	Internet Protocol Detail Record
IPM	Impulse per Minute
IPS	Intrusion Protection System
IPSec	Internet Protocol Security
IR	Intermediate Reach

ACRONYM	DEFINITION
IRC	Internet Relay Chat
IS	Intermediate System
ISAKMP	Internet Security Association and Key Management Protocol
iSCSI	Internet Small Computer Systems Interface
ISDN	Integrated Services Digital Network
IS-IS	Intermediate System to Intermediate System
iSNS	Internet Storage Name Service
ISO	International Organization for Standardization
ISS	Integrated Security Solution
IT	Information Technology
ITU-T	International Telecommunications Union – Telecommunication
IUA	Integrated Services Digital Network User Adaptation
IVR	Interactive Voice Response
IWF	Interworking Function
J2EE	Java 2 Platform Enterprise Edition
JC2	Joint Command and Control
JITC	Joint Interoperability Test Command
JM	Joint Menu
JROC	Joint Requirements Oversight Council
JROCM	Joint Requirements Oversight Council Memorandum
JS	Joint Staff
JTF	Joint Task Force
JWICS	Joint Worldwide Intelligence Communications System
KB	Kilobyte
kbps	Kilobits per Second
Kbps	Kilobytes per Second
KEYMAT	Keying Material
kHz	Kilohertz
L2	Open System Interconnect Layer 2
L3	Open System Interconnect Layer 3
LAN	Local Area Network
LBO	Line Buildout
LCAS	Link Capacity Adjustment Scheme
LDAP	Lightweight Directory Access Protocol
LDAPv3	Lightweight Directory Access Protocol Version 3
LDIF	Lightweight Directory Access Protocol Data Interchange Format

ACRONYM	DEFINITION
LDN	Listed Directory Number
LDP	Label Distribution Protocol
LDS	Lightweight Directory Services
LEF	Link Encryptor Family
LER	Label Edge Router
LFB	Look Forward Busy
LLDP	Link Layer Discovery Protocol
L-LSP	Label Only Inferred Label Switched Path
LMR	Land Mobile Radio
LNP	Local Network Protection
LOC	Letter of Compliance
LOC2	Loss of Command and Control
LOF	Loss of Frame
LOP	Loss of Pointer
LOS	Line of Sight
LR	Long Reach
LRDB	Local Real-Time Services Routing Database
LS	Local Area Network Switch
LSP	Label Switched Path
LSR	Label Switching Router
LTE	Long-Term Evolution
LUN	Logical Unit
MA	Mission Area
MAC	Media Access Control
MAC	Move, Add, Change
MAN	Metropolitan Area Network
MAP	Metadata Access Point
Mbps	Megabits per Second
MBps	Megabytes per Second
MBSS	Multifunction Mobile Device Backend Support System
MCN	Main Communication Node
MCU	Multipoint Conferencing Unit
MDI	Media Dependent Interface
MDM	Mobile Device Management
MDR	Maximum Deployment Range
MELPe	Enhanced Mixed Excitation Linear Production

ACRONYM	DEFINITION
MER	Minimum Essential Requirement
MF	Multifrequency
MFS	Multifunction Switch
MG	Media Gateway
MGC	Media Gateway Controller
MGCP	Media Gateway Control Protocol
MIB	Management Information Base
MILDEP	Military Department
MilPDS	Military Personnel Data System
MILSTAR	Military Strategic, Tactical, and Relay
MIME	Multipurpose Internet Mail Extensions
MIMO	Multiple In Multiple Out
MLD	Multicast Listener Discovery
MLPP	Multilevel Precedence and Preemption
MLS	Multi-Level Security
MMD	Multifunction Mobile Device
MME	Mobility Management Entity
MMF	Multi Mode Fiber
MNS	Mass Notification Systems
MNWS	Mass Notification Warning System
MOR	Maximum Operational Range
MOS	Mean Opinion Score
MPBGP	Multiprotocol Border Gateway Protocol
MPCA	Moving Picture Compression Algorithm
MPLS	Multiprotocol Label Switching
MPT	Maximum Possible Throughput
MR	Modem Relay
MRDB	Master Real-Time Services Routing Database
MRP	Modem Relay Preferred
MSC	Master Session Controller
MSDP	Multicast Source Discovery Protocol
MSPP	Multiservice Provisioning Platform
MSS	Maximum Segment Size
MS-UM	Microsoft Unified Messaging
MTBF	Mean Time Between Failures
MTIE	Maximum Time Interval Error

ACRONYM	DEFINITION
MTR	Maximum Transmission Range
MTU	Maximum Transmission Unit
MUF	Military Unique Feature
MUX	Multiplexer
MVI	Multi Vendor Interoperable
MWI	Message Waiting Indicator
N	NUMBER
N/A	Not Applicable
NA	Network Appliance
NA/SS	Network Appliance/Simple Server
NAC	Network Access Controller
NANP	North American Numbering Plan
NAPT	Network Address Port Translation
NAS	Network Access Server
NAT	Network Address Translation
NATO	North Atlantic Treaty Organization
NBMA	Non-Broadcast Multi-Access
NBT	Network Basic Input/Output System Over Transmission Control Protocol/Internet Protocol
NCA	No Circuit Available
NE	Network Element
NEBS	Network Equipment Building System
NENA	National Emergency Number Association
NES	Network Encryption System
NETBIOS	Network Basic Input/Output System
NetOps	Network Operations
NFAS	Non-Facility Associated Signaling
NFPA	National Fire Protection Association
NFS	Network File System
NI	Network Infrastructure
NI ½	National Integrated Services Digital Network 1/2
NIAP	National Information Assurance Partnership
NIC	Network Interface Card
NIPR	Non-Secure Internet Protocol Router
NIS	Network Information Service
NISP	Network Infrastructure Product
NIST	National Institute of Standards and Technology

ACRONYM	DEFINITION
NM	Network Management
NMS	Network Management System
NP	Not Permitted
NPA	Numbering Plan Area
NR	Not Required
NRT	Near-Real Time
nrtPS	Non Real-Time Polling Service
NSA	National Security Agency
NSN	Nationally Significant Number
NSTISS	National Security Telecommunications and Information Systems Security
NSTISSAM	National Security Telecommunications and Information Systems Security Authority Manual
NSTISSI	National Security Telecommunications and Information Systems Security Instruction
NT1	Network Termination 1
NTP	Network Time Protocol
O	OPTIONAL
O&M	Operations and Maintenance
O/E	Optical/Electrical
OAM&P	Operations, Administration, Maintenance, and Provisioning
OAN	Operational Area Network
OC-3	Optical Carrier 3
OCONUS	Outside the Continental United States
OCSP	Online Certificate Status Protocol
ODU	Optical Demultiplexing Unit
ODXC	Optical Digital Cross Connect
OEO	Optical to Electrical to Optical
OIF	Optical Internetworking Forum
OLA	Optical Line Amplifier
OLT	Optical Line Terminal
OMCI	Optical Network Terminal Management Control Interface
ONT	Optical Network Terminal
ONU	Optical Network Unit
OOB	Out of Band
OOBM	Out of Band Management
OOF	Out of Frame
OP	Optical Protection
ORD	Operational Requirements Document

ACRONYM	DEFINITION
ORL	Optical Return Loss
OS	Operating System
OSA	Optical Spectrum Analyzer
OSC	Optical Supervisory Channel
OSCR	Online Status Check Responder
OSD	Office of the Secretary of Defense
OSI	Open System Interconnect
OSNR	Optical Signal-to-Noise Ratio
OSPF	Open Shortest Path First
OTAR	Over-the-Air Rekey
OTN	Optical Transport Network
OTS	Optical Transport Switch
OTU	Optical Transport Unit
OXC	Optical Cross Connect
P	Precedence Level
P2N	Point-to-Multipoint
PA	Public Address
PALA	Precedence Access Limitation Announcement
PAS	Priority Access Service
PAT	Precedence Access Threshold
PB	Petabyte
PBAS	Precedence-Based Assured Services
PBX	Private Branch Exchange
PCA	Picture Compression Algorithm
PCD	Precedence Call Diversion
PCM	Pulse Code Modulation
PDA	Personal Digital Assistant
PDH	Plesiochronous Digital Hierarchy
PDS	Protected Distribution System
PDU	Protocol Data Unit
PE	Provider Edge
PEAP	Protected Extensible Authentication Protocol
PED	Portable Electronic Device
PEI	Proprietary Internet Protocol Voice End Instrument
PESQ	Perceptual Evaluation of Speech Quality
PFC	Priority-Based Flow Control

ACRONYM	DEFINITION
PHB	Per-Hop Behavior
PHY	Physical Layer
PIM	Protocol Independent Multicast
PIM-SM	Protocol Independent Multicast – Sparse Mode
PIN	Personal Identification Number
PIPT	Proprietary Internet Protocol Trunk
PKCS	Public-Key Cryptography Standard
PKE	Public Key Enablement
PKI	Public Key Infrastructure
PL/CA	Precedence Level Calling Area
PLI	Picture Loss Indication
PLL	Phase Locked Loop
PM	Performance Management
PMD	Phase Modulation-Demodulation
PMO	Project Management Office
PND	Private Networking Domain
PO	Program Office
PoE	Power Over Ethernet
PON	Passive Optical Network
POS	Packet Over Synchronous Optical Network
POTS	Plain Old Telephone Service
PPP	Point-to-Point Protocol
PPSM	Ports, Protocols, and Service Management
PQ	Priority Queuing
PRI	Primary Rate Interface
PS/ALI	Private Switch Automatic Location Information
PSAB	Public Safety Announcement Bulletin
PSAP	Public Safety Answering Point
PSQM	Perceptual Speech Quality Measure
PSTN	Public Switched Telephone Network
PTT	Push-To-Talk
Q	Quality
QAM	Quadrature Amplitude Modulation
QCIF	Quarter Common Intermediate Format
QoS	Quality of Service
QPSK	Quadrature Phase-Shift Keying

ACRONYM	DEFINITION
R	Router
R	ROUTINE
RAC	Resource Availability Confirmation
RADIUS	Remote Authentication Dial-in User Server/Service
RAE	Required Ancillary Equipment
RAI	Resource Availability Indicator
RAID	Redundant Array of Independent Disks
RAN	Radio Access Network
RAW	Read and Write
RBF	Radio Bridge Function
RDI	Remote Defect Indication
REI	Radio End Instrument
REST	Representational State Transfer
RF	Radio Frequency
RFC	Request for Comment
RFI	Remote Failure Indication
RFoG	Radio Frequency Over Glass
RIB	Routing Information Base
RID	Router Identification
RM	Remote Management
RMON	Remote Monitoring
RMUX	Real-Time Multiplexer
RO	ROUTINE only
ROADM	Reconfigurable Optical Add-Drop Multiplexer
ROEI	ROUTINE Only End Instrument
RP	Rendezvous Point
RPF	Reverse Path Forwarding
RPH	Reservation Priority High
RPR	Resilient Packet Ring
RPSI	Reference Picture Selection Indication
RSA	Rivest Shamir Adleman
RSF	Real-Time Services Stateful Firewall
RSVP	Resource Reservation Protocol
RTCP	Real-Time Transport Control Protocol
RTP	Real-Time Transport Protocol
rtPS	Real-Time Polling Service

ACRONYM	DEFINITION
RTS	Real-Time Services
RTT	Round Trip Time
S	Switch Link
SA	Security Association
SA	Source Address
SAC	Session Admission Control
SACK	Selective Acknowledgment
SAD	Security Association Database
SAFI	Sub Address Family Identifier
SAL	Security Access Level
SAMP	Single Acquisition Management Plan
SAN	Storage Area Network
SAR	Segmentation and Reassembly
S-AR	SECRET Aggregation Router
SATA	Serial Advanced Technology Attachment
SBC	Session Border Controller
SBU	Sensitive but Unclassified
SC	Session Controller
SC/SS	Session Controller/Softswitch
S-CE	SECRET Customer Edge
SCF	Selective Call Forwarding
SCI	Sensitive Compartmented Information
SCIF	Sensitive Compartmented Information Facility
SCIP	Secure Communications Interoperability Protocol
SCLS	Session Controller Location Service
SCPS	Space Communications Protocol Standards
SCS	Session Control and Signaling
SCS	Session Controller Service
SCSI	Small Computer Systems Interface
SCTP	Stream Control Transmission Protocol
SD	Security Device
SDF	Start Delimiter Frame
SDH	Synchronous Digital Hierarchy
SDP	Session Description Protocol
SD-SDI	Standard Definition Serial Digital Interface
SEF	Severely Errored Framing

ACRONYM	DEFINITION
SEFS	Severely Errored Framing Seconds
SEI	Secure End Instrument
SES	Severely Errored Seconds
SF	Signal Fail
SF	Superframe
SFP	Small Form-factor Pluggable
SG	Signaling Gateway
SHA	Secure Hash Algorithm
SIGTRAN	Signaling Transport
SIM	Subscriber Identity Module
SIP	Session Initiation Protocol
SIPR	Secure Internet Protocol Router
SLA	Service-Level Agreement
SLAAC	Stateless Address Autoconfiguration
SLI	Slice Loss Indication
SLO	Service Level Objective
SLS	Service Level Specification
SM	Sparse Mode
SMC	Synchronous Optical Network Minimum Clock
SMCU	Signaling Multipoint Control Unit
SME	Secure Mobile Environment
SMEO	Small End Office
SMF	Single Mode Fiber
SMIv2	Structure of Management Information Version 2
SMPTE	Society of Motion Picture and Television Engineers
SMS	Short Message Service
SMTP	Simple Message Transfer Protocol
SN	Satellite Network
SNCP	Support Subnetwork Connection Protection
SNF	SECRET/Not Releasable to Foreign Nationals
SNIA	Storage Networking Industry Association
SNMP	Simple Network Management Protocol
SNMPv3	Simple Network Management Protocol Version 3
SOAP	Simple Object Access Protocol
SONET	Synchronous Optical Network
SP	Special Publication

ACRONYM	DEFINITION
SPCS	Stored Program Control Switch
SPD	Security Policy Database
S-PE	SECRET Provider Edge
SPF	Shortest Path First
SPI	Security Parameter Index
SPRT	Simple Packet Relay Transport
SQCIF	Sub Quarter Common Intermediate Format
SQF	System Quality Factor
SR	Short Reach
SRTCP	Secure Real-Time Transport Control Protocol
SRTP	Secure Real-Time Transport Protocol
SS	Simple Server
SS	Softswitch
SS7	Signaling System No. 7
SSC	Subtended Session Controller
SSDP	System Services Delivery Point
SSE	State Signaling Event
SSHv2	Secure Shell Version 2
SSL	Secure Socket Layer
SSLS	Softswitch Location Service
SSM	Synchronization Status Message
SSM	Systems Security Manager
STANAG	Standardization Agreement
STD	Software Test Description
STE	Secure Terminal Equipment
STEP	Standardized Tactical Entry Point
STI	Standard Terminal Interface
STIG	Security Technical Implementation Guideline
STM	Synchronous Transport Module
STS-1	Synchronous Transport Signal 1
SUT	System Under Test
SVC	Scalable Video Coding
Sync	Synchronous
T&S	Timing and Synchronization
TA	Terminal Adapters
TACACS	Terminal Access Controller Access Control System

ACRONYM	DEFINITION
TBCT	Two B-Channel Transfer
TBD	To Be Determined
TCA	Traffic Conditioning Agreement
TCAP	Transaction Capabilities Application Part
TCI	Tag Control Information
TCLw	Weighted Terminal Coupling Loss
TCP	Transmission Control Protocol
TCS	Traffic Conditioning Specification
TDM	Time Division Multiplexing
TDMA	Time Division Multiple Access
TDMB	Time Division Multiplexing Session Budget
TDR	Technical Deficiency Report
TDS	Technology Development Strategy
TE	Terminal Equipment
TE	Traffic Engineering
TFTP	Trivial File Transfer Protocol
TIA	Telecommunications Industry Association
TL1	Transaction Language 1
TLP	Transmission Level Point
TLS	Transport Layer Security
TLSC	Transmission Link Session Capacity; also TSC
TLV	Type Length Value
TN	Tactical-Edge Network
TN	Terrestrial Network
TOD	Time of Day
TOS	Type of Service
TPID	Tag Protocol Identification
TRANSEC	Transmission Security
TRILL	Transparent Interconnection of Lots of Links
TRN	Tactical Radio Network
TS	Transport Switching
TSA	Time Slot Assignment
TSB	Telecommunication Standardization Bureau
TSC	Transmission Link Session Capacity
TSEC	Telecommunications Security
TSF	Transport Switch Function

ACRONYM	DEFINITION
TSI	Time Slot Interchange
TTA	Telecommunications Technology Association
TTC	Telecommunications Technology Committee
TTL	Time To Live
TTLS	Tunneled Transport Layer Security
TWC	Three-Way Calling
UAS	Unavailable Seconds
UAS	User Agent Server
UC	Unified Capabilities
UCCO	Unified Capabilities Connection Office
UCCS	Unified Capabilities Conference System
U-CE	Unclassified Customer Edge Router
UCF	Unified Capabilities Framework
UCR	Unified Capabilities Requirements
UDDI	Universal Discovery Description Interface
UDP	User Datagram Protocol
UFC	Unified Facilities Criteria
UFS	User Features and Services
UGS	Unsolicited Grant Service
UHF	Ultra High Frequency
UI	Unscheduled Interruption
UID	User Identifier
UIpp	Unit Interval Peak to Peak
UIrm	Unit Interval Root Mean Square
UL	Underwriter Laboratories, Inc.
ULA	Unicast Address
UM	Unified Messaging
UMTS	Universal Mobile Telecommunications System
UNI	User Network Interface
UPA	Unauthorized Precedence Level Announcement
U-PE	Unclassified Customer Edge Router
UPnP	Universal Plug and Play
UPS	Uninterruptible Power Supply
UPSR	Unidirectional Path Switched Ring
URI	Uniform Resource Identifier
URL	Uniform Resource Locator

ACRONYM	DEFINITION
USSTRATCOM	U.S. Strategic Command
UTP	Unshielded Twisted Pair
UUIE	User-to-User Information Element
UUT	Unit Under Test
VAD	Voice Activity Detection
VBD	Voiceband Data
VC	Virtual Circuit
VCA	Vacant Code Announcement
VCAT	Virtual Concatenation
VCFUR	Video Channel Fast Update Request
VDB	Video Session Unit Budget
VDC	Video Session Unit Count
VD-NE	Virtual Deployed Network Element
VDS	Video Distribution System
vDSC	Virtualized Data Storage Controller
VDS-IP	Video Distribution System Over IP
VESA	Video Electronics Standards Association
VF	Voice Frequency
VFR	Virtual Routing/Forwarding
VG	Voice Grade
VGA	Video Graphics Array
VHF	Very High Frequency
VID	Virtual Local Area Network Identification
VLAN	Virtual Local Area Network
VLR	Visitor Location Register
VMPS	Virtual Local Area Network Management Policy Server
VNAR	Voice Net Access Radio
VoIP	Voice over Internet Protocol
VoLTE	Voice over Long-Term Evolution
VPCC	Video Distribution System Peripheral Connector Conversion
VPLS	Virtual Private Local Area Network Service
VPN	Virtual Private Network
VRF	Virtual Routing/Forwarding
VRRP	Virtual Router Redundancy Protocol
VSAL	Variable Security Access Level
VSAT	Very Small Aperture Terminal

ACRONYM	DEFINITION
VSR	Very Short Reach
VSU	Video Session Unit
VT	Virtual Tributary
VTC	Video Teleconferencing
VTR	Video Tape Recorder/Recording
VTU	Video Teleconferencing Unit
VVoIP	Voice and Video over Internet Protocol
WAB	Wireless Access Bridge
WAN	Wide Area Network
WCDMA	Wideband Code Division Multiple Access
WD	Weather Day
WDM	Wavelength Division Multiplexing
WebDAV	Web Based Distributed Authoring and Versioning
WEI	Wireless End Instrument
WFQ	Weighted Fair Queuing
WIDS	Wireless Intrusion Detection System
WiMAX	Worldwide Interoperability for Microwave Access
WINS	Windows Internet Name Service
WLAN	Wireless Local Area Network
WLAS	Wireless Local Area Network Access System
WMM	WiFi Multimedia
WOC	Wide Area Network Optimization Controller
WPA2	WiFi Protected Access 2
WPS	Wireless Priority Service
WSDL	Web Service Description Language
WTR	Wait To Restore
WUXGA	Wide Ultra Extended Graphics Array
WWNDP	Worldwide Numbering and Dialing Plan
XDMCP	X Display Manager Control Protocol
XHTML	Extensible HyperText Markup Language
XML	Extensible Markup Language
XMPP	Extensible Messaging and Presence Protocol