Changes to UCR 2008, Change 1, Section 5.3.2, Assured Services Requirements

SECTION	CORRECTION	EFFECTIVE DATE
5.3.2 (Throughout Section)	Added support for AS SIP End Instruments (Generic EIs or GEIs). All instances of "EI" in UCR 08 Section were expanded to "EI and GEI", "EI or GEI", or similar in Change 1. Will update all instances of "EI" to "PEI" (Proprietary EI) and all instances of "GEI" to "AEI" (AS-SIP EI) before publication.	18-month Rule
5.3.2.1.3	Added the statement that LSC and WAN SS MGs may be located at remote sites which are not the same as the LSC or WAN SS site.	18-month Rule
5.3.2.1.5	Added both the "GEI" and the "WAN SoftSwitch (WAN SS)" to Table 5.3.2-1 as new "APL Products" in Change 1.	18-month Rule
5.3.2.1.5	Revised Figure 5.3.2-3, Functional Reference Model – MFSS & Figure 5.3.2-4, Functional Reference Model – LSC (and later Figures based on them) to explicitly show Appliance support for VVoIP GEIs.	18-month Rule
5.3.2.2.1.2	Revised requirements for Dual Homing between CE Router and Aggregation Router. Dual Homing is now Required for ASLANs serving C2 users, & Conditional for ASLANs serving C2 [Routine] and Non-C2 users.	Immediate
5.3.2.2.2.1	Revised Table 5.3.2-2 to show which Appliances (LSC, MFSS) the Features and Capabilities apply to.	Immediate
5.3.2.2.2.1	Added a Conditional Requirement for Call Pick-up as an Assured Services Feature	18-month Rule
5.3.2.2.2.1	Added a requirement indicating that AS Systems like LSCs and MFSSes should also still support vendor-proprietary VVoIP features and capabilities. Also indicated that support for these features and capabilities should not adversely affect the required operation of the MLPP or ASAC features, as specified in Sections 5.2 (Circuit-Switching), 5.3.2 (ASR), and 5.3.4 (AS-SIP) of Change 1.	18-month Rule

SECTION	CORRECTION	EFFECTIVE DATE
5.3.2.2.2.1.1	Revised RTS Call Forwarding (CF) requirements to differ from DSN CF requirements: 1) Routine RTS calls can be call forwarded without any consideration of MLPP rules; 2) For RTS calls above Routine, it is Conditional to implement CF with the MLPP interaction required for DSN switches	Immediate
5.3.2.4.4	Added information to clarify the "VVoIP Network Management System Interface Requirements". Explicitly stated that redundant physical Ethernet interfaces for local management were not required. Explicitly stated that redundant physical Ethernet interfaces for the (remote) RTS EMS were not required. Added language to indicate that the redundancy requirements for signaling and bearer traffic could be met through use of virtual interfaces and a minimum of two physical interfaces.	18-month Rule
5.3.2.5.4	Added VoIP device requirements for Loss of Packets: 1) Voice quality shall have a MOS of 4.0 (R-Factor = 80) or better, per the E-Model; 2) Devices shall not lose 2 consecutive packets in a minute, and shall not lose more than 7 voice packets in a 5-minute period.	18-month Rule
5.3.2.6.1.1	Changed playing the "Loss of C2 Announcement" to "Conditional" for RTS Appliances (EI, GEI, LSC, MFSS, WAN SS)	Immediate
5.3.2.6.1.2	Added support for the G.722.1 Audio Codec on Voice Devices (Voice EIs and GEIs)	18-month Rule
5.3.2.6.1.3	Revised the Voice EI Telephone Audio Performance requirements to state that Voice EIs and GEIs shall comply with all of the transmission requirements in TIA-810-B, *Telecommunications Telephone Terminal Equipment Transmission Requirements for Narrowband Digital Telephones* (not just the 810-B Handset Loudness and Frequency Responses requirements listed in UCR 2008)	18-month Rule

SECTION	CORRECTION	EFFECTIVE DATE
5.3.2.6.1.4	Revised Requirements for Voice Over IP Sampling Standard to indicate that 1) 20ms is default voice sample length for strategic-to-strategic calls, and 2) For other call types like strategic-to-tactical calls, different voice sample lengths can be negotiated at call setup (e.g., 50 ms for G.729 8 kbps Voice codec)	Immediate
5.3.2.6.1.6	Added requirements for both G.711 Voice and V.150.1 Modem Relay support on TAs and IADs for Analog Telephone devices	18-month Rule
5.3.2.6.1.7	Added Softphone End Instrument requirements (by extending the existing Hardphone End Instrument requirements)	18-month Rule
5.3.2.6.1.8	Added detailed Conditional requirements for ISDN BRI Telephone Support in TAs, IADs, and MGs (Line-side)	18-month Rule
5.3.2.6.2.2	Made support for the G.722 and G.722.1 Audio Codecs Conditional on Video Codecs (Video EIs and GEIs). Dropped support for the G.723.1, G.728, G.729, and G.729A Audio Codecs on Video Codecs (EIs, GEIs)	Immediate
5.3.2.6.4	Added requirements on Transparency of V.150.1 Inband Signaling to EBCs (e.g., transitions between Voice and Modem Relay at EIs, TAs, IADs and MGs are transparent to EBCs, and use the same media protocol & port numbers before and after the transition)	18-month Rule
5.3.2.7	Revised LSC requirements to indicate that LSCs are SIP Back-to-Back User Agents, and not SIP Proxy Servers	Immediate
5.3.2.7.2.4	Added the “CCA (LSC) to GEI” interface using “AS-SIP over IP” to Table 5.3.2-4, as a new “LSC Signaling Interface” in Change 1.	18-month Rule
5.3.2.7.3	Added a new section on Loop Avoidance for LSCs, including requirements for avoiding RTS Call Looping on T1.619A PRI trunk groups between LSC MGs and DSN EOs.	18-month Rule
5.3.2.8	Revised MFSS requirements to indicate that SSs within MFSSes are SIP Back-to-Back User Agents, and not SIP Proxy Servers	Immediate

SECTION	CORRECTION	EFFECTIVE DATE
5.3.2.8.2.3	Added the “CCA (MFSS) to GEI” interface using “AS-SIP over IP” to Table 5.3.2-5, as a new “MFSS Signaling Interface” in Change 1	18-month Rule
5.3.2.8.3.1	Added a pointer to Section 5.3.2.4.4 (VVoIP Network Management System Interface Requirements) into this Section (Network Management System (NMS) Interface). Section 5.3.2.4.4 explicitly states that redundant physical Ethernet interfaces for local EMS and RTS EMS are not required.	18-month Rule
5.3.2.8.4	Added new section on Wide Area Network Level SoftSwitch (WAN SS), giving new requirements for WAN SSes in RTS/UC. E.g.: 1) WAN SS does not need to contain an LSC (LSC is Conditional, not Required) 2) WAN SS does not require an SS7 Signaling Gateway (SG) 3) WAN SS MG is only required to support T1.619A PRI trunks to the separate MFS 4) The NM EMS for the WAN SS should be provided as a standalone EMS, separate from the MFS EMS. 5) The WAN SS’s MG(s) may be remotely located from the MGC within the CCA of the WAN SS. 6) The WAN SS does not need to implement an ASLAN; it can instead use a proprietary switched Ethernet LAN	18-month Rule
5.3.2.9.6	Added requirements for CCA Preservation of Call Ringing State during Failure Conditions	18-month Rule
5.3.2.12.13.2.2	Added a Change 1 requirement that extends the DSN Echo Canceller (EC) Requirements in Section 5.2 (Circuit-Switching) to RTS Media Gateways. (The UCR 2008 MG EC requirements are based on separate commercial VoIP MG EC requirements.)	18-month Rule

SECTION	CORRECTION	EFFECTIVE DATE
5.3.2.12.16	Added requirements on Transparency of V.150.1 Inband Signaling to EBCs (e.g., transitions between Voice and Modem Relay at MGs are transparent to EBCs, and use the same media protocol & port numbers before and after the transition)	18-month Rule
5.3.2.12.17	Added requirements for MG Preservation of Call Ringing State during Failure Conditions	18-month Rule
5.3.2.14.7	Revised CE-R Availability requirements to allow for four types of CE-Rs: High Availability (99.999%), Medium Availability with SQF (99.99%), Medium Availability without SQF (99.99%), and Low Availability (99.9%). System Quality Factors [SQF]: Availability & Downtime requirements per Sec. 5.3.2.5.2	Immediate
5.3.2.14.8	Revised CE-R Requirements for Packet Transit Time as follows: The CE-R shall be capable of receiving, processing, & transmitting a voice packet within 2 ms or less, *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.*	Immediate
5.3.2.14.9	Clarified that CE Router support for a WAN-side E1 interface is Conditional, not Required	Immediate
5.3.2.15.4, 5.3.2.15.5	Edge Boundary Controller (EBC) Policing of DSCPs and Codec Bandwidths was changed from Conditional to Required	18-month Rule
5.3.2.15.6	Revised EBC Availability requirements to allow for four types of EBCs: High Availability with NLAS (99.999%), High Availability without NLAS (99.999%), Medium Availability (99.99%), and Low Availability (99.9%). No Loss of Active Sessions [NLAS]: Means that active sessions are not disrupted when an EBC component fails	Immediate

SECTION	CORRECTION	EFFECTIVE DATE
5.3.2.16.1	Added clarification that RTS support for Domain Name Service (DNS) is an FY10-FY12 objective, and not a requirement	Immediate
5.3.2.17.2	Revised requirements for Appliance support for multiple Ethernet interfaces for Network Management, Signaling, & Bearer Traffic 1) Support for two physical Ethernet interfaces on each LSC, MFSS (SS side), and WAN SS 2) Support for at least two logical Ethernet interfaces on each physical interface: one for VVOIP Signaling and Bearer VLAN; other for Local or Remote EMS VLAN 3) Local EMS VLAN on physical interface 1 backs up Remote EMS VLAN on physical interface 2, and vice versa These requirements apply to the LSC, MFSS, WAN SS, EBC, and CE Router.	18-month Rule
5.3.2.17.2	Added a pointer to Section 5.3.2.4.4 (VVoIP Network Management System Interface Requirements) into this Section (General Management Requirements). Added information to clarify that the requirements for local management access and RTS EMS access may be met through the use of either a physical or virtual Ethernet interface.	18-month Rule
5.3.2.20	Added new Section on “RTS Stateful Firewall (RSF) Requirements” 1) RSF protects the LSC, MFSS, or WAN SS from attacks from within the enclave 2) Use of the RSF is not a mandatory requirement; individual sites can determine if RSF protection is needed 3) RSF requirements are based on the EBC requirements (the EBC protects devices from attacks from outside of the enclave)	18-month Rule

SECTION	CORRECTION	EFFECTIVE DATE
5.3.2.21	Added new Section on “V.150.1 Modem Relay Secure Phone Support Requirements” 1) Ensures that MGs can support SCIP secure phones for all scenarios required by the National Security Agency (NSA) 2) Based on NSA’s SCIP-216 and SCIP-215 requirements for VoIP MGs and VoIP Secure Phones 3) Also requires V.150.1 support in TAs, IADs, & MG line cards (allows support for analog SCIP phones on RTS / UC)	18-month Rule
5.3.2.22	Added new Section on “Generic AS-SIP End Instruments & Video Codec Requirements” 1) Intent is that Voice EIs, Secure Voice EIs, and Video EIs can connect to and interoperate with any LSC using AS-SIP 2) Supports AS-SIP Hardphone & Softphone EIs 3) Supports AS-SIP Video EIs (Video Codecs), but not AS-SIP MCUs 4) Supports Multiple Call Appearances on AS-SIP Voice and Secure Voice EIs	18-month Rule
5.3.2.23	Added a new Section on “Requirements for Supporting Commercial Cost Avoidance” 1) Allows an LSC to upload DSN and commercial number data to a remote RTS Routing Database 2) Allows the LSC to query this Routing DB on calls that are dialed to commercial (PSTN) numbers (9+9+E.164 number) 3) If the DB responds with a matching DSN number, the call is routed over RTS or DSN using AS-SIP or a T1.619A PRI 4) If the DB responds with “No number found”, the LSC routes call to the PSTN over a commercial PRI trunk group	18-month Rule

SECTION	CORRECTION	EFFECTIVE DATE
5.3.2.24	Added a new Section on "Requirements for Supporting AS-SIP-Based Interfaces for Voice Mail and Unified Messaging Systems". These conditional requirements apply when the LSC, MFSS, or WAN SS supports an AS-SIP-based interface for interconnection with a standalone Voice Mail system or Unified Messaging system. The requirements include LSC, MFSS, and WAN SS support for: 1) RFC 3842, "A Message Summary and Message Waiting Indication Event Package for the Session Initiation Protocol (SIP)" 2) Internet Draft draft-levy-sip-diversion-08.txt, "Diversion Indication in SIP" 3) RFC 4244, "An Extension to the Session Initiation Protocol (SIP) for Request History Information" 4) RFC 3725, "Best Current Practices for Third Party Call Control (3pcc) in the Session Initiation Protocol"	18-month Rule

TABLE OF CONTENTS

SECTION **PAGE**

LIST OF FIGURES

LIST OF TABLES

5.3.2 Assured Services Requirements

5.3.2.1 Introduction

This section addresses required functionality, performance, capabilities, and associated technical parameters for the assured services components of the DISN Voice over IP (VoIP) and Video over IP services. The assured services components described include the Proprietary End Instrument (PEI), AS-SIP End Instrument (AEI), LSC, MFSS, EBC, and CE Router. In addition, appliance functions associated with the assured services components described and specified in detail include the CCA, MG, SG, NM, and the Open Loop ASAC technique. They are to be used by the product.

This section specifies the SBU VVoIP services while UCR 2008, Section 6.2, Unique Classified Requirements, specifies the classified VVoIP services. These voice and video services are assumed to be implemented on a converged B/P/C/S LAN and the converged DISN WAN. In this UCR section, "converged" means that all types of services, as defined by the Net-Centric Implementation Document (NCID), Version 2 (NCIDv2) Quality of Service (QoS) (T300), exist simultaneously on the same IP network. Nevertheless, networks still may be separated because of security issues, as specified in UCR 2008, Section 5.4, Information Assurance Requirements. However, the UC goal is one "black core" transporting all service types and all classification levels using HAIPE encryption, beginning at the DISN SDNs, then moving to the B/P/C/Ss, and eventually moving to the PEIs/AEIs/servers.

A "call" is a VoIP or Video over IP call that is placed or answered by a PEI/AEI end user, and a "session" is the underlying AS-SIP or Proprietary VoIP session that is processed by the PEI/AEI and the LSC. The human end users see the VoIP or Video over IP "call," and the assured services network devices, such as the PEI/AEI and the LSC, see the underlying AS-SIP or Proprietary VoIP "session." "Call" is a "human end-user perspective" term, and "session" is a technical term describing the VoIP signaling and media streams in the appliance that supports an individual end user's call.

The terms PEI and AEI are defined in Appendix A, Definitions, Abbreviations and Acronyms, and References, of this document. In short:

1. A PEI is a user appliance that interacts with the serving appliance (i.e., LSC, MFSS, or WAN SS) using a proprietary protocol to originate, accept, and/or terminate a voice, video, or data session(s).

2. An AEI is a user appliance that interacts with an associated serving appliance using the AS-SIP to originate, accept, and/or terminate a voice, video, and/or data session(s).

5.3.2.1.1 Requirements Terminology

The terms Required, Conditional, Objective, and Optional are used in this section.

Requirements are designated as Required or Conditional as defined in Section 5.1.4, General Specification Language. Objective requirements are desirable, but do not have to be deployed until 2012. A function or capability may be desired for 2010 **[Objective: 2010]** and required for 2012 **[Required: 2012]**.

In addition, some requirements may be labeled as "Conditional – Deployable." This is a variation of the "Conditional" case, where the requirement is Required for Fixed appliances, such as LSCs and MFSSs in Fixed DoD networks, but is Conditional for Deployable appliances, such as LSCs in Deployable DoD networks. In other words, "Conditional – Deployable" means "Required for Fixed appliances, but Conditional for Deployable appliances."

Some requirements refer to, or are based on, IETF RFCs, ANSI standards, and ITU standards, which allow certain features or capabilities to be designated as Optional for implementation. Vendors or implementers need to be careful to ensure that their products process packets correctly whether or not an Option is actually implemented. For example, in RFC 3711 the Master Key Identifier (MKI) 4-byte field is Optional and may or may not be used in constructing an outgoing voice packet. One end of a voice session may not insert the MKI field into the packet while the other end of the voice session (possibly using a different vendor's equipment) may choose to insert the MKI field. Since communications in both directions must still be achieved in this situation, it is incumbent on the vendors to process packets correctly whether or not the Option is implemented at each end.

The term appliance and its relationship to APL products are defined in Section 5.3.2.1.5, Functional Reference Terminology – APL Products and Appliances.

5.3.2.1.2 Network Reference Model

Figure 5.3.2.1-1, High-Level DISN Assured Services Network Model, shows a typical arrangement of an LSC and an MFSS in the DISN assured services voice and video network. This high-level DISN network model was used as the basis for the requirements for the LSC and MFSS in this section.

The network is a hierarchical network supporting:

- Local services and features within an Edge Segment (B/P/C/S)

- Global services and features across the UC network

- Services and features to DoD allied networks, DoD coalition networks, and the external PSTN

The network consists of UC APL products, such as the LSC and the MFSS. These products are interconnected via the converged IP transport network to support the following necessary functions for global services and features:

- Signaling functions (e.g., call control and feature control signaling)

- Bearer functions (e.g., interworking between packetized voice and TDM voice media streams; support for various media stream Coder/Decoders (codecs))

- Management functions (e.g., appliance fault, configuration, accounting, performance, and security (FCAPS) management)

- Information Assurance functions

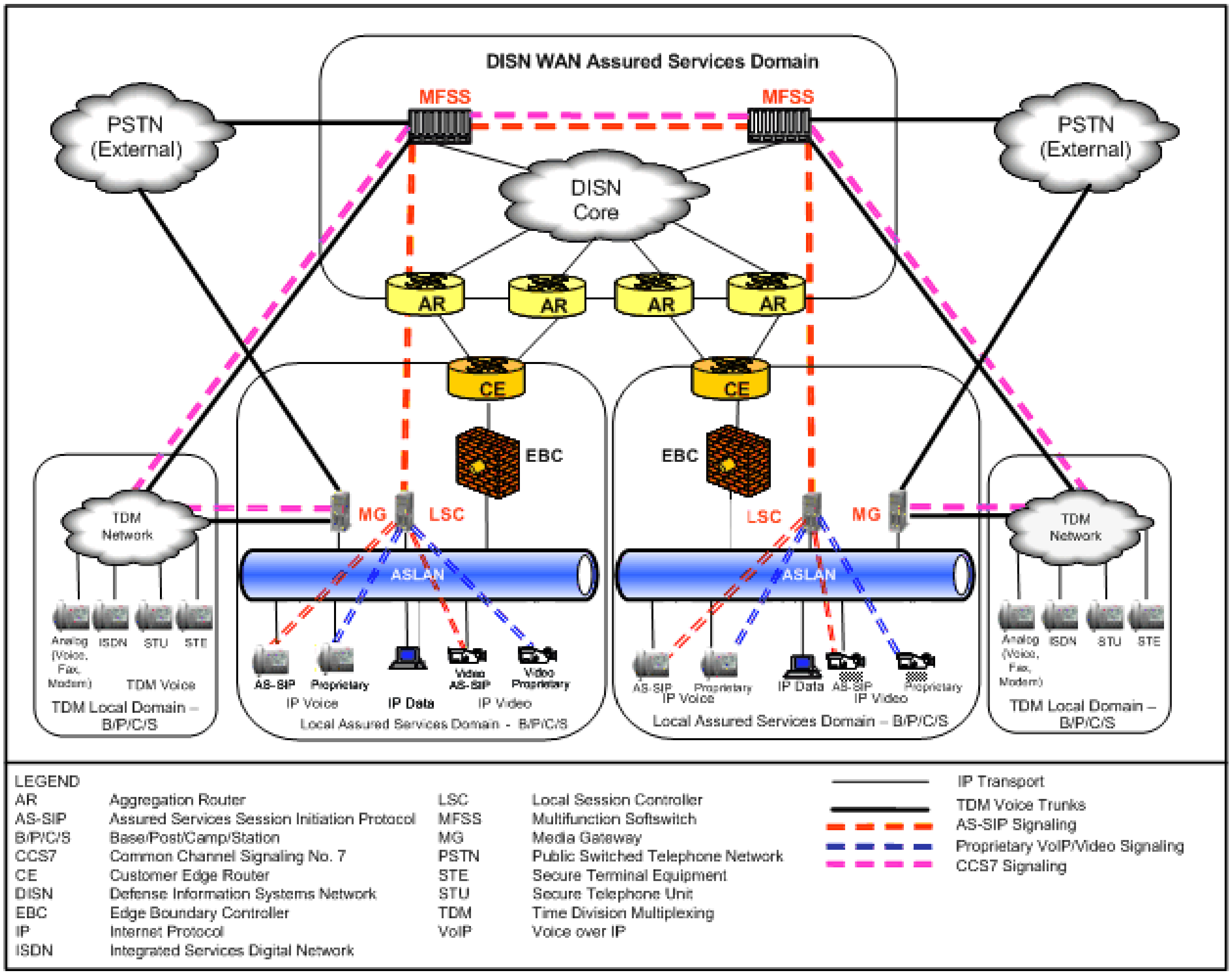

DISN WAN Assured Services Domain
MFSS
MFSS
PSTN (External)
PSTN (External)
DISN Core
AR
AR
AR
AR
CE
CE
EBC
EBC
MG
LSC
LSC
MG
ASLAN
ASLAN
TDM Network
TDM Network
Analog (Voice, Fax, Modem)
ISDN
STU
STE
TDM Voice
TDM Local Domain – B/P/C/S
AS-SIP
Proprietary
IP Voice
IP Data
Video AS-SIP
Video Proprietary
IP Video
Local Assured Services Domain - B/P/C/S
AS-SIP
Proprietary
IP Voice
IP Data
AS-SIP
Proprietary
IP Video
Local Assured Services Domain – B/P/C/S
Analog (Voice, Fax, Modem)
ISDN
STU
STE
TDM Local Domain – B/P/C/S
LEGEND
AR Aggregation Router
AS-SIP Assured Services Session Initiation Protocol
B/P/C/S Base/Post/Camp/Station
CCS7 Common Channel Signaling No. 7
CE Customer Edge Router
DISN Defense Information Systems Network
EBC Edge Boundary Controller
IP Internet Protocol
ISDN Integrated Services Digital Network
LSC Local Session Controller
MFSS Multifunction Softswitch
MG Media Gateway
PSTN Public Switched Telephone Network
STE Secure Terminal Equipment
STU Secure Telephone Unit
TDM Time Division Multiplexing
VoIP Voice over IP
IP Transport
TDM Voice Trunks
AS-SIP Signaling
Proprietary VoIP/Video Signaling
CCS7 Signaling

Figure 5.3.2.1-1. High-Level DISN Assured Services Network Model

In 2010, the network is expected to allow existing TDM trunk and signaling link connectivity to remain, including

- PRI, CAS, and DoD CCS7 trunks and signaling links between MFSSs, and
- PRI, CAS, and DoD CCS7 trunks and signaling links between LSCs and MFSSs, when needed.

In addition, PRI, CAS, and DoD CCS7 connectivity from MFSSs to other DoD TDM switches will still exist in the network.

5.3.2.1.3 General Assumptions

The following five general assumptions apply to the components described throughout this section (NOTE: The assumptions apply to the CCA, SG, and NM. In addition, the assumptions were used to develop VoIP, Facsimile over IP (FoIP), Modem over IP (MoIP), SCIP over IP, and ISDN over IP requirements for the MG within the UCR 2008.):

1. The LSC and MFSS will support 911 services for VoIP and TDM end users. Within the United States, 911 calls from VoIP and TDM lines may be routed either to a DoD Emergency Response Center, or to a PSTN 911 Selective Router (SR) and PSAP, depending on the LSC or MFSS configuration. The emergency services network that handles DoD and PSTN 911 calls may be TDM based or IP based. Outside the United States, 911 calls from VoIP and TDM lines may be routed to a DoD Emergency Response Center (if one exists within the DoD location), depending on the LSC or MFSS configuration.

   The details of the 911-service infrastructure within the network are outside the scope of the CCA VoIP and Video over IP requirements in this section.

2. In some cases, a function like an MGC or MG will be labeled as Conditional – Deployable in this section. In these cases, Conditional – Deployable means that normally this function is not used in a Deployable environment, but may be used in that environment under certain conditions. When this function is used in that environment, the function should conform to the MG requirements in this section. For example, an LSC deployed in one camp in a war zone overseas may not use an MGC or an MG, while another LSC deployed in another camp in the same zone may use both of them.

3. The CCA VoIP, FoIP, MoIP, SCIP over IP, and ISDN over IP requirements in this section assume that all functions within an individual appliance (i.e., LSC or MFSS) are provided by the same appliance supplier. Within a collection of network appliances, the same supplier may provide all appliances, or one supplier may provide some appliances and other suppliers may provide other appliances.

4. Interoperability between LSCs, MFSSs, and the MG requirements in this section is the goal of the UCR 2008. Integration between the functions within an individual LSC or MFSS is the responsibility of the network appliance supplier.

5. “Assured Services for Voice and Video” supports VoIP, voiceband FoIP, voiceband data (modems) over IP, SCIP over IP, ISDN over IP, and Video over IP. The voice budgets used to manage end users’ VoIP calls will manage those users’ VoIP calls collectively, FoIP calls, MoIP calls, and SCIP over IP calls. The separate video budgets used to manage end users’ Video over IP calls will manage those users’ Video over IP calls only, and will not manage any VoIP, FoIP, MoIP, or SCIP over IP calls for those users. In short, VoIP budgets and Video over IP budgets are maintained and managed separately in voice and video assured services.

Other assumptions are as follows:

1. The MFSS is assumed to support AS-SIP connectivity (for connections to other MFSSs and LSCs) and TDM connectivity (for connections to other MFSSs and DoD TDM switches). The TDM connectivity can use CCS7, PRI, or CAS signaling.

2. The LSC is assumed to include an MGC and an MG **[Required: Fixed – Conditional: Deployable]**, and an SG **[Conditional]**, which means that the TDM trunk groups that terminate on the LSC MG can use PRI, CAS, or CCS7 signaling.

3. The MFSS supports end users on both the SS (VoIP) side (i.e., VoIP end users using VoIP EIs) and on the TDM/EO side (i.e., end-users with traditional TDM-based telephones).

4. The MFSS supports TDM trunks on both its SS side (through the MGC and MG) and on the TDM side. Interworking between the TDM side and the SS side of the MFSS is considered an internal interface within the MFSS product. The internal interface may use CCS7 to AS-SIP conversion via an SG or ISDN-PRI, or CAS via an MG.

5. The VoIP signaling protocol used between the VoIP EI and the LSC (and between the VoIP EI and the LSC part of an MFSS) can be vendor proprietary. The VoIP signaling protocol does not need to be AS-SIP between a VoIP EI and LSC (or between the VoIP EI and the LSC component of an MFSS). The VoIP signaling protocol used between the VoIP AEI and the LSC (and between the VoIP AEI and the LSC part of an MFSS) cannot be vendor proprietary. The VoIP signaling protocol shall be AS-SIP between a VoIP AEI and LSC (or between the VoIP AEI and the LSC component of an MFSS). The VoIP signaling protocol used between VVoIP signaling appliances (i.e., LSCs and MFSSs) is required to be AS-SIP.

6. Both the LSC and the MFSS will use Location services (i.e., local or global, as needed) to route calls to their intended destination. Location services will be supported as an internal function of the LSC or MFSS, instead of an external function that the LSC or MFSS would have to access over an external interface using an industry-standard Location services protocol.

7. Route selections at the LSCs and the MFSS will be based on the originating call signaling type (i.e., either IP or TDM signaling). If the originating signaling is IP based, it is assumed that the call signaling will stay IP based for as long as possible as the signaling transits the network. Similarly, if the originating call signaling is TDM based, the call signaling will stay TDM based for as long as possible as the signaling transits the network.

8. Tones and announcements that are provided to VoIP end users will be provided from an internal media server, which is a functional component of the LSC or MFSS. An external media server that is separate from the LSC or MFSS is not envisioned.

9. The CCA VoIP and Video over IP requirements in this section assume that the same appliance supplier provides all functions within an individual appliance (e.g., LSC or MFSS). Within a collection of network appliances, the same supplier may provide all appliances, or one supplier may provide some appliances and other appliances may be provided by other suppliers, but will be offered as part of a single APL product.

10. The LSC supports MGC and MG functionality so that LSCs can support access to DoD TDM networks, allied TDM networks, coalition partner TDM networks, and the local PSTN when this access is needed in both Fixed and Deployable environments. In addition, the LSC supports MGC and MG functionality to enable TDM connectivity (i.e., PRI, CAS, and CCS7 trunks and signaling links) to interconnecting MFSSs when it is needed.

11. The LSCs and MFSSs will support proprietary VoIP videophones (using the vendor's version of SIP or H.323). The LSC and MFSS suppliers should also support AS-SIP videophones. The LSC and MFSS suppliers are required to support protocol interworking between their videophones (Proprietary VoIP and AS-SIP) and the AS-SIP protocol used on network-side interfaces between LSCs and MFSSs (and between LSCs, and between MFSSs).

12. The LSC MG(s) and the WAN SS MG(s) may be located at distributed/remote sites that are not the same site as that of the associated LSC or WAN SS. The MG control communications will be over the DISN/MILDEP Enterprise WAN and are expected to use the same control protocol used by the vendor when the MG is on the same local Ethernet LAN as the LSC CCA or WAN SS. This assumption is intended to allow the MILDEPs to use regional LSCs or WAN SSs enterprise architectures. It is the MILDEP's responsibility to ensure that when such enterprise architectures are employed, the signaling delays and media path delays remain within the requirements specified in UCR 2008, Section 5.3.3, Network Infrastructure End-to-End Performance Requirements. Also, the Information Assurance requirements of UCR 2008, Section 5.4, Information Assurance Requirements, including the use of firewalls still apply.

5.3.2.1.4 Information Assurance

Information Assurance Requirements are described in UCR 2008, Section 5.4, Information Assurance Requirements.

The Information Assurance function within the products and appliance functions ensures that end users, PEIs, AEIs, MGs, SGs, and EBCs that use 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 Assured Services Local Area Network (ASLAN) are encrypted properly (using SIP/Transport Layer Security (TLS) and Secure Real Time Protocol (SRTP), respectively).

5.3.2.1.5 Functional Reference Terminology – APL Products and Appliances

This paragraph describes relationships between VoIP and Video over IP network components, appliance functions, and UC products to be tested for APL certification. The term "appliance function" is introduced because IP-based UC APL products will often consist of software functions and features (e.g., appliances) that are distributed over several hardware components connected over a network infrastructure (e.g., LAN), while a TDM-based APL product, such as an EO, consists of a single unit containing all required telephony functions. Appliances operate at the signaling, bearer, and NM planes. Appliance functions are described and referred to throughout the UCR 2008, but are not considered products for APL certification; rather, they are functions and features that form a part of a UC APL product. Table 5.3.2.1-1, Summary of Appliances and UC APL Products, provides a summary of appliances and APL products.

Table 5.3.2.1-1. Summary of Appliances and UC APL Products

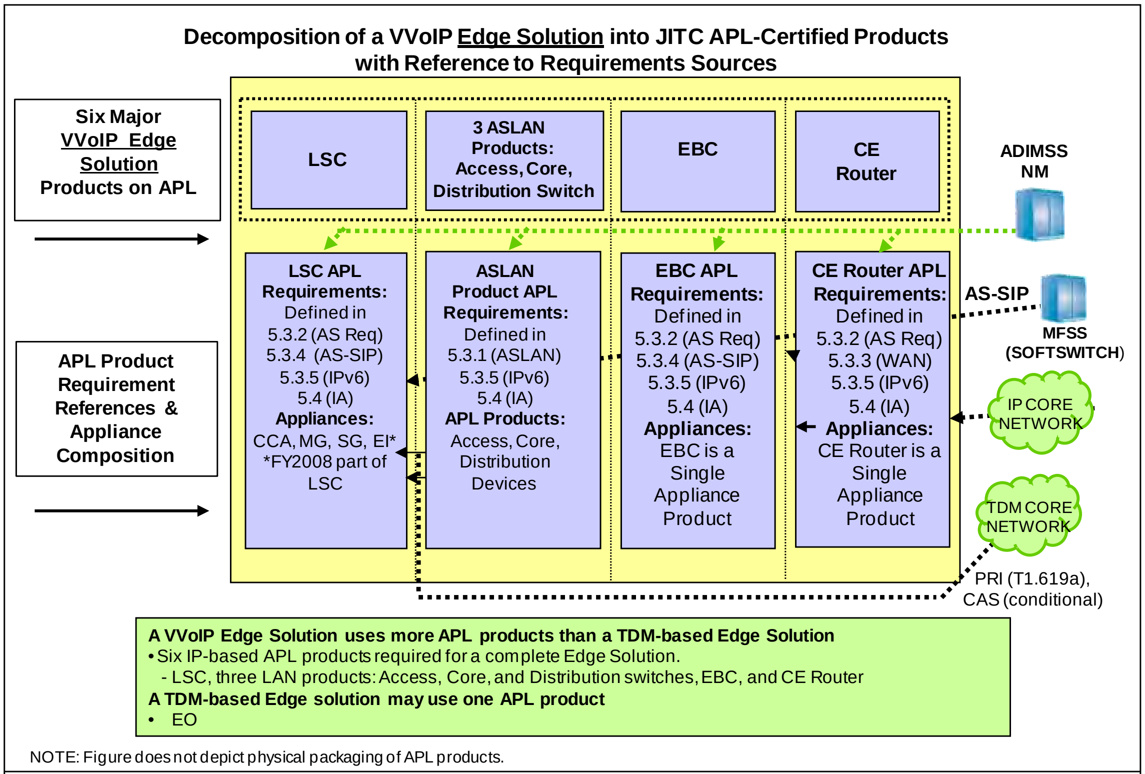
ITEM	ITEM CATEGORY	ROLE AND FUNCTIONS
EI	Appliance	Appliance part of LSC
AEI	APL Product	Product consisting of a single appliance
MG	Appliance	Media conversion function as part of the LSC and MFSS
SG	Appliance	Signaling conversion function as part of the LSC and MFSS
AS-SIP Signaling Appliance	Appliance	Appliance function within an LSC and MFSS that provides AS-SIP signaling capability
CCA	Appliance	Appliance function within an LSC and MFSS that performs parts of session control and signaling functions
Registrar	Appliance	Appliance function that stores the location of a registrant and its profile
Registrant	Appliance	Appliance function used to register with the network to seek and gain authority to invoke services or resources from the network
LAN Switch/Router (Access, Distribution, and Core)	APL Products	APL products used in an ASLAN
SEI	APL Product	Product consisting of a single appliance
LSC	APL Product	Product providing many local telephony functions
MFSS	APL Product	Large, complex product providing many local and WAN-related telephony functions

ITEM	ITEM CATEGORY	ROLE AND FUNCTIONS
WAN SS	APL Product	A standalone APL product that acts as an AS-SIP B2BUA within the UC architecture. It provides the equivalent functionality of a commercial SS and has similar functionality to the SS component of an MFSS.
Dual Signaling Softswitch (DSSS)	APL product	A WAN SS used in the Classified network that has both H.323 and AS-SIP signaling
Dual Signaling Multipoint Control Unit (DSMCU)	APL product	APL product that supports multiple video conferencing signaling protocols, H.320, H.323, and AS-SIP
EBC	APL Product	Product providing firewall functions
CE Router	APL Product	Product providing routing functions at the enclave boundary
DISN WAN P/PE Router	APL product	Product providing routing of IP packets
DISN MSPP	APL Product	Product providing transport access to the DISN WAN
M1-3 Multiplexer	APL Product	Product providing transport interface to the DISN
DISN Optical Switch	APL product	Product serving as an optical transport node

LEGEND

APL	Approved Products List	LAN	Local Area Network
ASLAN	Assured Services Local Area Network	LSC	Local Session Controller
AS-SIP	Assured Services Session Initiation Protocol	MFSS	Multifunction Softswitch
B2BUA	Back-to-Back User Agent	MG	Media Gateway
CCA	Call Connection Agent	MSPP	Multi-Service Provisioning Platforms
CE	Customer Edge	P	Provider
DISN	Defense Information System Network	PE	Provider Edge
EBC	Edge Boundary Controller	SEI	Secure End Instrument
EI	End Instrument	SG	Signaling Gateway
AEI	AS-SIP End Instrument	WAN	Wide Area Network
IP	Internet Protocol		

The architectural differences between TDM-based APL products and IP-based APL products are illustrated further in Figure 5.3.2.1-2, IP-Based Voice Edge Solution in Terms of the JITC APL Approved Products. The figure illustrates how several appliance functions and APL products replace what is provided by a single TDM-based APL product (e.g., DSN EO) to provide telephone service on a B/P/C/S. It also illustrates how an IP-based edge solution is composed of JITC APL components.


Decomposition of a VVoIP Edge Solution into JITC APL-Certified Products
with Reference to Requirements Sources
Six Major VVoIP Edge Solution Products on APL
APL Product Requirement References & Appliance Composition
LSC
3 ASLAN Products: Access, Core, Distribution Switch
EBC
CE Router
ADIMSS NM
LSC APL Requirements: Defined in 5.3.2 (AS Req) 5.3.4 (AS-SIP) 5.3.5 (IPv6) 5.4 (IA) Appliances: CCA, MG, SG, EI* *FY2008 part of LSC
ASLAN Product APL Requirements: Defined in 5.3.1 (ASLAN) 5.3.5 (IPv6) 5.4 (IA) APL Products: Access, Core, Distribution Devices
EBC APL Requirements: Defined in 5.3.2 (AS Req) 5.3.4 (AS-SIP) 5.3.5 (IPv6) 5.4 (IA) Appliances: EBC is a Single Appliance Product
CE Router APL Requirements: Defined in 5.3.2 (AS Req) 5.3.3 (WAN) 5.3.5 (IPv6) 5.4 (IA) Appliances: CE Router is a Single Appliance Product
AS-SIP
MFSS (SOFTSWITCH)
IP CORE NETWORK
TDM CORE NETWORK
PRI (T1.619a), CAS (conditional)
A VVoIP Edge Solution uses more APL products than a TDM-based Edge Solution
• Six IP-based APL products required for a complete Edge Solution.
- LSC, three LAN products: Access, Core, and Distribution switches, EBC, and CE Router
A TDM-based Edge solution may use one APL product
• EO
NOTE: Figure does not depict physical packaging of APL products.

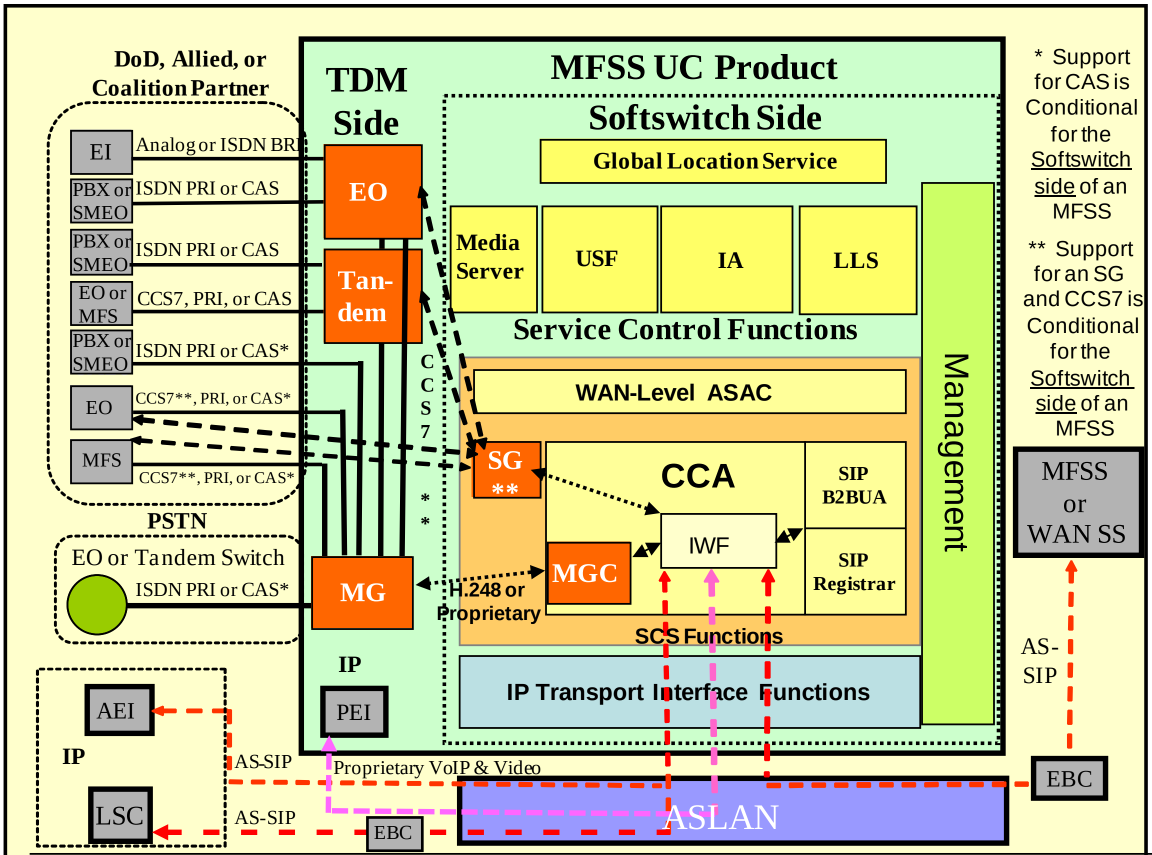
LEGEND

ADIMSS	Advanced DSN Integrated Management Support System
APL	Approved Products List
ASLAN	Assured Service Local Area Network
AS-SIP	Assured Services Session Initiation Protocol
CAS	Channel Associated Signaling
CCA	Call Connection Agent
CE	Customer Edge Router
EBC	Edge Boundary Controller
EI	End Instrument
EO	End Office
FY	Fiscal Year
IA	Information Assurance
IP	Internet Protocol
IPv6	Internet Protocol Version 6
JITC	Joint Interoperability Test Command
LAN	Local Area Network
LSC	Local Session Controller
MFSS	Multifunction Softswtich
MG	Media Gateway
NM	Network Management
PRI	Primary Rate Interface
SG	Signaling Gateway
TDM	Time Division Multiplexing
VVoIP	Voice and Video over IP
WAN	Wide Area Network

Figure 5.3.2.1-2. IP-Based Voice Edge Solution in Terms of JITC APL Approved Products

Figure 5.3.2.1-3, Functional Reference Model for an MFSS, and Figure 5.3.2.1-4, Functional Reference Model for an LSC, represent the DISN Reference Functional Model for an MFSS and for an LSC. The two figures illustrate appliance functions internal to the MFSS and LSC UC products configurations. The appliance functions, which include the CCA, Interworking Function (IWF), MGC, SG, and MG are described in subsequent paragraphs within this section.

All interfaces between appliances contained with the MFSS and LSC shown in Figure 5.3.2.1-3 and Figure 5.3.2.1-4 are internal, proprietary interfaces. Interfaces between one APL product and functional entities in physically different APL products are standards-based external interfaces.

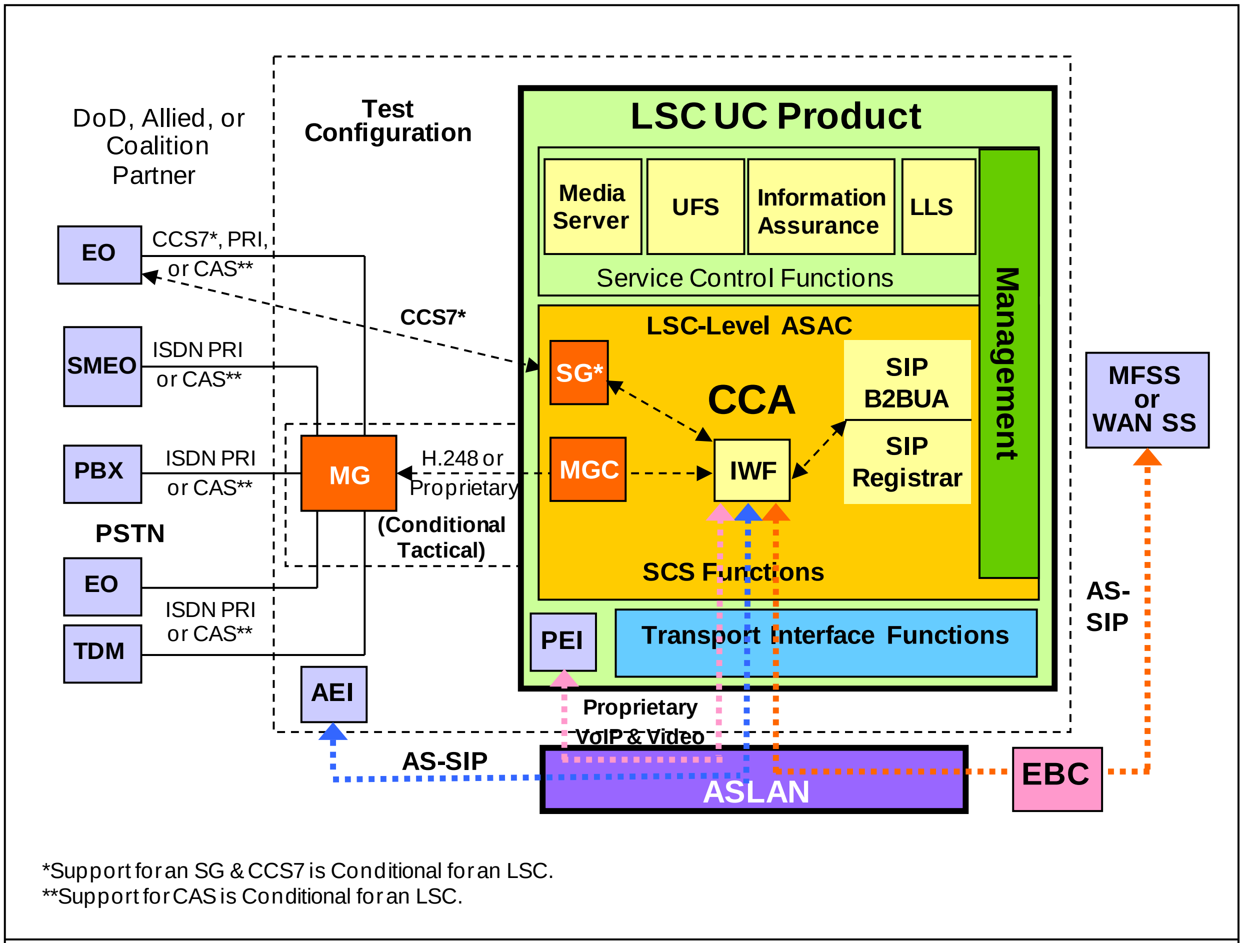


LEGEND:

AEI	AS-SIP End Instrument
ASAC	Assured Service Admission Control
ASLAN	Assured Services Local Area Network
AS-SIP	Assured Services Session Initiation Protocol
B2BUA	Back-to-Back User Agent
CAS	Channel Associated Signaling
CCA	Call Connection Agent
CCS7	Common Channel Signaling No. 7
DoD	Department of Defense
EBC	Edge Border Controller
EO	End Office
IA	Information Assurance
ISDN	Integrated Services Digital Network
IWF	Interworking Function
LLC	Logical Link Control [sublayer]
LSC	Local Session Controller
MFS	Multifunction Switch
MFSS	Multifunction Softswitch
MG	Media Gateway
MGC	Media Gateway Controller
PBX	Private Branch Exchange
PEI	Proprietary End Instrument
PRI	Primary Rate Interface
PSTN	Public Switched Telephone Network
SCS	Session Control and Signaling
SG	Signaling Gateway
SIP	Session Initiation Protocol
SUT	System Under Test
TDM	Time Division Multiplexer
USF	User Service and Feature
WAN	Wide Area Network

Note: The PEI (using Proprietary VoIP and Video) is part of the MFSS UC Product ; the AEI (using AS-SIP VoIP and Video) is not.

Figure 5.3.2.1-3. Functional Reference Model – MFSS



*Support for an SG & CCS7 is Conditional for an LSC.
**Support for CAS is Conditional for an LSC.

LEGEND:

AEI	AS-SIP End Instrument
ASAC	Assured Service Admission Control
ASLAN	Assured Services Local Area Network
AS-SIP	Assured Services Session Initiation Protocol
B2BUA	Back-to-Back User Agent
CAS	Channel Associated Signaling
CCA	Call Connection Agent
CCS7	Common Channel Signaling No. 7
DoD	Department of Defense
EBC	Edge Border Controller
EO	End Office
ISDN	Integrated Services Digital Network
IWF	Interworking Function
LLS	Local Location Service
LSC	Local Session Controller
MFS	Multifunction Switch
MFSS	Multifunction Softswitch
MG	Media Gateway
MGC	Media Gateway Controller
PBX	Private Branch Exchange
PEI	Proprietary End Instrument
PRI	Primary Rate Interface
PSTN	Public Switched Telephone Network
SCS	Session Control and Signaling
SG	Signaling Gateway
SIP	Session Initiation Protocol
TDM	Time Division Multiplexer
UC	Unified Capabilities
UFS	User Features and Services

Note: The PEI (using Proprietary VoIP and Video) is part of the LSC UC Product; the AEI (using AS-SIP VoIP and Video) is not.

Figure 5.3.2.1-4. Functional Reference Model – LSC

5.3.2.2 Assured Services Product Features and Capabilities

5.3.2.2.1 Overview of VoIP and Video over IP Product Design Attributes

A key component of the military robust VoIP and Video over IP product design is the Assured Services subsystem. The Assured Services subsystem addresses Assured Services by replacing the current TDM-based Multilevel Precedence and Preemption (MLPP) functionality with IP-based ASLANs and ASAC. The Assured Services subsystem, in conjunction with the ASLAN subsystem, and the DISN WAN subsystem make up the total product that is required to initiate, supervise, and terminate voice and video, precedence and preemption sessions on an EI-to-EI basis, while functioning within a converged total DoD UC network.

The logical location of the major VVoIP attributes within the UC E2E system is shown in Figure 5.3.2.2-1, Overview of VVoIP System Design Attributes. The location of attributes in terms of Edge (B/P/C/S) and the network infrastructure (access and DISN Core) is depicted, and the differentiation between assured service and non-assured service is shown between the top half of the diagram and the bottom half of the diagram, respectively.

The functions contained in the boxes located within the top half of Figure 5.3.2.2-1 constitute the scope of the Assured Services subsystem, while the placement of the boxes indicates where in the overall VoIP and Video over IP product design (WAN to Edge) the functions logically reside. Voice, video, and data sessions are converged in the DISN WAN and the ASLAN, while the Assured Services subsystem in 2012 is anticipated to support voice, video, and non-real-time sessions with priority.

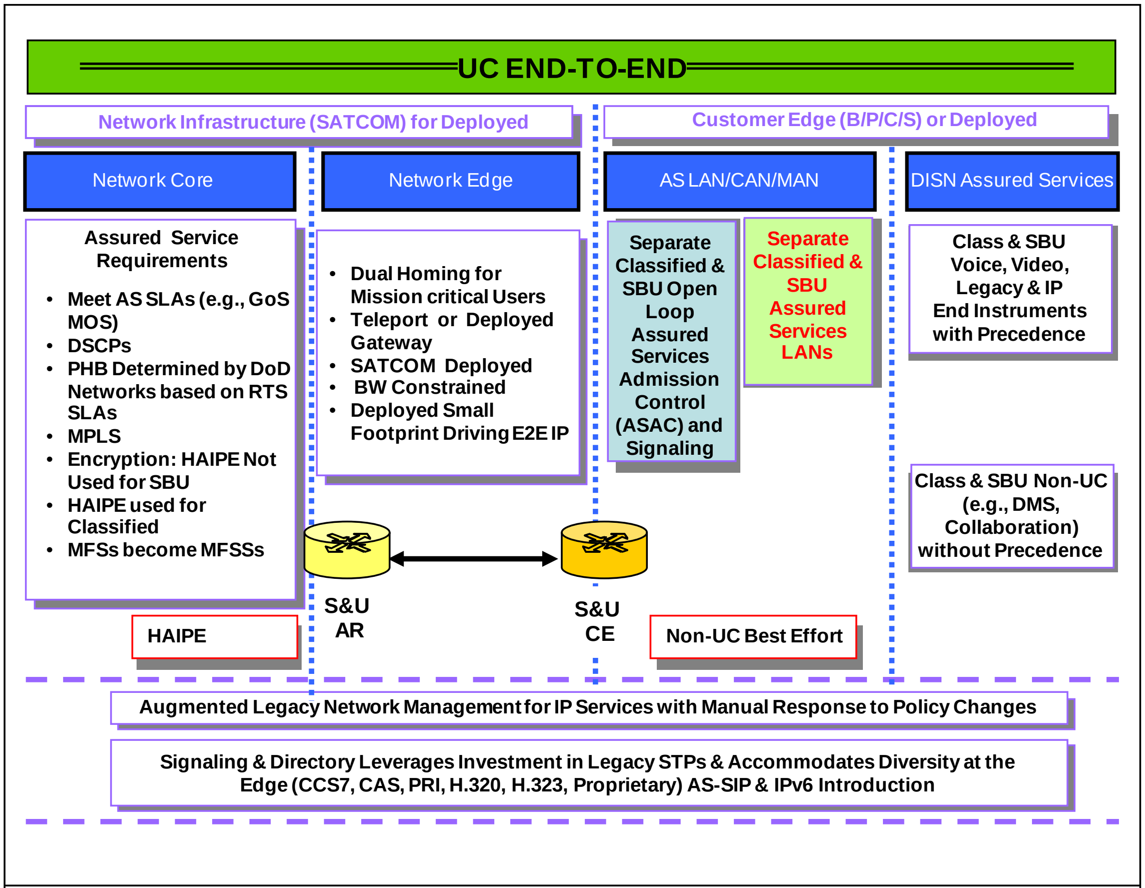
5.3.2.2.1.1 Attributes within the Edge Segment

The attributes within the Edge Segment include the following:

1. Nonblocking ASLAN. At the Edge, the design has an ASLAN that is designed as nonblocking for voice and video traffic.

2. Traffic Admission Control. The LSCs on a B/P/C/S use an Open Loop ASAC technique to ensure that only as many user-originated sessions (voice and video) in precedence order are permitted on the traffic-engineered access circuit, consistent with maintaining a voice quality of 4.0 as measured by the MOS method.

3. Call Preemption. Lower precedence sessions will be preempted on the access circuit to accept the LSC setup of higher precedence level outgoing or incoming session establishment requests.


UC END-TO-END
Network Infrastructure (SATCOM) for Deployed
Customer Edge (B/P/C/S) or Deployed
Network Core
Network Edge
AS LAN/CAN/MAN
DISN Assured Services
Assured Service Requirements
• Meet AS SLAs (e.g., GoS MOS)
• DSCPs
• PHB Determined by DoD Networks based on RTS SLAs
• MPLS
• Encryption: HAIPE Not Used for SBU
• HAIPE used for Classified
• MFSSs become MFSSs
• Dual Homing for Mission critical Users
• Teleport or Deployed Gateway
• SATCOM Deployed
• BW Constrained
• Deployed Small Footprint Driving E2E IP
Separate Classified & SBU Open Loop Assured Services Admission Control (ASAC) and Signaling
Separate Classified & SBU Assured Services LANs
Class & SBU Voice, Video, Legacy & IP End Instruments with Precedence
Class & SBU Non-UC (e.g., DMS, Collaboration) without Precedence
S&U AR
S&U CE
HAIPE
Non-UC Best Effort
Augmented Legacy Network Management for IP Services with Manual Response to Policy Changes
Signaling & Directory Leverages Investment in Legacy STPs & Accommodates Diversity at the Edge (CCS7, CAS, PRI, H.320, H.323, Proprietary) AS-SIP & IPv6 Introduction

LEGEND:

AR	Aggregation Router
AS	Assured Services
ASAC	Assured Services Admission Control
AS-SIP	Assured Services SIP
BW	Bandwidth
C2	Command and Control
CAN	Campus Area Network
CAS	Channel Associated Signaling
CCS7	Common Channel Signaling System No. 7
CE	Customer Edge Router
DISN	Defense Information Systems Network
DMS	Defense Message System
DSCP	Differentiated Services Code Point
E2E	End to End
GIG	Global Information Grid
GOS	Grade of Service
HAIPE	High Assurance Internet Protocol Encryptor
IP	Internet Protocol
IPv6	Internet Protocol version 6
LAN	Local Area Network
MAN	Metropolitan Area Network
MFS	Multifunction Switch
MFSS	Multifunction Softswitch
MOS	Mean Opinion Score
MPLS	Multiprotocol Label Switching
OCONUS	Outside CONUS
PHB	Per Hop Behavior
PRI	Primary Rate Interface
RTS	Real Time Services
S&U	Secret and Unclassified
SATCOM	Satellite Communications
SBU	Sensitive But Unclassified
SDN	Service Delivery Node
SLA	Service Level Agreement
STP	Signal Transfer Point

Figure 5.3.2.2-1. Overview of VVoIP System Design Attributes

4. Voice and Video Traffic Service Classification and Priority Queues. In terms of the CE Router queuing structure, voice and video traffic will be assigned to the higher priority queues by Aggregated Service Class as described in Section 5.3.3, Network Infrastructure End-to-End Performance Requirements.

5.3.2.2.1.2 Attributes within the DISN WAN (Access/Distribution and Core)

Under the access part of the DISN WAN, dual homing is required between the CE Router and the AR that serve an ASLAN having FO/F users and I/P users, and R users. Dual homing is conditional for cases where only Routine Users [I/P (ROUTINE) and non-I/P users] are supported. In 2010, SBU ASLANs do not use HAIPEs. The DISN Core part of the DISN WAN is assumed to be bandwidth rich, i.e., the bandwidth from the AR to AR, for whatever AR queue the voice and video traffic is placed in, is greater than or equal to the voice and video traffic-engineered load/bandwidth required for the voice/video busy-hour traffic in each of the DISN worldwide geographic locations. Since the ASLAN is required to be implemented as nonblocking for voice and video traffic, the access circuit from the Customer Edge Segment to the DISN Core SDN is the only potential bandwidth-limited resource requiring the use of ASAC to prevent session overload from the Edge Segment. The DISN WAN provides high availability (99.96 percent or greater) using dual-homed access circuits and the MPLS fast reroute (FRR) in the Network Core. Naturally, users are provided a lower availability if they choose not to or cannot implement dual homing.

5.3.2.2.1.3 E2E Protocol Planes

End-to-end services are set up, managed, and controlled by a series of functions or protocols that operate in three planes commonly referred to as signaling, bearer, and NM planes.

The signaling plane is associated with the signaling and control protocols, such as AS-SIP, H.323, and RSVP.

The transport plane is associated with the bearer traffic and protocols, such as SRTP and RTCP.

The NM plane is associated with NM protocols and is used to transfer status and configuration information between an NMS and a network appliance. Network management protocols include SNMP, Common Open Policy Service (COPS), and Secure Shell Version 2 (SSHv2).

5.3.2.2.1.4 DSCP Packet Marking

[Required: PEI, AEI, LSC, MFSS] As part of the session setup process, the LSC controls what DSCP to use in the subsequent session media stream packets.

For inter-LSC media sessions (across the WAN),

- The PEI or AEI shall be commanded by the LSC about which DSCP to insert in the session media stream packets, or

- The PEI or AEI shall populate the DSCP marking on its own.

[Required: PEI, AEI, LSC, MFSS] The exact DSCP method used by the implementer shall comply with Section 5.3.3, Network Infrastructure End-to-End Performance Requirements.

[Required: PEI, AEI, LSC, MFSS] For intra-LSC media streams (internal to the enclave),

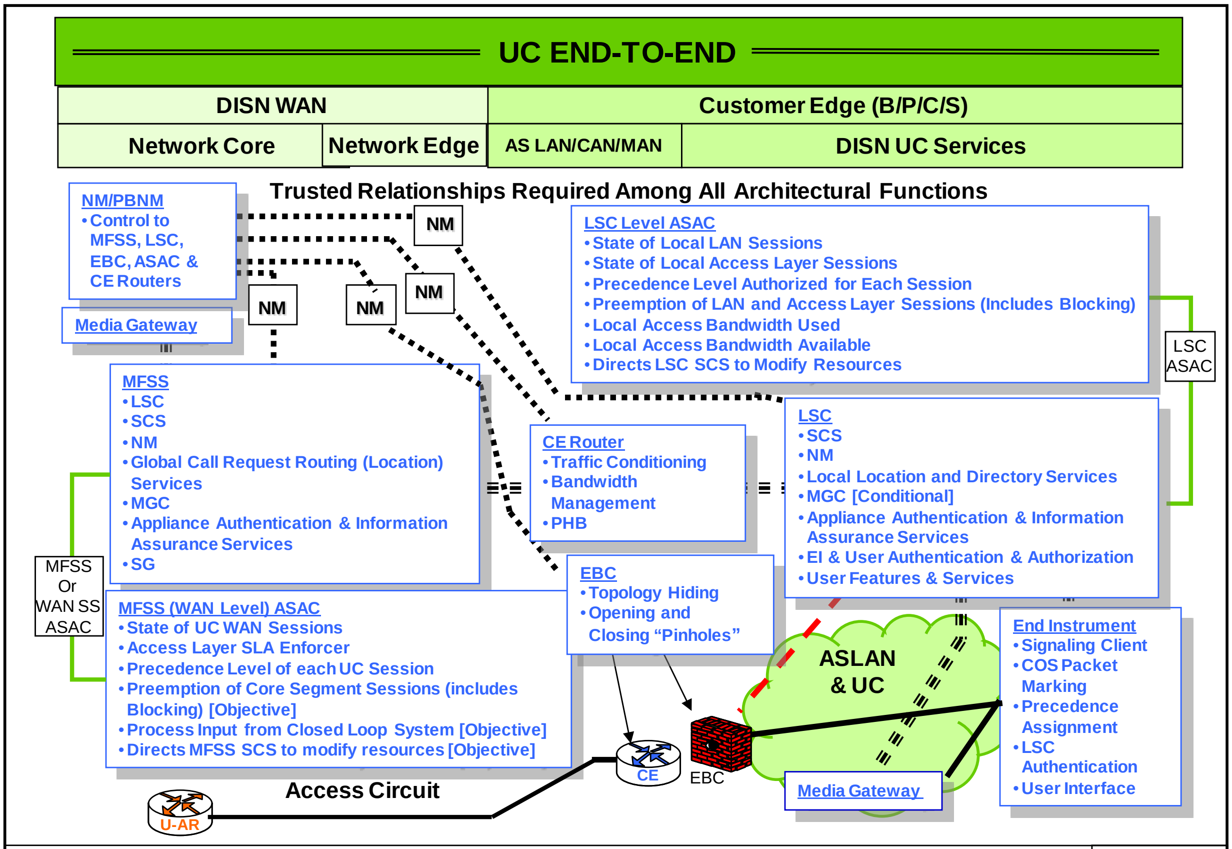
- The PEI or AEI shall be commanded by the LSC about which DSCP to insert in the session media stream packets, or

- The PEI or AEI shall populate the DSCP marking on its own, or

- The PEI or AEI shall use a standard ROUTINE DSCP marking for all voice media streams (or video media streams) IAW Section 5.3.3, Network Infrastructure End-to-End Performance Requirements. NOTE: This "ROUTINE DSCP" option will be deleted in the next version of the UC Requirements.

5.3.2.2.2 Assured Services Subsystem

The Assured Services subsystem, shown in Figure 5.3.2.2-2, Assured Services Subsystem Functional Diagram; the DISN WAN subproduct (see Section 5.3.3, Network Infrastructure End-to-End Performance Requirements); and the ASLAN subproduct (see Section 5.3.1, ASLAN Infrastructure Product Requirements) make up the total system These subproducts are required to initiate, supervise, and terminate voice and video, precedence and preemption sessions on an EI-to-EI basis, while functioning within a converged DoD network.


UC END-TO-END
DISN WAN
Customer Edge (B/P/C/S)
Network Core
Network Edge
AS LAN/CAN/MAN
DISN UC Services
Trusted Relationships Required Among All Architectural Functions
NM/PBNM
• Control to MFSS, LSC, EBC, ASAC & CE Routers
Media Gateway
NM
NM
NM
NM
LSC Level ASAC
• State of Local LAN Sessions
• State of Local Access Layer Sessions
• Precedence Level Authorized for Each Session
• Preemption of LAN and Access Layer Sessions (Includes Blocking)
• Local Access Bandwidth Used
• Local Access Bandwidth Available
• Directs LSC SCS to Modify Resources
LSC ASAC
MFSS
• LSC
• SCS
• NM
• Global Call Request Routing (Location) Services
• MGC
• Appliance Authentication & Information Assurance Services
• SG
CE Router
• Traffic Conditioning
• Bandwidth Management
• PHB
LSC
• SCS
• NM
• Local Location and Directory Services
• MGC [Conditional]
• Appliance Authentication & Information Assurance Services
• EI & User Authentication & Authorization
• User Features & Services
MFSS Or WAN SS ASAC
MFSS (WAN Level) ASAC
• State of UC WAN Sessions
• Access Layer SLA Enforcer
• Precedence Level of each UC Session
• Preemption of Core Segment Sessions (includes Blocking) [Objective]
• Process Input from Closed Loop System [Objective]
• Directs MFSS SCS to modify resources [Objective]
EBC
• Topology Hiding
• Opening and Closing “Pinholes”
ASLAN & UC
End Instrument
• Signaling Client
• COS Packet Marking
• Precedence Assignment
• LSC Authentication
• User Interface
CE
EBC
Media Gateway
Access Circuit
U-AR

LEGEND

AS	Assured Services	EBC	Edge Boundary Controller	PHB	Per Hop Behavior
ASAC	Assured Service Admission Control	EI	End Instrument	RTS	Real Time Services
ASLAN	Assured Service Local Area Network	IA	Information Assurance	SCS	Session Control and Signaling
B/P/C/S	Base/Post/Camp/Station	LSC	Local Session Controller	SG	Signaling Gateway
C2	Command and Control	MFSS	Multifunction Softswitch	SLA	Service Level Agreement
CE	Customer Edge Router	MGC	Media Gateway Controller	UC	Unified Capabilities
COS	Class of Service	NM	Network Management	U-AR	Unsecure Aggregated Router
DISN	Defense Information Systems Network	PBNM	Policy Based NM	WAN	Wide Area Network

Signaling ≡ ≡ ≡ ≡ ≡ ≡
Bearer ━━━━━━
Router Control ▬ ▬

Figure 5.3.2.2-2. Assured Services Subsystem Functional Diagram

The functions contained in the Figure 5.3.2.2-2 boxes and the EBC router symbol constitute the scope of the Assured Services subsystem, while the placement of the boxes indicates where in the overall system (WAN to Edge) the functions logically reside.

Voice, video, and data sessions are converged in the DISN WAN and the ASLAN, while assured services are provided for voice and video sessions only.

The functional behavior and performance metrics for each of the assured services major functions defined by a box in Figure 5.3.2.2-2 and subordinate functions listed within each box are specified in this section. Also, the interfaces between the major functional groupings (defined by a box) are specified in terms of electrical interfaces, protocols operating over these electrical interfaces, and their associated parameters. Best commercial practices and existing standards will be specified to the maximum extent possible, and any deviations or enhancements to these will be specified in detail.

The following list of capabilities and functional elements are defined and specified:

- Legacy and IP EIs with precedence marking capability
- The ability to complete a higher precedence session to a busy PEI or AEI by interrupting the current session
- ASAC as part of the LSC functions
- EBC (firewall/CE Router)
- Local call control (LSC)
- Session control and signaling (SCS)
- Local and global directories
- User Features and Services (UFS) (voicemail and attendant services)
- Network level call control (MFSS)
- MGC
- MGs
- Media gatekeeper (H.323)
- NM with PBNM

5.3.2.2.2.1 Voice Features and Capabilities

This section describes assured services capabilities and characteristics together with the design and performance metrics associated with each capability or characteristic. For 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 5.3.2.2-1, Assured Services Product Features and Capabilities, summarizes the product features and capabilities.

Table 5.3.2.2-1. Assured Services Product Features and Capabilities

	FEATURE AND CAPABILITY	UCR 2008 SECTION	UCR 2008 GRAPHIC	REFERENCE DOCUMENT
1.	Precedence Call (Session) Waiting **[Required: LSC, MFSS]**	Sections 5.2.2.2.1 through 5.2.2.2.4 Section 5.2.2.1.1 Section 5.2.2.1.4 Section 5.2.2.3 Section 5.2.2.6.2.1 Sections 5.2.2.8.1 through 5.2.2.8.1.4 Section 5.2.2.8.6	Table 5.2.4-5, DSN Information Signals	Telcordia Technologies GR-571-CORE Telcordia Technologies GR-572-CORE
2.	Call (Session) Forwarding **[Required with Conditional sub features: LSC, MFSS]**	Section 5.3.2.2.2.1.1		Telcordia Technologies GR-217-CORE Telcordia Technologies GR-580-CORE Telcordia Technologies GR-586-CORE
3.	Call (Session) Transfer **[Required: LSC, MFSS]**	Section 5.2.2.2 Sections 5.2.2.8.3 through 5.2.2.8.3.2		
4.	Call (Session) Hold **[Required: LSC, MFSS]**	Section 5.2.2.8.4 (inclusive)		
5.	Preset Conferencing **[Objective: LSC, MFSS]**	Section 5.2.2.8.7 (inclusive)		
6.	Three-Way Calling **[Required: LSC, MFSS]**	Section 5.2.2.8.5 (inclusive)		
7.	Release to Pivot **[Objective: LSC, MFSS]**	Section 5.2.1.2.8		
8.	Hotline Service **[Required: LSC, MFSS]**	Sections 5.2.1.12 through 5.2.1.12.4 (inclusive) Sections 5.2.2.4 through 5.2.2.4.3		
9.	Calling Party and Called Party ID (number only) **[Required: LSC, MFSS]**	Section 5.2.3.5.1.8		Telcordia Technologies GR-317-CORE
10	Call Pick-up [Conditional**: LSC, MFSS**]	Section 5.2.1.1.9 (inclusive) Section 5.2.2.8.6		Telcordia Technologies GR-590-CORE

[Required: LSC, MFSS] It is expected that all Assured Services products, such as LSCs and MFSSs, will support vendor-proprietary VVoIP features and capabilities, in addition to supporting the required VVoIP features and capabilities that are listed in Table 5.3.2.2-1, Assured Services Product Features and Capabilities.

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 UCR 2008, Section 5.2, Circuit-Switched Capabilities and Features; this section; and Section 5.3.4, AS-SIP Requirements.

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 2008 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.

5.3.2.2.2.1.1 Call Forwarding

The requirements for VVoIP call forwarding (CF) differ from the TDM requirements for call forwarding. The revised VVoIP CF procedure logic is shown in Figure 5.3.2.2-3, Call Forwarding Logic Diagram. In essence, ROUTINE precedence level calls can be call forwarded (assuming CF activation by the EI or craftsperson) without any consideration of TDM MLPP processing rules or CF feature interactions with TDM MLPP as required for TDM switches. The VVoIP CF requirements now make it a Conditional requirement to implement CF for calls above the ROUTINE precedence level with the TDM MLPP call interaction treatment that is required for TDM switches.

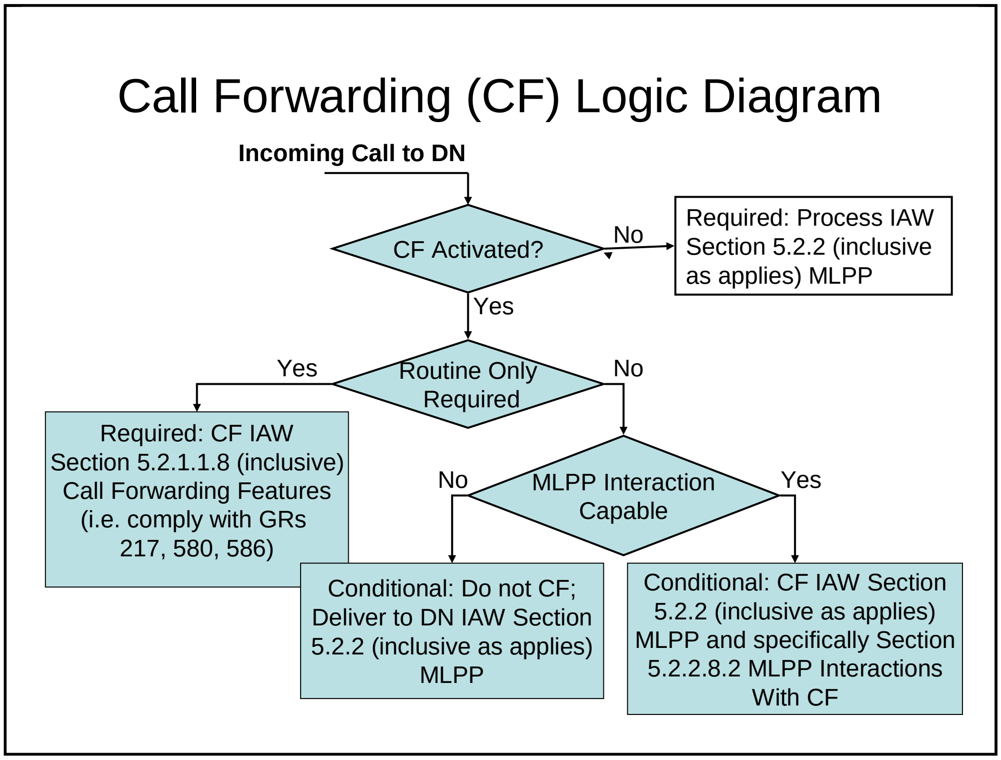

Call Forwarding (CF) Logic Diagram
Incoming Call to DN
CF Activated?
No
Required: Process IAW Section 5.2.2 (inclusive as applies) MLPP
Yes
Routine Only Required
Yes
No
Required: CF IAW Section 5.2.1.1.8 (inclusive) Call Forwarding Features (i.e. comply with GRs 217, 580, 586)
MLPP Interaction Capable
No
Yes
Conditional: Do not CF; Deliver to DN IAW Section 5.2.2 (inclusive as applies) MLPP
Conditional: CF IAW Section 5.2.2 (inclusive as applies) MLPP and specifically Section 5.2.2.8.2 MLPP Interactions With CF

Figure 5.3.2.2-3. Call Forwarding Logic Diagram

Call forwarding implementations (i.e., Call Forwarding Busy (CFB), CF Variable (CFV), CF – Don’t Answer (CFDA), and SCF), as described in UCR 2008 Section 5.2.1.1.8 (inclusive), Call Forwarding Features and Subfeatures, shall provide a new VVoIP-only feature. It will allow ROUTINE precedence calls destined to a DN that has any of the stated CF options, to be completed as a ROUTINE call. Call forwarding implementations (i.e., CFB, CFV, CFDA, and SCF) on switches that do not have TDM MLPP interaction capability shall provide a feature allowing any DSN precedence call above the ROUTINE level, destined to a DN that has any of the stated CF options activated, to be completed to the dialed destination DN, and shall not exercise any CF features. Call forwarding is a line option that could be activated by the switch craftsperson or the subscriber, and the feature shall have the following requirements:

1. **[Required: LSC, MFSS]** Calls to a DN that does not have any CF feature activated shall be delivered to the DN EI IAW the MLPP procedures specified in UCR 2008, Section 5.2.2 Multilevel Precedence and Preemption (inclusive as applies).

2. **[Required: LSC, MFSS]** Call forwarding, when activated on a line DN, shall allow any terminating call at a ROUTINE DSN precedence level, to be completed to the designated destination (IAW the call forward options activated), and shall comply with the requirements as stated in Telcordia Technologies GR-217-CORE, GR-580-CORE, and GR-586-CORE.

3. **[Conditional: LSC, MFSS]** Any switch type that is compliant with Telcordia Technologies GR-217-CORE, GR-580-CORE, and GR-586-CORE, and is not compliant with the stated MLPP interaction requirements for CF, as stated in UCR 2008, Section 5.2.2.8.2, MLPP Interactions with Call Forwarding, shall comply with the following unique MLPP interaction. Call forwarding (any CF feature type), when activated, shall allow any terminating call that is higher than a ROUTINE DSN precedence level, to be completed to the designated destination DN, and shall not be call forwarded. Calls above the ROUTINE DSN precedence level that encounter a busy DN shall exercise the same preemption sequences as stated in UCR 2008, Section 5.2.2 (inclusive as applies), Multilevel Precedence and Preemption.

4. **[Conditional: LSC, MFSS]** Any switch type that is compliant with Telcordia Technologies GR-217-CORE, GR-580-CORE, and GR-586-CORE, and the MLPP interaction requirements for CF, as stated in UCR 2008, Section 5.2.2.8.2, MLPP Interactions with Call Forwarding, shall comply with the following MLPP interaction. Call forwarding (any CF feature type), when activated, shall allow any terminating call that is higher than a ROUTINE DSN precedence level, to be completed in accordance with UCR 2008, Section 5.2.2.8.2, MLPP Interactions with Call Forwarding.

5.3.2.2.2.2 Public Safety Features

5.3.2.2.2.2.1 Basic Emergency Service (911)

[Required: LSC, MFSS] The Basic 911 Emergency Service feature provides a three-digit universal telephone number (911) that gives the public direct access to an emergency service bureau. The emergency service is one way only, terminating to the service bureau. A given local switching system shall serve no more than one emergency service bureau. When the originating line and the emergency service bureau are served by the same switching system, the bureau can hold and disconnect the connection and monitoring the supervisory state, and ringing the originating station back. When the local switching system is in an area with enhanced emergency service (E911) served through a tandem switch, the emergency call is advanced to the tandem switch with calling line Automatic Number Identification (ANI) or Calling Number Delivery (CND).

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

Calling 911 from an LSC or MFSS shall not require the use of access codes such as 99. Dialing 911 only shall connect to the public emergency service bureau. If this feature is provided, it shall be in accordance with Telcordia Technologies GR-529-CORE (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.

Calls to 911 shall be preempted in accordance with assured service priority rules specified in UCR 2008, Section 5.2.2, Multilevel Precedence and Preemption. This is to reinforce the concept that critical military mission requirements take precedence over other uses of the DISN. NOTE: Precedence calls above ROUTINE can and should preempt 911 calls.

5.3.2.2.2.2.2 Tracing of Terminating Calls

[Required: LSC, MFSS] The Tracing of Terminating Calls feature identifies the calling number on intraoffice and interoffice calls terminating to a specified DN. When this feature is activated, the originating DN, the terminating DN, and the time and date are printed out for each call to the specified line.

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

5.3.2.2.2.2.3 Outgoing Call Tracing

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

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

5.3.2.2.2.2.4 Tracing of a Call in Progress

[Required: LSC, MFSS] The Tracing of a Call in Progress feature identifies the originating DN for a call in progress. Authorized personnel entering a request that includes the specific terminating DN involved in the call activate the feature.

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

5.3.2.2.2.2.5 Tandem Call Trace

[Required: LSC, MFSS] The Tandem Call Trace feature identifies the incoming trunk of a tandem call to a specified office DN. The feature is activated by entering the specified distant office DN for a tandem call trace. A printout of the incoming trunk number and terminating DN, and the time and date, is generated for every call to the specified DN.

Requirements for this feature shall be in accordance with Telcordia Technologies GR-529-CORE, FSD 15-03-0000.

5.3.2.2.2.3 ASAC – Open Loop

[Required: LSC, MFSS] This section presents the ASAC requirements for the LSC and the MFSS. In the execution of ASAC, certain procedures need to be followed, such as (a) actions to be taken if a precedence session request cannot be completed because existing sessions are at equal or higher precedence, or (b) tones to be generated when a session is preempted. UCR 2008, Section 5.2.2, Multilevel Precedence and Preemption, addresses these issues. UCR 2008, Section 5.3.4, AS-SIP Requirements, provides a more detailed description of the session control signaling requirements of the LSC and the MFSS.

5.3.2.2.2.3.1 ASAC Requirements for the LSC and MFSS Related to Voice

[Required: LSC, MFSS] One voice session budget unit shall be equivalent to 110 kilobits per second (kbps) of access circuit bandwidth independent of the PEI or AEI codec used. This includes ITU-T Recommendation G.711 encoding rate plus Internet Protocol Version 6 (IPv6) packet overhead plus ASLAN Ethernet overhead. IPv6 overhead, not IPv4 overhead, is used to determine bandwidth equivalents here.

5.3.2.2.2.3.1.1 ASAC Requirements for LSC Related to Voice

5.3.2.2.2.3.1.1.1 LSC States

The states that the LSC must maintain for ASAC purposes are as follows:

1. Line Side States. As a minimum, the LSC shall maintain the session state of each local PEI and AEI in its domain as follows:

    a. Busy/Not Busy. The Busy State includes the session setup phase and the active session phase.

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

c. The Line Side States also apply to multi-appearance EIs, but at this time, no more than two line appearances are dealt with, and the procedures are the same as for ISDN BRI instruments, as specified in UCR 2008, Section 5.2, Circuit-Switched Capabilities and Features.

2. Trunk Side States. The following applies only to the CE Router to WAN access circuit and not to multi-appearance EIs:

a. VoIP Session Budget. If directionalization is not implemented, the LSC and its associated MFSS shall manage the total number of sessions on its IP access link. If directionalization is implemented, the LSC and its associated MFSS shall manage the number of inbound sessions and outbound sessions. An inbound session is one that has been initiated by a PEI or AEI outside the LSC's domain, whereas an outbound session is one that is initiated by a PEI or AEI within the LSC's domain. The LSC and its associated MFSS shall be configurable with the following VoIP budgets:

(1) IPB. The total budget of VoIP sessions plus session attempts in the session setup phase that are allowed on the IP access link.

(2) IPBo. The budget for outbound VoIP sessions plus session attempts in the session setup phase that are allowed on the IP access link.

(a) IPBo may take any value in the range (0, IPB) or "null."
(b) Null implies that there are no outbound directionalization restrictions.

(3) IPBi. The budget for inbound VoIP sessions plus session attempts in the session setup phase that are allowed on the IP access link.

(a) IPBi may take any value in the range (0, IPB) or "null."
(b) Null implies that there are no inbound directionalization restrictions.

(4) Relationship among IPB, IPBo, and IPBi.

(a) IPBi plus IPBo equals IPB, if there is directionalization.
(b) IPBi equals null if, and only if, IPBo equals null.

b. VoIP Session Counts. The LSC and its associated MFSS shall maintain a running session count for the following VoIP sessions:

(1) IPC. The total number of interbase IP sessions in progress plus the number of session attempts in the session setup phase.

(2) IPCo. The number of outbound IP sessions in progress plus the number of outbound session attempts in the session setup phase.

(3) IPCi. The number of inbound IP sessions in progress plus the number of inbound session attempts in the session setup phase.

c. TDM Session Budget. The following session budget is maintained at each LSC, at its associated gateway, and at the corresponding EO/Small End Office (SMEO)/Private Branch Exchange 1 (PBX1)/Private Branch Exchange 2 (PBX2) (NOTE: The LSC and the associated EO/SMEO/PBX1/PBX2 reside on the same B/P/C/S; hence, no directionalization is required for TDM sessions.):

– TDMB. The overall number of TDM sessions plus sessions in the session setup phase on the TDM link. This equals the number of digital signal level 0s (DS0s) on the trunk between the LSC MG and the EO/SMEO/PBX1/PBX2.

d. TDM Session Count. The following session count is maintained at each LSC, at its associated medium gateway, and at the corresponding EO/SMEO/PBX1/PBX2:

– TDMC. The total number of sessions in progress between the TDM switch and the media gateway, plus the total number of session attempts in the session setup phase.

5.3.2.2.2.3.1.1.2 Session Control Processing with No Directionalization

This section considers the functions carried out by the LSC and the MFSS when IPBo equals IPBi equals null.

1. LSC Processing for an Outbound Session.

a. VoIP Session Processing. If IPBo equals IPBi equals null, the LSC will manage the aggregate session count to ensure that IPC does not exceed IPB. If IPBo and IPBi are not null, then the LSC will process the inbound sessions and the outbound sessions individually and independently to ensure that they do not exceed IPBi and IPBo, respectively. This section describes the processing for the case when IPBo equals IPBi equals null. The alternate case is identical to this, except the LSC performs this function on both the inbound and the outbound VoIP sessions.

Actions taken when an outbound session request is initiated by a local PEI or AEI are as follows:

(1) Users and/or PEIs and/or AEIs that place sessions shall be authenticated as per UCR 2008, Section 5.4, Information Assurance Requirement, before processing the outbound session.

(2) If IPC is less than IPB, the session request shall be forwarded to the WAN MFSS for forwarding to the sessioned LSC for processing (see item 2, LSC Processing for an Inbound Session).

(3) If IPC equals IPB and all existing sessions are at precedence equal to or greater than the new session request, then the LSC shall not place the session, and the caller shall receive a BPA. If it is a ROUTINE call, the caller shall receive a Fast Busy Announcement as per UCR 2008, Section 5.2.2.1.3, Announcements.

(4) If IPC equals IPB and at least one existing session is of lower precedence than the new session, the LSC shall preempt one of the lowest precedence sessions and shall forward the session INVITE (via the MFSS) to the sessioned LSC for processing. The algorithm for selecting the session to preempt shall be deterministic.

(5) IPC is greater than IPB is not an allowed state. If this occurs, the LSC shall deterministically preempt sessions starting with those of lowest precedence until IPC equals IPB, and then proceed as specified in items (3) and (4) previously. The LSC shall notify the NMS of this fault state.

(6) The LSC shall increment and decrement its IPC as follows:

(a) The LSC increments its IPC upon forwarding a session request to the MFSS, which it received from its local PEI or AEI.

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

2. LSC Processing for an Inbound Session. Actions taken by the LSC when a new inbound session INVITE is received from a remote LSC are as follows:

a. If IPC is less than IPB and the local PEI or AEI is not busy, then the LSC shall place the session.

b. 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 LSC shall preempt the existing session and place the new session.

c. If 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, the new session is not placed. The caller shall receive a BPA, and if it is a ROUTINE call, the caller shall receive a Fast Busy Announcement as per UCR 2008, Section 5.2.2.1.3, Announcements.

d. If IPC equals IPB and the local 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 LSC shall not place the new session. The caller shall receive a BPA, and if it is a ROUTINE call, the caller shall receive a Fast Busy Announcement as per UCR 2008, Section 5.2.2.1.3, Announcements.

e. 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 LSC shall deterministically preempt one of the lowest precedence sessions. Then it shall forward the session INVITE to the sessioned LSC via the MFSS for processing.

f. 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 LSC shall preempt the session and forward the session INVITE to the local PEI or AEI.

g. 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 LSC shall not place the session. The caller shall receive a BPA, and if it is a ROUTINE call, the caller shall receive a Fast Busy Announcement as per UCR 2008, Section 5.2.2.1.3, Announcements.

h. The IPC is greater than IPB is not an allowed state. If this occurs, the LSC shall deterministically preempt sessions starting with those of the lowest precedence level until IPC equals IPB, and then proceed as specified in items d, e, f, and g. The LSC shall notify the NMS of this fault state.

3. Incrementing and Decrementing the Session Count. The LSC shall increment and decrement its IPC as specified in UCR 2008, Section 5.3.4, AS-SIP Requirements.

4. LSC 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.

a. If the sessioned PEI or AEI is not busy, the LSC shall complete the session.

b. If the sessioned PEI or AEI is busy with a session that is of a lower precedence level than the new session, the LSC shall preempt the session, and then complete the new session.

c. If the call attempt is at a precedence level above ROUTINE and the local PEI or AEI is busy with a session that is equal to or higher than precedence level the new session, the LSC shall not complete it. The caller shall receive a BPA. If the call attempt is a ROUTINE call and the local PEI or AEI is busy with a session, the caller shall receive a Slow Busy tone as per UCR 2008, Section 5.2.4.5.1, Ringing.

d. The LSC does not modify its IPC when local sessions are connected or disconnected because they do not affect traffic in the access link to the WAN.

e. **[Conditional]** An intrabase session count shall be maintained separately, independent of precedence, and when this valve is reached no more ROUTINE precedence level session requests shall be processed for intrabase connection. PRIORITY, IMMEDIATE, FLASH, and FLASH OVERRIDE session requests shall be processed as specified in items a, b, and c.

5.3.2.2.2.3.1.1.3 LSC Session Control Processing with Directionalization

The LSC directionalization requirements are applicable to VoIP sessions transmitted over an IP access link. They are not applicable to TDM sessions because they are transmitted via a local EO/SMEO/PBX1/PBX2. Any directionalization for these sessions will be implemented by the EO/SMEO/PBX1/PBX2.

When IPBo and IPBi are not null, the LSC will keep a running count of IPCo and IPCi to 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.

5.3.2.2.2.3.1.2 ASAC Requirements for the MFSS Related to Voice

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

1. <u>MFSS States</u>. The MFSS shall be configurable with the IPB, IPBi, and IPBo budget parameters for each LSC in its domain.

2. MFSS Session Counts. The MFSS shall maintain a running count of IPC, IPCo, and IPCi for each LSC in its domain. It shall do this by monitoring the AS-SIP messages associated with each of its subordinate LSCs as specified in UCR 2008, Section 5.3.4, AS-SIP Requirements.

3. MFSS Session Processing with no Directionalization. Initially, the IPC for each LSC is set to zero. The MFSS shall increment and decrement the IPC as follows:

   a. For outbound sessions:

      (1) After having received a session request (i.e., INVITE) from its local LSC, the MFSS increments the corresponding IPC upon forwarding that session request to the far-end LSC.

      (2) The MFSS decrements its IPC when it determines that a session request is completely terminated or an established session is completely terminated.

   b. For inbound sessions:

      (1) The MFSS increments its IPC upon transmitting to the far-end LSC a "session accepted" (i.e., 1XX or 2XX) response to an INVITE request that it received from the far-end LSC. (The IPC is not incremented for INVITE requests.)

      (2) The LSC decrements its IPC when it determines that a session request is completely terminated or an established session is completely terminated.

4. MFSS Policing. The MFSS shall police each LSC in its domain to ensure that the IPC does not exceed IPB.

   a. If IPC equals IPB, and an LSC attempts to place another session by forwarding a session INVITE to its MFSS, the MFSS shall not forward the session INVITE and shall send an error message to the NMS. The caller shall receive a busy announcement as per UCR 2008, Section 5.2.2.1.3, Announcements.

   b. If IPC equals IPB at an LSC_a, and its $MFSS_a$ receives a session INVITE intended for LSC_a from another LSC_b or another $MFSS_b$, the $MFSS_a$ shall forward the session INVITE to LSC_a. If LSC_a accepts the session (without preempting another session so that IPC would be greater than IPB), the $MFSS_a$ shall not forward the "session accepted" to the sessioning LSC, and shall send an error message to the NMS. The caller shall receive a busy announcement as per UCR 2008, Section 5.2.2.1.3, Announcements.

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

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

5. MFSS Session Processing with Directionalization. When directionalization is applied, the MFSS 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 both are identical to that carried out for IPC in the no-directionalization case.

5.3.2.2.2.3.2 ASAC Requirements for the LSC and the MFSS Related to Video Services

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

Since the bandwidth of a video session can vary, video sessions will be budgeted in terms of Video Session Units (VSUs). One VSU equals 500 kbps, and bandwidth for video sessions will be allocated in multiples of VSUs. For example, the bandwidth allocated to video sessions may be 500 kbps, 1000 kbps, 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.

1. VSU Budgets. The LSC and its corresponding MFSS shall be configurable with the following budgets:

   - VDB. The total number of inbound and outbound VSUs plus the in-progress VSU connection attempts that an LSC is allowed to have over the IP access link.

Video and voice will each be allocated adequate bandwidth to support its traffic-engineered budgets. Since each of these two services is allocated its own bandwidth, preemption of low-precedence video sessions by high-precedence voice sessions (and vice versa) will not be necessary and will not be implemented. Voice sessions will strictly preempt within their allocated bandwidth, and video sessions likewise.

The LSC processing requirements of video sessions will be similar to its processing of VoIP sessions. For the no-directionalization case (i.e., VDBi equals VDBo equals null), the LSC shall manage VDC to ensure that it does not exceed VDB. For the directionalization case where

VDBi and VDBo are not null, the LSC will manage VDCo and VDCi independently to ensure that neither one exceeds its corresponding budget. The preemption rules for video sessions are the same as for voice sessions as specified in UCR 2008, Section 5.2.2, Multilevel Precedence and Preemption. However, some extensions to the rules are required to take into account that video sessions can be of different budgets (i.e., 1, 2, 5, or 8 budgets corresponding to 500 kbps, 1000 kbps, 2500 kbps, and 4000 kbps, respectively). The following rule extensions apply to a video session request of 1, 2, 5, or 8 budgets:

1. Preempt sessions in the process of signaling setup (progress) before preempting active sessions.

2. Preempt the minimum number of sessions to accumulate the number of budgets needed to satisfy the video session request.

3. Accumulate the needed number of budgets by preempting all sessions of a lower precedence level (starting at the ROUTINE level) before proceeding to preempt from sessions of the next higher precedence level for the remaining required budgets.

4. When the number of sessions selected for preemption result is more budgets (excess) than are required to satisfy the video session request, return the excess budgets to the ASAC pool.

The MFSS processing requirements of video sessions will be similar to its processing of VoIP sessions. For the no-directionalization case (i.e., VDBi equals VDBo equals null), the MFSS shall police by blocking to ensure that the respective budgets are not exceeded: VDC to ensure that it does not exceed VDB.

[Required: MFSS] If necessary, the MFSS will preempt for a session request that is at precedence level FLASH OVERRIDE or FLASH and the counts equal the budgets.

5.3.2.2.3 Signaling Protocols

[Required: PEI, LSC, MFSS] The control/management protocol between the PEI and the LSC is, in general, proprietary.

[Required: AEI, LSC, MFSS] The control/management protocol between the AEI and the LSC is AS-SIP as specified in Section 5.3.4, AS-SIP Requirements, of this document.

[Required: LSC, MFSS] The signaling protocol used on UC IP trunks is AS-SIP as specified in Section 5.3.4, AS-SIP Requirements, of this document.

[Required: MFSS] The TDM-side of an MFSS uses DSN CCS7 signaling (see UCR 2008, Section 5.2.2.9.1, General Description) on CCS7-like trunks.

[Required: LSC, MG within the MFSS] The LSC and the MG within the MFSS use DSN T1-619a PRI signaling on DSN PRI trunks.

[Conditional: LSC, MG within the MFSS] The LSC and the MG within the MFSS use CAS signaling on CAS trunks.

5.3.2.2.4 Signaling Performance

Call setup times should adhere to the following guidelines:

1. **[Conditional: Intra-Enclave Calls]** 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.

2. **[Conditional: Inter-Enclave Calls]** For inter-enclave and worldwide calls within the IP environment, average delay should not exceed 6 seconds, with 95 percent of calls not to exceed 8 seconds during normal traffic conditions.

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

1. **[Conditional: Intra-Enclave Calls]** 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.

2. **[Conditional: Inter-Enclave Calls]** 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.

5.3.2.3 Registration, Authentication, and Failover

5.3.2.3.1 Registration and Authentication

[Required: LSC, MFSS] Registration and authentication between NEs shall follow the requirements set forth in UCR 2008, Section 5.4, Information Assurance Requirements.

5.3.2.3.2 LSC and MFSS Failover Requirements

[Required: LSC, MFSS, EBC] The LSCs shall be registered to a primary and backup MFSS. In case of failure of the primary MFSS, the LSC will default to the backup MFSS.

5.3.2.3.2.1 General Description

The MFSS (SSs) will be deployed as active-active pairs, whereby one MFSS will act as the primary SS for one set of LSCs (set A) and as the secondary SS for another set of LSCs (set B). Similarly, the other MFSS will act as primary for the set B LSCs and secondary for the set A LSCs. LSCs shall be assigned to a primary and a secondary (backup) MFSS during network configuration. In case of the loss of connectivity (either a transport or MFSS failure) to the primary MFSS, the LSC in conjunction with its EBC will default to sending the AS-SIP signaling messages to the secondary MFSS. Sessions (calls) that were established with the primary MFSS will remain in progress until SIP keep-alive timers expire and the sessions are closed by the LSC. If desired, the caller can redial the DN and re-establish the session through the secondary MFSS. Each MFSS (SS part) in the network will know each pair of SSs that act as backups for each other. This will be done by operations personnel during MFSS configuration.

The failover detection mechanism will be accomplished by using a periodic AS-SIP OPTIONS request between each LSC and its primary and secondary MFSSs, and between each MFSS network pair. Through this, an LSC can learn when its primary MFSS has failed and later relay AS-SIP messages to the secondary MFSS, and an MFSS can learn when any other MFSS has failed and later relay AS-SIP messages to the secondary MFSS for delivery to the LSC. When an SS receives an OPTIONS request from an LSC or another MFSS, it responds with a 200 OK response. Consequently, through the periodic “pinging” of all network signaling appliances using the AS-SIP OPTIONS request and 200 OK responses, each signaling appliance learns its neighbors’ operational status and can route around the failure of any individual signaling appliance. The specific LSC, MFSS, and EBC failover requirements are discussed in the following subsections.

5.3.2.3.2.2 LSC Monitors Primary MFSS (SS) for Status

[Required] The LSC shall send an OPTIONS request with a Request-URI identifying the primary SS (the Request-URI does not have a userinfo part) on a configurable periodic time interval (default equals 45 seconds; minimum time interval equals 35 seconds).

[Required] When a properly functioning primary SS receives the OPTIONS request from a served LSC, the primary SS shall respond with a 200 OK response that includes the Accept header and the Supported header.

[Required] The OPTIONS requests sent by the LSC include a route set comprised of two Route Headers, where the first Route Header is the SIP Universal Resource Identifier (URI) for the EBC at the enclave, and the second Route Header is the SIP URI for the EBC serving the primary SS.

[Required] Whenever the LSC sends an INVITE request to its EBC and receives a 408 (Request Time-Out), 503 (Service Unavailable), or 504 (Server Time-Out) response and the LSC is not already awaiting a response to a pending OPTIONS request, then the LSC shall send an OPTIONS request immediately with a Request-URI identifying the primary SS (the Request-URI does not have a userinfo part).

[Required] The LSC shall be capable of sending OPTIONS requests to the primary SS, or to both the primary and secondary SS via a configuration setting.

5.3.2.3.2.3 LSC Failover to Secondary MFSS (SS)

[Required] When the LSC sends a defined configurable number of successive OPTIONS requests (default equals 2) for which there either is no response or the response is a 408 (Request Time-Out), 503 (Service Unavailable), or 504 (Server Time-Out) response, then:

1. **[Required]** All new outbound SIP messages (with the exception of OPTIONS requests destined for the primary SS) are sent to the secondary SS. The OPTIONS requests generated by the LSC continue to be sent to the primary SS.

2. **[Required]** All outbound SIP requests sent by the LSC to its EBC (with the exception of OPTIONS requests) shall include a route set comprised of two Route Headers, where the first Route Header is the SIP URI for the EBC at the enclave, and the second Route Header is the SIP URI for the EBC serving the secondary SS.

3. **[Required]** Upon failover from the primary SS to the secondary SS, the EBC serving the secondary SS shall respond with a 481 (Call/Transaction Does Not Exist) response upon receipt of any Re-INVITE, UPDATE, or BYE request on behalf of an existing call that had been established through the primary SS.

[Required] If the LSC receives a 200 OK response to an OPTIONS request from the primary SS before the configurable number of successive failures to the OPTIONS requests (default equals 2) has been reached, then no action is taken to failover to the secondary SS. For example, using the default of two successive failures, if one OPTIONS request to the primary SS fails, then if the next OPTIONS request receives a 200 OK response, no action is taken to fail over to the secondary SS.

5.3.2.3.2.4 LSC Failback to Primary MFSS (SS)

[Required] Upon failover, the LSC will send OPTIONS requests to the primary SS at a failback configurable periodic time interval (default equals 60 seconds; minimum time interval equals 35 seconds).

[Required] The OPTIONS requests sent by the LSC shall include a route set comprised of two Route Headers, where the first Route Header is the SIP URI for the EBC at the enclave, and the second Route Header is the SIP URI for the EBC serving the primary SS.

[Required] When the LSC receives a 200 OK response to an OPTIONS request from the primary SS, the LSC shall send the INVITE requests corresponding to new call requests to the primary SS. The LSC shall continue to send SIP messages pertaining to existing calls that were established through the secondary SS to the secondary SS until those calls terminate normally.

[Required] When the LSC sends INVITE requests (as well as the subsequent SIP requests) for new call requests, the INVITE requests (and the subsequent SIP requests) shall include a route set comprised of two Route Headers, where the first Route Header is the SIP URI for the EBC at the enclave, and the second Route Header is the SIP URI for the EBC serving the primary SS.

[Required] Upon failback, the LSC returns to the original configurable periodic time interval (default equals 45 seconds; minimum time interval equals 35 seconds)for sending OPTIONS requests to the primary SS.

5.3.2.3.2.5 MFSS (SS) Monitors the Other MFSSs (SSs) in the Network

[Required] Each SS shall send an OPTIONS request to every other SS on a "standard" configurable periodic time interval (default equals 45 seconds; minimum time interval equals 35 seconds). In each OPTIONS request, the Request-URI identifies the destination SS (the Request-URI does not have a userinfo part). The OPTIONS requests shall include a route set comprised of two Route Headers, where the first Route Header is the SIP URI for the EBC of the SS originating the OPTIONS request, and the second Route Header is the SIP URI for the EBC serving the destination SS.

[Required] Whenever an originating SS sends an INVITE request to another SS and receives either a 408 (Request Time-Out), 503 (Service Unavailable), or 504 (Server Time-Out) response and the originating SS is not already awaiting a response to a pending OPTIONS request to the other SS, then the originating SS shall send an OPTIONS request with a Request-URI identifying the SS. The OPTIONS request shall include a route set comprised of two Route Headers, where the first Route Header is the SIP URI for the EBC of the SS originating the OPTIONS request, and the second Route Header is the SIP URI for the EBC serving the destination SS.

[Required] When a properly functioning SS receives the OPTIONS request, the SS shall respond with a 200 OK response that includes the Accept header and the Supported header.

5.3.2.3.2.6 MFSS Failover to Secondary MFSS (SS)

[Required] Each MFSS (SS) shall be configured with knowledge of each pair of SSs that act as backups for each other.

[Required] When the originating SS sends a defined configurable number of successive OPTIONS requests (default equals 2) to another SS (that is NOT its own paired secondary SS) for which there is either no response or the response is either a 408 (Request Time-Out), 503 (Service Unavailable), or 504 (Server Time-Out) response, then:

1. **[Required]** The originating SS sends all new SIP messages intended for the failed SS (with the exception of OPTIONS requests that it generates for the failed SS) to the paired secondary SS for the failed SS. The SIP requests shall include a route set comprised of two Route Headers, where the first Route Header is the SIP URI for the EBC at the originating SS, and the second Route Header is the SIP URI for the EBC serving the paired secondary SS for the failed SS. The originating SS will continue to send OPTIONS requests to the failed SS whereby the OPTIONS requests include a route set comprised of two Route Headers, where the first Route Header is the SIP URI for the originating SS, and the second Route Header is the SIP URI for the EBC serving the failed SS.

2. **[Required]** Upon failover from the primary SS to the secondary SS, the EBC serving the secondary SS shall respond with a 481 (Call/Transaction Does Not Exist) response upon receipt of any Re-INVITE, UPDATE, or BYE request received on behalf of an existing call that had been established through the primary SS.

[Required] If the originating SS receives a 200 OK response to an OPTIONS request from its paired SS or another SS before the configurable number of successive failures to the OPTIONS requests (default equals 2) has been reached, then no action is taken to fail over to the paired SS. For example, using the default of two successive failures, if one OPTIONS request to the other SS fails, then the next OPTIONS request receives a 200 OK response, no action is taken to fail over to the paired SS.

[Required] When the originating SS sends a defined configurable number of successive OPTIONS requests (default equals 2) to its own paired SS for which there either is no response or the response is either a 408 (Request Time-Out), 503 (Service Unavailable), or 504 (Server Time-Out) response, then:

1. **[Required]** The SS sends all new SIP messages intended for its paired SS (with the exception of OPTIONS requests it generates for its failed paired SS) directly to the LSCs served by its paired SS. The SIP requests shall include a route set comprised of two Route Headers, where the first Route Header is the SIP URI for its own EBC, and the second Route Header is the SIP URI for the EBC for the intended LSC. The SS will continue to

send OPTIONS messages to its failed paired SS whereby the OPTIONS messages include a route set comprised of two Route Headers, where the first Route Header is the SIP URI for its own EBC, and the second Route Header is the SIP URI for its failed paired SS.

2. **[Required]** Upon failover of its paired SS, the EBC serving the operational SS shall respond with a 481 (Call/Transaction Does Not Exist) response upon receipt of any Re-INVITE, UPDATE, or BYE request received on behalf of an existing call that had been established through its paired SS.

5.3.2.3.2.7 MFSS Failback to Original MFSS (SS)

[Required] Upon failover, the SS will send OPTIONS requests to the failed SS at a "failback" configurable periodic time interval (default equals 60 seconds; minimum time interval equals 35 seconds). The OPTIONS requests shall include a route set comprised of two Route Headers, where the first Route Header is the SIP URI for the EBC of the originating SS, and the second Route Header is the SIP URI for the EBC serving the failed SS.

[Required] When the SS receives a 200 OK response to an OPTIONS request from a failed SS (that is NOT its paired SS), then the SS shall send to the newly recovered SS the INVITE requests corresponding to new call requests intended for LSCs where their primary SS is supposed to be the newly recovered SS. The new INVITE requests shall include a route set comprised of two Route Headers, where the first Route Header is the SIP URI for the originating SS, and the second Route Header is the SIP URI for the EBC serving the newly recovered SS.

[Required] The SS will continue to send SIP messages pertaining to existing calls that were established through the secondary SS to the secondary SS until those calls terminate normally.

[Required] When the SS receives a 200 OK response to an OPTIONS request from its paired SS, then the SS shall send its newly recovered paired SS the INVITE requests corresponding to new call requests intended for LSCs where their primary SS is supposed to be the newly recovered paired SS. The new INVITE requests shall include a route set comprised of two Route Headers, where the first Route Header is the SIP URI for the originating SS, and the second Route Header is the SIP URI for the EBC serving its newly recovered paired SS.

[Required] The SS will continue to send SIP messages pertaining to existing calls that were established through itself to its served secondary LSCs until the calls terminate normally.

[Required] Upon failback, the SS returns to the original configurable periodic time interval (default equals 45 seconds; minimum time interval equals 35 seconds) for sending OPTIONS requests to the newly recovered SS.

5.3.2.4 Product Interface Requirements

5.3.2.4.1 Internal Interface Requirements

[Required: PEI, AEI, LSC (including the MG, SG, and Media Server), MFSS, EBC, and CE Router] Internal interfaces are functions that operate internal to a System Under Test (SUT) or UC approved product (e.g., LSC, MFSS). The interfaces between SCS functions within an LSC, e.g., between the Call Admission Control (CAC), IWF, MGC, MG, and SG, are considered internal to the LSC regardless of the physical packaging. These interfaces are vendor proprietary and unique, especially the protocol used over the interface. Whenever the physical interfaces use Institute of Electrical and Electronics Engineers, Inc. (IEEE) 802.3 Ethernet standards, they shall support auto-negotiation even when the IEEE 802.3 standard has it as optional. This applies to 10/100/1000-T Ethernet standards; i.e., IEEE, Ethernet Standard 802.3, 1993; or IEEE, Fast Ethernet Standard 802.3u, 1995; and IEEE, Gigabit Ethernet Standard 802.3ab, 1999.

5.3.2.4.2 External Physical Interfaces between Network Components

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

[Required: LSC, MFSS, EBC, CE Router, ASLAN, PEI, AEI] The physical interfaces between an LSC (and its appliances), the EBC, the ASLAN switches/routers, and the CE Router shall be a 10/100/1000-T Mbps Ethernet interface. 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.

5.3.2.4.3 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).

5.3.2.4.3.1 Deployable Networks Interface Requirements

[Conditional] The Deployable interface requirements are specified in Section 6.1, Deployable Requirements; Section 5.3.3, Wide Area Network Requirements; and Section 7, Requirements Matrix.

5.3.2.4.3.2 DISN Teleport Site Interface Requirements

[Required] The Assured Services subsystem shall interface the Teleport sites on both a TDM basis and an IP basis. A T1.619a MG with PRI signaling will be used for T1 trunks to the Teleport sites. If the Teleport site contains an LSC, then the interface will be via the DISN WAN for both the media and signaling, with the signaling being AS-SIP (Section 5.3.4, AS-SIP Requirements) between the Teleport LSC and the UC MFSS.

5.3.2.4.3.3 PSTN Interface Requirements

[Required] The Assured Services subsystem shall interface with the PSTN and host-nation PTTs via the SG or MG interfaces as specified in Section 5.3.2.12, Media Gateway Requirements, and Section 5.3.2.13, Signaling Gateway Requirements.

5.3.2.4.3.4 Allied and Coalition Network Interface Requirements

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

5.3.2.4.4 VVoIP NMS Interface Requirements

[Required] The physical interface between the DISA VVoIP EMS and the network components (i.e., LSC, MFSS, EBC, CE Router) is a 10/100-Mbps Ethernet interface. The interface will work in either of the two following modes using auto-negotiation: IEEE, Ethernet Standard 802.3, 1993; or IEEE, Fast Ethernet Standard 802.3u, 1995.

Local management traffic and VVoIP EMS management traffic are required to 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. The failover from the primary to the secondary interface shall comply with the specifications in Section 5.3.1.7.7.2., 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. If signaling and bearer traffic shares a physical Ethernet interface with local or VVoIP EMS management traffic, then the signaling and bearer traffic must use a separate VLAN.

5.3.2.5 Product Physical, Quality, and Environmental Factors

5.3.2.5.1 Physical Characteristics

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

5.3.2.5.2 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.

5.3.2.5.2.1 Product Availability

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

1. <u>Dual Power Supplies</u>. The platform shall provide a minimum of two power supplies, each with a power capacity to support the entire chassis’s electrical load.

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

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

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

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

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

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

8. Backup Power Uninterruptible Power Supply (UPS) Requirements. The components that comprise the subsystem for Special C2 users FO/F users and I/P users and R users shall meet the appropriate UCR 2008, Section 5.2.11.3, Backup Power, switch type backup power UPS requirements (e.g., 8 hours for an MFSS and LSC) for all devices including the 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 LSC or MFSS. Backup power is only required for as many hours as it will take the base to switch over to backup generator power, but the total combination of backup times shall not be less than 8 hours.

9. No Loss of Active Sessions. In the event of component failure in the subsystem, all active sessions shall not be disrupted (namely, the loss of existing connection requiring redialing), and the path through the network shall be restored within 5 seconds. All devices used to implement redundancy shall be capable of handling the entire session processing load in the event that its counterpart device fails.

5.3.2.5.2.2 Maximum Downtimes

[Required: LSC, MFSS, ASLAN] The performance parameters associated with the ASLAN, MFSS, and LSC, when combined, shall meet the following maximum downtime requirements:

- IP (10/100 Ethernet) network links – 35 minutes/year
- IP subscriber – 12 minutes/year

5.3.2.5.3 Environmental Conditions

[Required] Environmental conditions requirements are contained in Telcordia Technologies GR-63-CORE. This document identifies the minimum generic spatial and environmental criteria for all new telecommunications equipment systems used in a telecommunications network. Included with these equipment systems are associated cable distribution systems, distributing and interconnecting frames, power equipment, operations support systems, and cable entrance facilities. The detailed specifications of this section are those of best commercial practice and will be specified by the acquiring DoD organization.

5.3.2.5.4 Loss of Packets

[Required: PEI, AEI, IAD, ATA, MG] For these VoIP devices, the voice quality shall have a MOS of 4.0 (R-Factor equals 80) or better, as measured in accordance with 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 only applies to devices that generate media and have a Network Interface Card (NIC).

5.3.2.6 End Instruments

The IP voice and IP video EIs are addressed in this section. Legacy voice and video EIs, secure and nonsecure, are addressed in UCR 2008, Section 5.2, Circuit-Switched Capabilities and Features. Data/PC EIs will not be addressed in this section. Secure IP EIs are addressed in, Section 5.2.12.6, DoD Secure Communications Devices, and UCR 2008, Section 6.2, Unique Classified Requirements. Softphones are addressed in UCR 2008, Section 5.2.12.8.3, Softphones, when used with circuit switches. Softphones and collaboration will be addressed in future versions of this document when softphones and softvideophones are added to the STIGs.

5.3.2.6.1 Voice Instrument

Voice instruments are considered associated with the LSC and must have been designed in conjunction with the LSC design. An IP voice instrument shall be designed in accordance with the acquiring activity requirements, but the following capabilities are specifically required as indicated:

- **[Objective]** DoD Common Access Card (CAC) reader
- **[Required]** Display calling number
- **[Required]** Display precedence level of the session
- **[Required]** Support for Dynamic Host Configuration Protocol (DHCP).

[Required] For multiple line appearance, only two-appearance IP voice instruments are specified and they shall function as specified in UCR 2008, Section 5.2.2.6, ISDN MLPP BRI.

5.3.2.6.1.1 Tones and Announcements

[Required: PEI, AEI, LSC, MFSS, SS] Tones and announcements, as required in UCR 2008, Sections 5.2.4.5.2, DSN Information Signals, and Section 5.2.2.1.3, Announcements, shall be supported, except for the loss of C2 announcement. These tones and announcements may be generated locally by the PEI or AEI upon command of the LSC, or be generated upon command of the LSC by an internal LSC 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 LSC SUT.

[Conditional: PEI, AEI, LSC, MFSS, SS] The required conditions for playing the loss of C2 announcement have been changed from those contained in UCR 2008, Section 5.2.2.1.3, Announcements. They only apply to calls via an LSC MG or an SS MG to a non-MLPP PRI or CAS trunk. The required conditions are as follows:

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

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

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

4. Play before ringback is provided to the caller.

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

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

7. The loss of C2 announcement is not signaled by AS-SIP.

5.3.2.6.1.2 Audio Codecs

[Required: PEI, AEI, LSC-MG, MFSS] The product shall support the origination and termination of a voice session using the following codecs:

- ITU-T Recommendation G.711, to include both the μ-law and A-law algorithms

- ITU-T Recommendation G.723.1
- ITU-T Recommendation G.729 or G.729A
- ITU-T Recommendation G.722.1

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

5.3.2.6.1.3 VoIP PEI or AEI Telephone Audio Performance Requirements

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

5.3.2.6.1.4 Voice over IP Sampling Standard

[Required] 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).

As an example, for a Fixed-to-Fixed call using the G.711 codec, the 64-kbps codec rate multiplied by the 20-ms sample length equals 1280 bits, or 160 bytes of voice payload packet size (where payload does not include SRTP, UDP, and IP packet header fields). This results in a packet-per-second rate (where “packet” means payload packet) of one packet every 20 ms equals 50 packets per second (PPS).

For a Deployable-to-Fixed call, the Navy may use the G.729 (8-kbps) codec to minimize the bandwidth required on a ship-to-shore satellite link, and may use a 50-ms voice sample length. This results in an 8-kbps codec rate multiplied by a 50-ms sample length equals 400 bits, or 50 bytes of voice packet payload size. This results in a PPS rate of one payload packet every 50 ms equals 20 PPS.

5.3.2.6.1.5 Authentication to LSC

[Required: PEI, AEI, LSC, MFSS] The PEI or AEI shall be capable of authenticating itself to its associated LSC and vice versa in accordance with UCR 2008, Section 5.4, Information Assurance Requirements.

5.3.2.6.1.6 Analog Telephone Support

Analog instruments, including secure analog EIs, analog facsimile EIs, and analog modem EIs, shall be supported by the LSC either by a TA or an Integrated Access Device (IAD) connected to an Ethernet port.

[Required: TA, LSC, MFSS] Terminal Adapter (RJ-11 POTS) telephone to RJ-45 Ethernet interface). The TA shall support G.711 standards.

[Conditional: TA, LSC, MFSS] Terminal Adapter (RJ-11 POTS telephone to RJ-45 Ethernet interface). The TA shall support V.150.1 Modem Relay and T.38 Fax Relay standards

[Required: IAD, LSC, MFSS] Integrated Access Device (4–16 ports of RJ-11 POTS telephone to one port of RJ-45 Ethernet interface). The IAD shall support G.711 standards.

[Conditional: IAD, LSC, MFSS] Integrated Access Device (4–16 ports of RJ-11 POTS telephone to one port of RJ-45 Ethernet interface). The IAD shall support V.150.1 Modem Relay and T.38 Fax Relay standards

[Conditional: IAD, LSC, MFSS] Integrated Access Device (17 or more ports of RJ-11 POTS telephone to one port of RJ-45 Ethernet interface). The IAD shall support G.711 standards.

[Conditional: IAD, LSC, MFSS] Integrated Access Device (17 or more ports of RJ-11 POTS telephone to one port of RJ-45 Ethernet interface). The IAD shall support V.150.1 Modem Relay and T.38 Fax Relay standards

[Required: EI, TA, IAD, LSC, MFSS] Analog telephones, when combined with a TA or IAD, together shall comply with TIA-810-B, November 3, 2006.

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 LSC MG.

[Required: MG Line Card, LSC, MFSS] The line card shall support G.711 standards.

[Conditional: MG Line Card, LSC, MFSS] The line card shall support V.150.1 Modem Relay and T.38 Fax Relay standards.

[Required: EI, MG Line Card, LSC, MFSS] 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.

[Conditional: LSC, MFSS] The LSC and MFSS 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. However, every analog TA, IAD, and MG line card on the LSC or MFSS is not required to support secure analog EIs, and is not required to support ITU–T Recommendation V.150.1 Modem Relay.

[Conditional: LSC, MFSS] The LSC and MFSS 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 .38 standard for Fax Relay. However, every analog TA, IAD, and MG line card on the LSC or MFSS is not required to support analog facsimile EIs, and is not required to support ITU-T Recommendation .38 Fax Relay.

[Conditional: LSC, MFSS] The LSC and MFSS 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. However, every analog TA, IAD, and MG line card on the LSC or MFSS is not required to support analog modem EIs, and is not required to support ITU-T Recommendation V.150.1 Modem Relay.

5.3.2.6.1.7 Softphones

[Conditional: PEI, AEI, LSC, MFSS] 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.

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 UCR 2008 requirements:

- Section 5.3.2.2.2.1, Voice Features and Capabilities

- Section 5.3.2.5.2.1, System Availability (NOTE: The softphone application shall be exempt from these requirements.)

- Section 5.3.2.6.1, Voice Instrument

- Section 5.3.2.6.1.1, Tones and Announcements
- Section 5.3.2.6.1.2, Audio Codecs
- Section 5.3.2.6.1.3, Handset Loudness and Frequency Response Requirement VoIP PEI or AEI Telephone Audio Performance Requirements
- Section 5.3.2.6.1.4, Voice over IP Sampling Standard
- Section 5.3.2.6.1.5, Authentication to LSC
- Section 5.3.2.6.3, End Instrument to ASLAN Interface
- Section 5.3.3, Network Infrastructure End-to-End Performance Requirements

  The softphone application shall be exempt from the performance (i.e., packet loss, jitter, latency) requirements specified in Section 5.3.3, Network Infrastructure End-to-End Performance Requirements, e.g., the PEI/AEI 50-ms codec latency and the 20-ms de-jitter buffer latency.
- Section 5.3.3.3.2, VVoIP Differentiated Services Code Point
- Section 5.4, Information Assurance Requirements

5.3.2.6.1.8 ISDN BRI Telephone Support

[Conditional: LSC] The ISDN BRI EIs, including secure ISDN BRI EIs, shall be supported by the LSC. The ISDN BRI EI shall be supported either

- By a BRI-capable TA or a BRI-capable IAD that is connected to an Ethernet port, or
- By the existing twisted-pair cable plant connected to a BRI-capable line card that is part of the LSC MG.

[Conditional: LSC, TA] The LSC shall support BRI-capable TAs that support standard (nonsecure) ISDN BRI EIs. These BRI-capable TAs shall support the ITU-T Recommendation G.711 standard. Also, each BRI-capable TA shall support one port with an RJ-11 BRI interface, one port with an RJ-45 BRI interface, and one port with an RJ-45 Ethernet interface.

[Conditional: LSC, IAD] The LSC shall support BRI-capable IADs that support standard (nonsecure) ISDN BRI EIs. These BRI-capable IADs shall support the ITU-T Recommendation

G.711 standard. Also, each BRI-capable IAD shall support from 4–16 ports with RJ-11 BRI interfaces, from 4–16 ports with RJ-45 BRI interfaces, and one port with an RJ-45 Ethernet interface.

[Conditional: LSC, TA] The LSC shall support BRI-capable TAs that support secure ISDN BRI EIs. These BRI-capable TAs shall support both the ITU-T Recommendations G.711 and V.150.1 standards. Also, each BRI-capable TA shall support one port with an RJ-11 BRI interface, one port with an RJ-45 BRI interface, and one port with an RJ-45 Ethernet interface.

[Conditional: LSC, IAD] The LSC shall support BRI-capable IADs that support secure ISDN BRI EIs. These BRI-capable IADs shall support both the ITU-T Recommendations G.711 and V.150.1 standards. Also, each BRI-capable IAD shall support from 4–16 ports with RJ-11 BRI interfaces, from 4–16 ports with RJ-45 BRI interfaces, and one port with an RJ-45 Ethernet interface.

[Conditional: EI] The ISDN BRI telephones when combined with a BRI-capable TA or BRI-capable IAD shall comply with TIA-810-B, November 3, 2006.

[Conditional: LSC MG] The LSC MG shall support BRI-capable MG line cards that support standard (nonsecure) ISDN BRI EIs. These BRI-capable MG line cards shall support the ITU-T Recommendation G.711 standard. Also, each BRI-capable MG line card shall support one port with an RJ-11 BRI interface, and one port with an RJ-45 BRI interface.

[Conditional: LSC MG] The LSC shall support BRI-capable MG line cards that support secure ISDN BRI EIs. These BRI-capable MG line cards shall support both the ITU-T Recommendations G.711 and V.150.1 standards. Also, each BRI-capable MG line card shall support one port with an RJ-11 BRI interface, and one port with an RJ-45 BRI interface.

[Conditional: EI] The ISDN BRI telephones when combined with a BRI-capable MG line card shall comply with TIA-810-B, November 3, 2006.

[Conditional: LSC, TA, IAD, LSC MG, EI] When the LSC, TA, IAD, and LSC MG support ISDN BRI EIs (both standard and secure), the LSC, TA, IAD, and LSC MG shall support all the DSN ISDN BRI requirements in the following DSN sections of UCR 2008:

- Section 5.2.1.3.3, National ISDN 1/2 Basic Access
- Section 5.2.2.6, ISDN MLPP BRI
- Section 5.2.2.8, MLPP Interactions with Common Optional Station Features and Services

- Section 5.2.2.10, MLPP Interactions with Electronic Key Telephone Systems Features

- Section 5.2.4.7, ISDN Digital Subscriber Signaling System No. 1 Signaling

- Section 5.2.9, Integrated Services Digital Network.

5.3.2.6.2 Video End Instrument

Video EIs are considered associated with the LSC and must have been designed in conjunction with the LSC design. An IP video instrument shall be designed in accordance with the acquiring activity requirements, but the following capabilities are specifically required as indicated:

1. **[Conditional]** DoD CAC card reader.

2. **[Required]** Automatic enabling of the video camera is not permitted after video session negotiation or acceptance. The called party must take a positive action to enable the camera.

3. **[Required]** Display calling number.

4. **[Required]** Display precedence level of the session.

5. **[Required]** Support for DHCP.

5.3.2.6.2.1 Display Messages, Tones, and Announcements

[Required: PEI, AEI, LSC, MFSS] Tones and announcements, as appropriate for voice and video over IP, and as required, in UCR 2008, Sections 5.2.4.5.2, DSN Information Signals, 5.2.2.1.3, Announcements, shall be supported by the PEI and AEI. These tones and announcements may be generated locally by the PEI and AEI, or generated by the LSC or a server connected to the ASLAN, and passed as a media stream to the PEI and AEI.

5.3.2.6.2.2 Video Codecs (Including Associated Audio Codecs)

1. **[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 must 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.)

2. **[Required: PEI, AEI]** Video PEIs and AEIs shall support, at a minimum, G.711 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.

3. **[Conditional: PEI, AEI]** It is recommended that video PEIs and AEIs support other audio codecs in addition to G.711 PCM. Recommended audio codecs include:

   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.

4. **[Required: PEI, AEI]** If a video PEI or AEI is intended for directly establishing video sessions with other video PEIs or AEIs (in addition to, or in place of, connectivity to a multipoint video conferencing unit), then the video PEI or AEI shall support, at a minimum, the ITU-T Recommendation H.263-2000 codec.

5. **[Required: PEI, AEI]** A video PEI or AEI intended for connectivity with a Multipoint Conferencing Unit (MCU) shall support at least one of the following video codecs:

   a. ITU-T Recommendation H.263-2000
   b. ITU-T Recommendation H.264
   c. ITU-T Recommendation H.261

5.3.2.6.2.3 Authentication to LSC

[Required: PEI, AEI, LSC, MFSS] The PEI and AEI shall be capable of authenticating themselves to their associated LSC and vice versa in accordance, Section 5.4, Information Assurance Requirements.

5.3.2.6.3 End Instrument to ASLAN Interface

[Required: PEI, AEI] The interface to the ASLAN shall be in accordance with Ethernet (IEEE 802.3) LAN technology. The 10-Mbps and 100-Mbps Fast Ethernet (IEEE 802.3u) shall be supported.

Tones and announcements may be generated locally by the PEI or AEI upon command of the LSC, or be generated upon command of the LSC by an internal LSC media server or an external media server (not part of the LSC) connected to the ASLAN and passed as a media stream to the PEI or AEI.

5.3.2.6.4 PEIs, AEIs, TAs, and IADs Us the V.150.1 Protocol

[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 applies:

1. ITU-T Recommendation V.150.1 provides for three states: audio, voice band data (VBD), and modem relay. After call setup, inband signaling may 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.

2. When the product uses ITU-T Recommendation V.150.1 inband signaling to transition between audio, FoIP, modem relay, or VBD states or modes, the product 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 EBC.

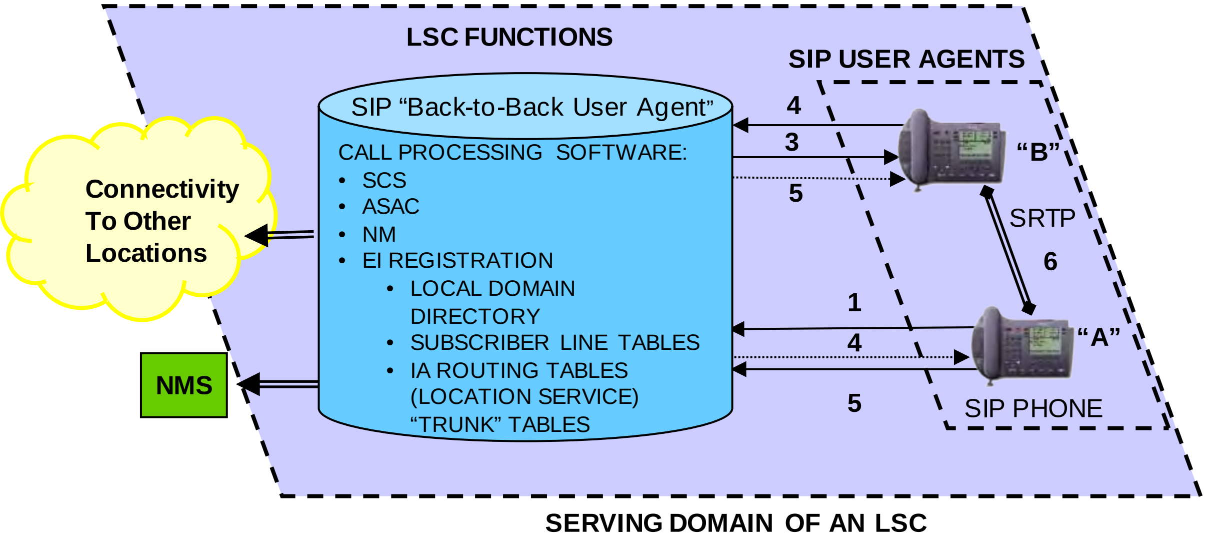
5.3.2.7 Local Session Controller

The LSC is a software-based call processing product that provides voice and video services to IP telephones and media processing devices within a local service domain. Additionally, an LSC extends signaling and call control services to allow calls to reach connections outside the local service domain. Connectivity to external networks outside a local service domain is provided via gateways to non-IP networks, or to an IP-based long-haul network.

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

Figure 5.3.2.7-1, Simple Overview of LSC Functionality, provides a simple overview of an LSC and its functions.

OVERVIEW OF AN LSC FUNCTIONALITY AND SIP SIGNALING



1. "A" SENDS DIALED DIGITS TO LSC "INVITE."
2. LSC CALL PROCESSOR PERFORMS TABLE SEARCH; LOCATES ADDRESS OF "B."
3. LSC SENDS "INVITE" MESSAGE TO "B."
4. "B" SENDS RESPONSE TO "A" VIA LSC "200 OK" (ANSWER).
5. "A" SENDS RESPONSE TO "B" VIA LSC "ACK."
6. MEDIA STREAM ESTABLISHED (NOTE: THE RTS WILL USE SRTP).

NOTE: "180" RINGING NOT SHOWN

TERMINOLOGY

SIP User Agents: Intelligent IP phones with SIP software that create and manage a SIP session.

SIP Registrar Server: Equivalent to TDM subscriber line database tables and classmarks for all telephones served directly off or by the LSC controlling a domain. In SIP messaging, these servers retrieve and send participant's IP addresses and other pertinent information to the SIP Back-to-Back User Agent (B2BUA).

(B2BUA): Equivalent to TDM call processing software that detects call for service ("off-hook"), analyzes address digits received, and based on data contained in translation tables/local subscriber line tables obtains the called telephone addressing information. Then it forwards the session invitation directly to the called telephone if it is located in the same domain, or to another B2BUA if the called telephone resides in another domain.

SIP Redirect Server: Equivalent to TDM routing tables that allow SIP B2BUAs to direct SIP session invitations to external domains. SIP redirect servers may reside in the same hardware as SIP registrars and SIP B2BUAs.

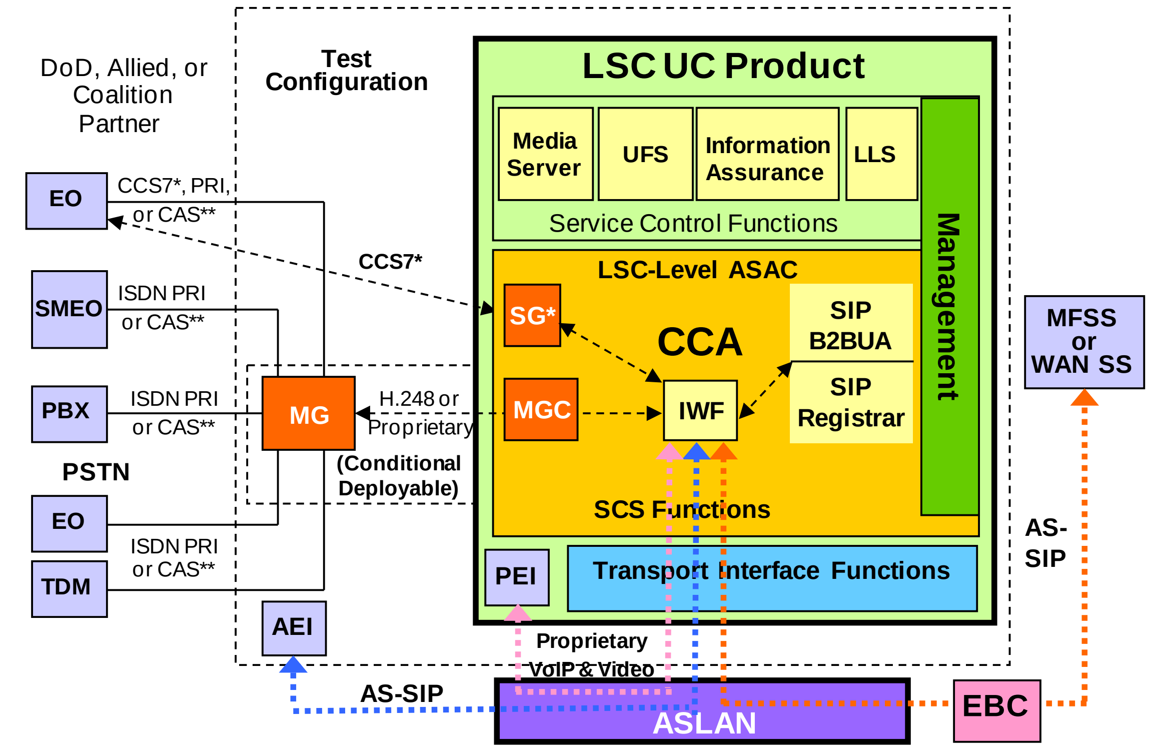
LEGEND:

ACK	Acknowledge	LSC	Local Session Controller	SIP	Session Initiation Protocol
ASAC	Assured Service Admission Control	NM	Network Management	SRTP	Secure Real-Time Transport Protocol
		NMS	Network Management System		
EI	End Instrument	RTS	Real Time Services	TDM	Time Division Multiplexing
		SCS	Session Control and Signaling		

Figure 5.3.2.7-1. Simple Overview of LSC Functionality

5.3.2.7.1 *LSC Functional Reference Model and Assumptions*

Figure 5.3.2.7-2, Functional Reference Model – LSC, shows the reference model for the LSC. The LSC consists of several SCS functions performed by the CCA, IWF, MG, MGC, and SG. These are connected via proprietary internal interface functions. Connectivity to other networks, long-haul transport systems (via an ASLAN), and DISA's VVoIP NMS (ADIMSS) are provided by external interfaces.



*Support for an SG & CCS7 is Conditional for an LSC.
**Support for CAS is Conditional for an LSC.

LEGEND:

AEI	AS-SIP End Instrument	MFSS	Multifunction Softswitch
ASAC	Assured Service Admission Control	MG	Media Gateway
ASLAN	Assured Services Local Area Network	MGC	Media Gateway Controller
AS-SIP	Assured Services Session Initiation Protocol	PEI	Proprietary End Instrument
B2BUA	Back-to-Back User Agent	PRI	Primary Rate Interface
CAS	Channel Associated Signaling	PSTN	Public Switched Telephone Network
CCA	Call Connection Agent	SCS	Session Control and Signaling
CCS7	Common Channel Signaling No. 7	SG	Signaling Gateway
DoD	Department of Defense	SIP	Session Initiation Protocol
EBC	Edge Border Controller	SMEO	Small End Office
EO	End Office	TDM	Time Division Multiplexer
ISDN	Integrated Services Digital Network	UC	Unified Capabilities
IWF	Interworking Function	UFS	User Features and Services
LLS	Local Location Service	VoIP	Voice over Internet Protocol
LSC	Local Session Controller	WAN	Wide Area Network

Note: The PEI (using Proprietary VoIP and Video) is part of the LSC UC Product; the AEI (using AS-SIP VoIP and Video) is not.

Figure 5.3.2.7-2. Functional Reference Model – LSC

Generic Requirements for the CCA, MG, and SG functions and NM are provided in separate sections of the UCR 2008, as follows:

1. Section 5.3.2.9, Call Connection Agent, contains CCA requirements, including requirements for the CCA-associated Interworking Function (IWF), which apply to both the LSC and the MFSS.

2. Section 5.3.2.12, Media Gateway Requirements, contains MG and MGC requirements.

3. Section 5.3.2.13, Signaling Gateway Requirements, contains SG requirements.

4. Section 5.3.2.17, Management of Network Appliances, contains NM requirements.

5.3.2.7.1.1 Assumptions – LSC

The following assumptions are made based on the LSC reference model:

1. The MGC and IWF are both components of the CCA. The MGC is responsible for controlling the MG in the LSC and the CAS and ISDN TDM trunk groups that are connected to it. The IWF is responsible for supporting all the VoIP and TDM signaling protocols in the LSC, and for interworking the different protocols together (see Table 5.3.2-7, Full IWF Interworking Capabilities for VoIP and TDM Protocols) for the full set of IWF capabilities. For example, the IWF is responsible for interworking AS-SIP on the IP network side with ISDN PRI on the TDM side, and interworking Proprietary VoIP on the EI side with AS-SIP on the MFSS side.

2. The MG provides circuit-switched trunk termination (for DoD PRI and CAS trunks) and TDM/VoIP interworking. The MG is controlled by the MGC. The protocol that the MGC uses to control the MG can be ITU-T Recommendation H.248 (specifically, H.248.1, Gateway Control Protocol, Version 3, September 2005), or a proprietary protocol chosen by the LSC supplier.

3. Figure 5.3.2-8, Functional Reference Model – LSC, shows the LSC supporting a single MG on a single ASLAN. In addition, a single LSC can support multiple MGs on multiple ASLANs, where those ASLANs are interconnected to form a MAN or Community of Interest Network (COIN). In this arrangement, it is expected that the set of ASLANs forming the MAN or COIN can meet the single-ASLAN performance requirements in Section 5.3.1, Assured Services Local Area Network Infrastructure. In this case, the LSC supports sessions between an MG on one ASLAN and a PEI, AEI, MG, or EBC on another ASLAN, as long as both ASLANs are part of the same MAN or COIN.

Another way of stating this is that a single LSC is able to support MGs at multiple physical locations. In some deployments, an LSC in one location will serve ASLANs and PEIs or AEIs at distant locations, where both locations are part of the same regional MAN or COIN. In these cases, each distant ASLAN may want to have its own gateway to the local PSTN. In these cases, the LSC supports MGs at multiple locations over MAN or COIN infrastructures that meet the ASLAN performance requirements in UCR 2008.

4. The LSC support for (and inclusion of) an MGC and an MG is Conditional-Deployable. That is, LSC support for (and inclusion of) an MGC and an MG is required for Fixed products, but conditional for Deployable products.

5. The LSC support for (and inclusion of) an SG is Conditional.

6. Each functional component in the LSC has associated management-related functions for FCAPS management and audit logs.

7. The signaling requirements and the Proprietary VoIP requirements for the EI-LSC interface are outside the scope of this section, and are left to the supplier's discretion. The CCA IWF is responsible for interworking the supplier's Proprietary VoIP EI implementations with DISN-standard AS-SIP on the LSC/MFSS interface. The signaling requirements for the AEI-LSC interface are DISN-standard AS-SIP.

8. The CCA interacts with the Service Control functions using internal interfaces and proprietary protocols that vary from one supplier's solution to another.

9. The LSC interactions with its EBC are as follows:

   a. The EBC controls signaling streams between an LSC (connected to an ASLAN) and an MFSS (whose separate ASLAN is connected to the DISN WAN). In doing so, the EBC also controls media streams between LSC PEIs, AEIs, and MGs (connected to the ASLAN), and PEIs, AEIs, and MGs on other LSCs (whose separate ASLANs are connected to the DISN WAN). The LSC accesses the DISN WAN via the LSC EBC and an associated Provider Edge (PE) Router on the DISN WAN.

   b. As a result, it is possible for an LSC MG to direct a VoIP media stream (interworked from a TDM media stream from the TDM side of that MG) through an EBC to the DISN WAN, and through the DISN WAN to a remote PEI, AEI, or MG.

5.3.2.7.2 Summary of LSC Functions and Features

The LSC provides voice functions and features similar to a DSN EO switching system. Line-Side (Local) Custom Calling features implemented at a vendor's discretion must not interfere with the functional requirements specified within the UCR 2008. Table 5.3.2.7-1, Summary of LSC Functions, provides a summary of LSC functions.

Table 5.3.2.7-1. Summary of LSC Functions

FUNCTION	DESCRIPTION
Session Control and Signaling	Verifies call request is consistent with policy rules call management, CAC, AS-SIP signaling function serving PEIs and AEIs: B2BUA or Call Stateful Proxy Server (assumes that some EIs will not use AS-SIP; AS-SIP used on "trunk side"), intermediary in all inbound and outbound signaling messages to/from the PEI or AEI Requests Network Resources [**Conditional**] Control (Master-Slave) to EBC on a per-session basis [**Conditional**] Signaling interworking [**Conditional**] H.323, H.248 PRI, MGCP
ASAC	Executes AS functions in the local service domain via control of the PEI, AEI, and CE Router. Determines and performs preemption where required. Maintains local active session state knowledge (session precedence level, CoS, local access bandwidth used and available).
Network Management	Provides traffic call information to, and responds to traffic flow control commands from, an NMS.
Local Domain Directory	Subscriber information, including telephone number, organization name, code address, and subscriber name.
MGC	**[Required: Fixed; Conditional: Deployed**]; Controls the MG when the MG in included in the LSC.
PEI, AEI, and User Registration	Information Assurance; access control information for authentication and authorization; PEI and AEI registration: User identification, authentication, and authorization; numbering and addressing information; user profile; CoS; precedence level.
Dialing, numbering, and routing tables; UFS Administration	Dialing, numbering, and routing tables (location services for sending call requests) regarding local calling features, multiple line appearances, voice mail, and speed call.

LEGEND

AEI	AS-SIP End Instrument	CE	Customer Edge	MGC	Media Gateway Controller
AS	Assured Services	CoS	Class of Service	MGCP	Media Gateway Control Protocol
ASAC	Assured Service Admission Control	EBC	Edge Boundary Controller		
AS-SIP	Assured Services Session Initiation Protocol	EI	End Instrument	NMS	Network Management System
		IA	Information Assurance	PEI	Proprietary End Instrument
B2BUA	Back-to-Back User Agent	LSC	Local Session Controller	RTS	Real Time Services
CAC	Call Admission Control	MG	Media Gateway	UFS	User Features and Services

5.3.2.7.2.1 PBAS/ASAC Requirements

[Required: LSC] The LSC shall meet all the requirements for PBAS/ASAC, as appropriate for VoIP and Video over IP services, as specified in UCR 2008, Section 5.2.2, Multilevel Precedence and Preemption.

5.3.2.7.2.2 Calling Number Delivery Requirements

[Required: LSC] The LSC shall support CND, as specified in UCR 2008, Section 5.2.3.5.1.8.2, Calling Number Delivery.

5.3.2.7.2.3 LSC Signaling Requirements

[Required: LSC] The LSC must provide signaling on the line side for local intra-enclave subscriber-to-subscriber calls, and trunk-side signaling for calls between an external enclave and a local subscriber. An important element of signaling is the method of addressing used to forward AS-SIP requests within the network. Table 5.3.2.7-2, LSC Support for VoIP and Video Signaling Interfaces, provides a complete list of the LSC signaling requirements.

5.3.2.7.2.4 Service Requirements under Total Loss of WAN Transport Connectivity

[Required: LSC] In the event that a total loss of connectivity to the DISN WAN occurs, the LSC shall provide the following functions:

- Completion of local (intra-enclave) calls
- Routing of calls to the PSTN using a local MG (PRI or CAS as required by the local interface)
- User look-up of local directory information

Table 5.3.2.7-2. LSC Support for VoIP and Video Signaling Interfaces

FUNCTIONAL COMPONENT	VoIP AND VIDEO SIGNALING INTERFACES	VoIP AND VIDEO SIGNALING PROTOCOLS
CCA	CCA (LSC)-to- CCA (MFSS)	AS-SIP over IP
CCA	CCA (LSC)-to-PEI (details outside the scope of this section)	Proprietary VoIP Signaling over IP
CCA	CCA (LSC) to AEI	AS-SIP over IP
CCA/MGC and MG	CCA (MGC)-to-MG	ITU-T H.248 over IP (used with DoD CCS7, ISDN PRI, and CAS trunks) **[Objective, not Required]**
CCA/MGC and MG	CCA (MGC)-to-MG	ISDN PRI over IP (North American National ISDN Version, used with ISDN PRI trunks only) **[Objective, not Required]**
CCA/MGC and MG	CCA (MGC)-to-MG	Proprietary Supplier Protocols (used as an alternative to ITU-T Recommendation H.248 over IP and ISDN PRI over IP) (used with DoD CCS7, ISDN PRI, and CAS trunks)
CCA and SG	LSC CCA-to-LSC SG	DoD CCS7 over IP (used with DoD CCS7 trunks) **[Conditional, not Required]**
CCA and SG	LSC CCA-to-LSC SG	Proprietary Supplier Protocols Used as an alternative to DoD CCS7 over IP (used with DoD CCS7 trunks) **[Conditional, not Required]**

LEGEND

AEI	AS-SIP End Instrument
AS-SIP	Assured Services Session Initiation Protocol
CAS	Channel Associated Signaling
CCA	Call Connection Agent
CCS7	Common Channel Signaling No. 7
DoD	Department of Defense
IP	Internet Protocol
ISDN	Integrated Services Digital Network
ITU-T	International Telecommunications Union – Telecommunication
LSC	Local Session Controller
MFSS	Multifunction Softswitch
MG	Media Gateway
MGC	Media Gateway Controller
PEI	Proprietary End Instrument
PRI	Primary Rate Interface
SG	Signaling Gateway
VoIP	Voice over IP

5.3.2.7.2.5 Local Location Server and Directory

[Required: LSC] The purpose of the Local Location Server (LLS) is to provide information on call routing and called address translation (where a called address is contained within the called SIP URI in the form of the called number). The CCA uses the routing information stored in the LLS to

- Route internal calls from one LSC PEI or AEI to another PEI or AEI on the same LSC.

- Route outgoing calls from an LSC PEI or AEI to another LSC, an MFSS, or a TDM network.

- Route incoming calls from another LSC, an MFSS, or a TDM network to an LSC PEI or AEI.

5.3.2.7.2.6 LSC Management Function

[Required: LSC] The LSC Management function supports functions for LSC FCAPS management and audit logs. Collectively, these functions are called FCAPS Management and Audit Logs. A complete description of these requirements is provided in

- Section 5.3.2.17, Management of Network Appliances

- Section 5.3.2.18, Network Management Requirements of Appliance Functions

- Section 5.3.2.19, Accounting Management

The CCA interacts with the LSC Management function by

1. Making changes to its configuration and to its end users' configurations, in response to commands from the Management function that requests these changes.

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

3. Sending information to the Management function on a periodic basis (e.g., on a set schedule), keeping the Management function up-to-date on CCA activity. An example of this update would be a periodic transfer of Call Detail Records (CDRs) from the CCA to the Management function, so that the Management function either could store the records locally or transfer them to a remote NMS for remote storage and processing.

5.3.2.7.2.7 LSC Transport Interface Functions

[Required: LSC] The LSC Transport Interface functions provide interface and connectivity functions with the ASLAN and its IP packet transport network. Examples of Transport Interface functions include the following:

- Network Layer functions: IP, IP security (IPSec)

- Transport Layer functions: IP Transport Protocols (Transport Control Protocol (TCP), UDP, TLS)

- LAN Protocols

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

- Each PEI or AEI served by the LSC

- Each MG served by the LSC (even though the MG may be physically connected to the CCA/MGC over an internal proprietary interface, instead of being connected logically to the CCA/MGC over the ASLAN)

- The CCA/IWF/MGC itself

- The EBC (for LSC, PEI, AEI, and MG communication with other LSCs, MFSSs, PEIs, AEIs, and MGs over the DISN WAN)

As an example, the CCA interacts with the LSC Transport Interface functions when it uses IP, TLS, TCP, and the native ASLAN protocols to exchange AS-SIP signaling messages with PEIs or AEIs and the EBC over the ASLAN.

The MGs controlled by the CCA interact with the LSC Transport Interface functions when they use IP, UDP, and the native ASLAN protocols to route SRTP media streams to and from PEIs or AEIs, other LSC MGs, and the EBC over the ASLAN.

5.3.2.7.2.8 LSC-to-NMS Interface

[Required: LSC] The LSC shall provide an interface to the DISA NMS. The interface consists of a 10/100-Mbps Ethernet connection as specified in Section 5.3.2.4.4, VVoIP Network Management System Interface Requirements.

5.3.2.7.2.9 ASAC Requirements for LSC Related to Voice and Video

[Required: LSC] For ASAC requirements, see Section 5.3.2.2.2.3, ASAC – Open Loop.

5.3.2.7.2.10 LSC to PEI, AEI, and Operator Console Status Verification

[Required: LSC] Periodically, the LSC shall verify the status of its registered and authenticated IP EIs, including operator (dial service attendant) consoles. The verification interval shall be configurable with the default set at 5 minutes.

5.3.2.7.2.11 Line-Side Custom Features Interference

[Conditional: LSC] Vendors may implement unique custom features applicable to the line side of the LSC.

[Required: LSC] Line-side custom features must not interfere with the Assured Services requirements.

5.3.2.7.3 Loop Avoidance for LSCs

[Required: LSC] During the call establishment process, the product shall be capable of preventing or detecting and stopping hair-pin routing loops over 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 LSC (see Figure 5.3.2.7-3, Example of a Hairpin Routing Loop). The Loop Avoidance mechanism must 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 LSC 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 LSC shall provide a VCA to the caller in each case.

NOTE: Currently, this feature is not required a WAN SS or MFSS with the following exceptions: (a) if the WAN SS has a Conditional LSC component, this LSC must comply with the Loop Avoidance requirement as defined in this section, and (b) likewise, the LSC component of an MFSS must comply with the Loop Avoidance requirement as defined previously. Operational experience may dictate that the scope of this requirement should be expanded to address “tandem” routing carried out by the WAN SS or the SS component of an MFSS.

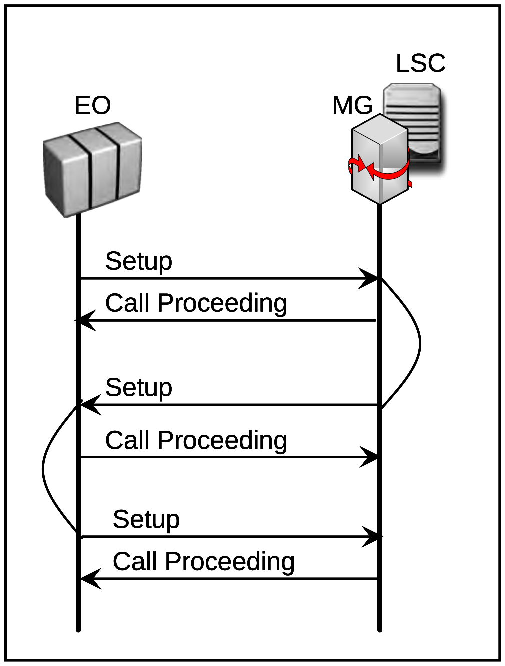


Figure 5.3.2.7-3. Example of a Hairpin Routing Loop

5.3.2.7.4 AS-SIP TDM Gateway

5.3.2.7.4.1 Overview

The AS-SIP TDM Gateway is a VVoIP appliance, and its purpose is to enable the interconnection and interoperation of a traditional TDM switch with the DISN UC system. The AS-SIP TDM Gateway performs interworking for voice and video sessions in both the signaling plane and the bearer plane.

NOTE: The AS-SIP TDM Gateway does NOT support interworking of IP-based signaling platforms and does NOT support or serve any TDM EIs or IP EIs.

Figure 5.3.2.7-4, depicts examples of the two basic topologies that use the AS-SIP TDM Gateway. The first example depicts an enclave having one assured services precedence-capable TDM switch that interfaces with the AS-SIP TDM Gateway over ISDN MLPP PRI trunks. The second example depicts an enclave with multiple TDM switches that may include a PBX2 as well as MLPP-capable TDM switches wherein on assured services precedence-capable TDM switch interfaces with the AS-SIP TDM Gateway over ISDN MLPP PRI trunks, and the other TDM switches interface with the TDM switch connected to the AS-SIP TDM Gateway.

The AS-SIP TDM Gateway only interfaces with one assured services precedence-capable TDM switch. When multiple TDM switches are located at an enclave, only one of those TDM switches is permitted to directly interface with the AS-SIP TDM Gateway. A PBX2 (or any other non-assured services precedence-capable TDM switch) is NOT permitted to directly interface with an AS-SIP TDM Gateway.

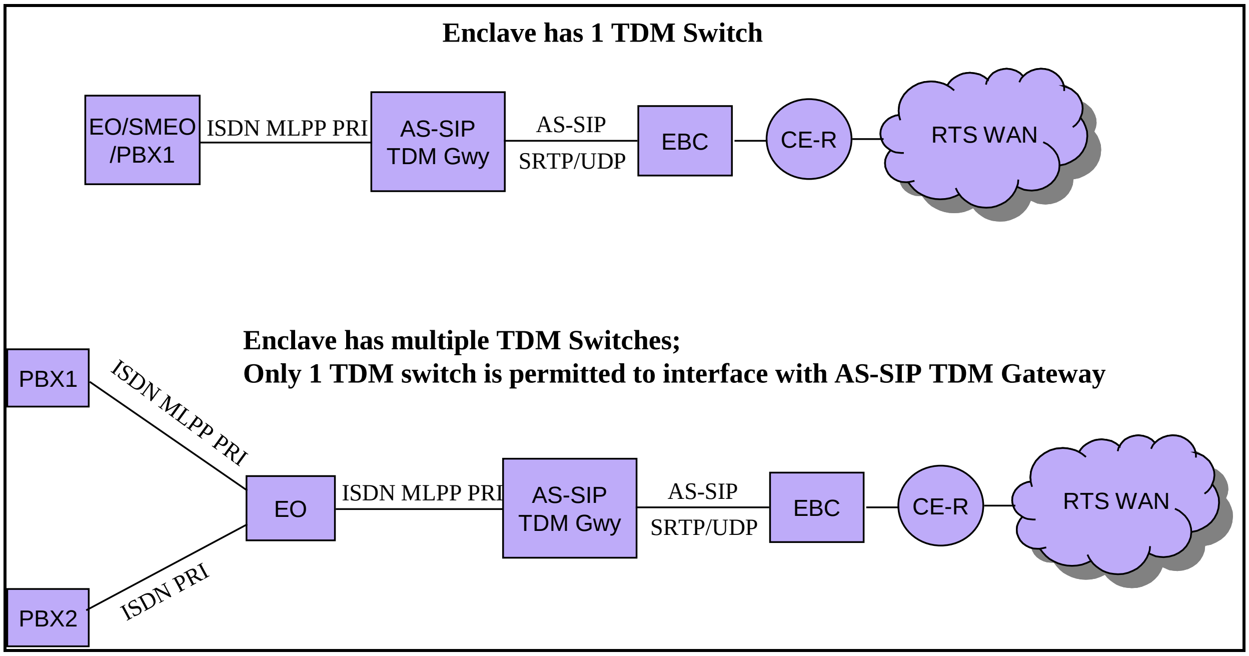


Figure 5.3.2.7-4. AS-SIP TDM Gateway Topologies

The AS-SIP TDM Gateway does NOT support ASAC and relies on the subtended TDM switch to perform that functionality. It is assumed and expected that appropriate traffic engineering will be performed with respect to the TDM trunks that interface to the AS-SIP TDM Gateway to ensure that the total number of DS0s available for serving calls via the AS-SIP TDM Gateway does not exceed the bandwidth constraints of the access link between the CE Router and the AR.

The MFSS that serves the AS-SIP TDM Gateway performs standard ASAC policing of the AS-SIP TDM Gateway.

The AS-SIP TDM Gateway MUST support the following TDM interface:

- ISDN MLPP PRI

[**Conditional**] The AS-SIP TDM Gateway MAY support the following TDM interface:

- ISDN PRI

NOTE: At this time, a use case for the ISDN PRI interface has NOT been identified.
When the AS-SIP TDM Gateway receives a SETUP message from an ISDN MLPP PRI, the AS-SIP TDM Gateway MUST interwork the SETUP message to an AS-SIP INVITE and forward the

AS-SIP INVITE to the EBC. The MLPP IE network identity digits, precedence level bits, and service domain MUST be interworked into the Resource-Priority header's network domain subfield, r-priority field, and precedence domain subfield, respectively see Section 5.3.2.7.4.3.2. Interworking of MLPP IE and RPH.

The AS-SIP TDM Gateway MUST add a CCA-ID parameter to the Contact header.

The AS-SIP TDM Gateway MUST add a route set comprising two Route headers where the first Route header is the SIP URI for the EBC at the enclave, and the second Route header is the SIP URI for the EBC serving the MFSS.

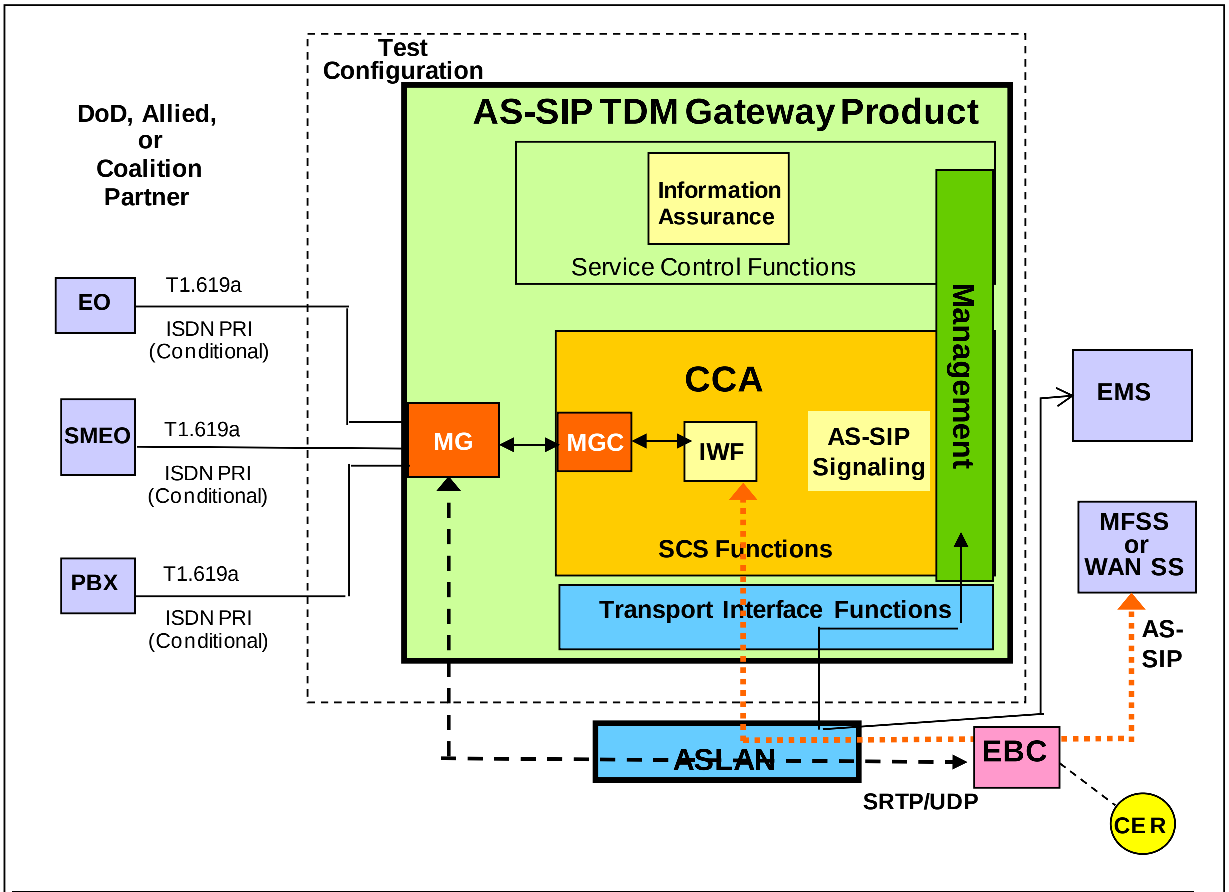
When the AS-SIP TDM Gateway receives an AS-SIP INVITE from the MFSS via the EBC intended for an ISDN MLPP PRI, the AS-SIP TDM Gateway MUST interwork the INVITE to a SETUP message (including MLPP IE) and forward the SETUP message on the D-channel.

The TDM switch is responsible for implementing the assured services Precedence Capability function and the AS-SIP TDM Gateway MUST interwork INVITEs received from the EBC to the TDM switch, even if all DS0s are currently in use. The TDM switch is responsible for either rejecting the call request, conducting preemption, or diverting the call request to an attendant or voicemail system.

The AS-SIP TDM Gateway MUST NOT perform directionalization and MUST NOT perform code blocking. Both of these functions are the responsibility of the TDM switch connected to the AS-SIP TDM Gateway.

5.3.2.7.4.2 AS-SIP TDM Gateway Functional Reference Model and Assumptions

Figure 5.3.2.7-5. Functional Reference Model – AS-SIP TDM Gateway, shows the reference model for the AS-SIP TDM Gateway. The AS-SIP TDM Gateway consists of several SCS functions performed by the CCA, IWF, MGC, and MG. These are connected via proprietary internal interface functions. Connectivity to other networks, long-haul transport systems (via an ASLAN), and DISA's VVoIP NMS (ADIMSS) are provided by external interfaces.



LEGEND:

ASLAN	Assured Services Local Area Network	MG	Media Gateway
AS-SIP	Assured Services Session Initiation Protocol	MGC	Media Gateway Controller
CCA	Call Connection Agent	PBX	Private Branch Exchange
CE R	Customer Edge Router	PEI	Proprietary End Instrument
DoD	Department of Defense	PRI	Primary Rate Interface
EBC	Edge Border Controller	SCS	Session Control and Signaling
EMS	Element Management System	SMEO	Small End Office
EO	End Office	SRTP	Secure Real Time Transport Protocol
ISDN	Integrated Services Digital Network	SS	Softswitch
IWF	Interworking Function	UDP	User Datagram Protocol
MFSS	Multifunction Softswitch	WAN	Wide Area Network

Figure 5.3.2.7-5. Functional Reference Model – AS-SIP TDM Gateway

Generic Requirements for the CCA and MG functions and NM are provided in separate sections of the UCR, as follows:

1. Section 5.3.2.9, Call Connection Agent, contains CCA requirements, including the CCA-associated IWF.

2. Section 5.3.2.12, Media Gateway Requirements, contains MG and MGC requirements.

3. Section 5.3.2.17, Management of Network Appliances, contains NM requirements.

5.3.2.7.4.2.1 Assumptions – AS-SIP TDM Gateway

The following assumptions are made based on the AS-SIP TDM Gateway reference model:

1. The AS-SIP TDM Gateway only interfaces with one TDM switch, and the TDM switch MUST implement assured services precedence capability.

2. All of the trunks of the assured services precedence-capable TDM switch (i.e. EO, SMEO, or PBX1) that interface to the AS-SIP TDM Gateway MUST be ISDN MLPP PRI trunks.

3. The TDM switch has no other TDM or IP connectivity to the UC WAN aside from the AS-SIP TDM Gateway. The TDM trunks to the MFS will be eliminated to avoid hybrid routing issues at the MFSS/MFS and WAN SS.

4. The MGC and IWF are both components of the CCA. The MGC is responsible for controlling the MG in the AS-SIP TDM Gateway and the ISDN MLPP PRI TDM trunk groups that are connected to it. The IWF is responsible for supporting all the VoIP and TDM signaling protocols in the AS-SIP TDM Gateway, and for interworking the different protocols together (see Table 5.3.2.7-3 which is a subset of the interworking capabilities set forth in Table 5.3.2.9-2, Full IWF Interworking Capabilities for VoIP and TDM Protocols).

Table 5.3.2.7-3. AS-SIP TDM Gateway IWF Interworking Capabilities for VoIP and TDM Protocols

IWF INPUT PROTOCOL	IWF OUTPUT PROTOCOL		
	AS-SIP (TO AN EBC)	ISDN MLPP PRI	ISDN PRI
AS-SIP (from an EBC)	*No interworking needed*	Required	Conditional (use case yet to be identified)
ISDN MLPP PRI	Required	*No interworking needed*	*N/A*
ISDN PRI	Conditional (Use case yet to be identified)	N/A	*No interworking needed*

LEGEND:

AS-SIP	Assured Services Session Initiation Protocol	ISDN	Integrated Services Digital Network
CAS	Channel-Associated Signaling	IWF	Inter Working Function
EBC	Edge Boundary Controller	MLLP	Multilevel Precedence and Preemption
		N/A	Not Applicable
		PRI	Primary Rate Interface

5. The MG provides circuit-switched trunk termination (for ISDN MLPP PRI trunks and [**conditional**] for ISDN PRI trunks) and TDM/VoIP interworking. The MG is controlled

by the MGC. The interface between the MGC and MG is internal to the AS-SIP TDM Gateway and the choice of protocol is left to the vendor.

6. The MG functionality is an integral component of the AS-SIP TDM Gateway and the AS-SIP TDM Gateway does not support remote MGs or multiple MGs.

7. The AS-SIP TDM Gateway does NOT include a SG.

8. Each functional component in the AS-SIP TDM Gateway has associated management-related functions for FCAPS management and audit logs.

9. The CCA interacts with the Service Control functions using internal interfaces and proprietary protocols that vary from one supplier's solution to another.

10. The AS-SIP TDM Gateway interactions with its EBC are as follows:

    a. The EBC controls signaling streams between an AS-SIP TDM Gateway (connected to an ASLAN) and an MFSS (where a separate ASLAN is connected to the UC WAN). The AS-SIP TDM Gateway accesses the UC WAN via the EBC and an associated AR on the UC WAN.

    b. As a result, it is possible for an AS-SIP TDM Gateway to direct a VoIP media stream (interworked from a TDM media stream from the TDM side of that MG) through an EBC to the UC WAN, and through the UC WAN to a remote EI or MG.

5.3.2.7.4.3 Summary of AS-SIP TDM Gateway Functions and Features

Table 5.3.2.7-4 provides a summary of AS-SIP TDM Gateway functions.

Table 5.3.2.7-4. Summary of AS-SIP TDM Gateway Functions

FUNCTION	DESCRIPTION
Session Control and Signaling	Signaling interworking ISDN MLPP PRI [**Conditional**] ISDN PRI 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 NMS.
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

FUNCTION	DESCRIPTION
	Assignment of appropriate value to DSCP field when generating SRTP/UDP/IP packets

LEGEND

AS-SIP	Assured Services Session Initiation Protocol	NMS	Network 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		

5.3.2.7.4.3.1 AS-SIP TDM Gateway Signaling Requirements

The AS-SIP TDM Gateway must provide signal interworking between the connected TDM switch and the designated MFSS. Table 5.3.2.7-5, AS-SIP TDM Gateway Support for VoIP and Video Signaling Interfaces. Provides the list of the AS-SIP TDM Gateway signaling requirements.

Table 5.3.2.7-5. 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 (MFSS)	AS-SIP over IP
CCA/MGC and MG	CCA (MGC) – to – MG	Internal interface to integrated MG functional component (used with ISDN MLPP PRI trunks) (Conditional: ISDN PRI – Use case yet to be identified)

LEGEND

AS-SIP	Assured Services Session Initiation Protocol	ISDN	Integrated Services Digital Network	MG	Media Gateway
				MGC	Media Gateway Controller
CAS	Channel Associated Signaling	MFSS	Multifunction Softswitch	PRI	Primary Rate Interface
CCA	Call Connection Agent	MLPP	Multilevel Precedence and Preemption	TDM	Time Division Multiplexing
IP	Internet Protocol			VoIP	Voice over IP

5.3.2.7.4.3.2 Interworking of MLPP IE and Resource-Priority Header

Per UCR Sections 5.3.4.10.2.1, Resource-Priority Header Field, 5.3.4.10.2.1.1, Namespace; 5.3.4.10.2.1.2, r-priority, 5.2.2.7.2, Precedence Level Information Elements; and 5.3.4.18.2 Requirements for Interworking AS-SIP Signaling Appliances, when the AS-SIP TDM Gateway receives a SETUP message from an ISDN MLPP PRI trunk then the AS-SIP TDM Gateway interworks:

1. The four network identity digits found in octets 5 and 6 of the MLPP IE into the Network Domain subfield of the Namespace of the Resource-Priority header of an INVITE message

NOTE: From FY 2008–FY 2012, the only valid value for the Network Domain subfield is "uc".

2. The precedence level specified in bits 1–4 of octet 3 of the MLPP IE to the equivalent representation in the r-priority field of the Resource Priority header of an INVITE message.

3. The MLPP service domain found in octets 7–9 of the MLPP IE into the Precedence-Domain subfield of the Namespace of the Resource-Priority header.

   NOTE: From FY 2008–FY 2012, the only valid value for the Precedence-Domain subfield is " 000000".

Per UCR Sections 5.3.4.10.2.1, Resource-Priority Header Field; 5.3.4.10.2.1.1, Namespace, 5.3.4.10.2.1.2, r-priority; 5.2.2.7.2 Precedence Level Information Elements; and 5.3.4.18.2, Requirements for Interworking AS-SIP Signaling Appliances, when the AS-SIP TDM Gateway receives an AS-SIP INVITE message intended for an ISDN MLPP PRI trunk then the AS-SIP TDM Gateway interworks:

1. The Network Domain subfield of the Namespace of the Resource-Priority header to the four network identity digits found in octets 5 and 6 of the MLPP IE of a SETUP message

   NOTE: From FY 2008-2012 the only valid value for the network identity digits of the MLPP IE is the binary coded decimal value "0000."

2. The precedence level in the r-priority field of the Resource Priority header to the equivalent representation in bits 1-4 of octet 3 of the MLPP IE of a SETUP message.

3. The precedence-domain subfield of the Namespace of the Resource-Priority header to the MLPP service domain in octets 7–9 of the MLPP IE of the SETUP message.

   NOTE: From 2008-2012, the only valid value for the MLPP service domain is $000000000000000000000000_{\text{binary}}$ (i.e., 0x000000)

5.3.2.7.4.3.3 SIP URI and Mapping of Telephone Number

When the AS-SIP TDM Gateway receives a call request over an ISDN MLPP PRI then the AS-SIP TDM Gateway MUST map the telephony numbers received from the Q.931 SETUP message to SIP URIs in accordance with UCR Section 5.3.4.14.3, SIP URI and Mapping of Telephony Number into SIP URI, and UCR Section 5.3.4.7.6, SIP URI and Mapping of Telephone Number into SIP URI.

5.3.2.7.4.3.4 AS-SIP TDM Gateway Media Requirements

Summary of Relevant Media Packet Requirements from Other UCR Sections

The AS-SIP TDM Gateway MG MUST support the ITU-T Recommendation G.711 (μ-law and A-law) audio codec.

The AS-SIP TDM Gateway MG MUST support RFC 4040 and the AS-SIP TDM Gateway MUST support the signaling for establishing the 64kbps unrestricted bearer per Section 5.3.4.7.7, 64 kbps Transparent Calls (Clear Channel).

NOTE: The 64 kbps "clearmode" data streams are used to transport individual H.320 video/64 kbps video streams across the IP network from one TDM H.320 end point to another. The AS-SIP TDM Gateway MG is NOT required to participate in the "bonding" of the 64 kbps video streams.

The AS-SIP TDM Gateway MG does NOT support interworking of H.320 TDM video and IP video.

The AS-SIP TDM Gateway MG is NOT required to perform transcoding between codec types but MUST perform A-law/μ-law conversion when needed.

The AS-SIP TDM Gateway MG MUST support T.38 Fax Relay (see Section 5.3.2.12.12.6.6, MG Support for Group 3 Fax Calls.

The AS-SIP TDM Gateway MG MUST support the SCIP-216 subset of V.150.1 Modem Relay (see Section 5.3.2.21.2, RTS SCIP Gateway Requirements) and the AS-SIP TDM Gateway MUST support the AS-SIP signaling requirements in support of modem relay (See 5.3.4.13.9.1, AS-SIP Signaling Requirements in Support of Modem Relay-Capable Gateways).

5.3.2.7.4.3.5 Information Assurance Requirements

The AS-SIP TDM Gateway MUST satisfy the Information Assurance requirements in Section 5.4 Information Assurance for a media gateway.

5.3.2.7.4.3.6 Service Requirements under Total Loss of WAN Transport Connectivity

Upon total loss of WAN transport the AS-SIP TDM Gateway becomes incapable of exchanging either signaling messages or media packets between the connected TDM switch and the UC WAN. The immediate consequence is that the users on the existing voice and video sessions can no longer successfully send or receive media, and will go on-hook. The signaling termination messages (triggered by going on-hook) will fail to transit the WAN due to the loss of WAN transport. In addition, since the AS-SIP TDM Gateway provides the only connectivity to the UC WAN for the TDM switch, the TDM switch loses the ability to establish new calls over the UC WAN until WAN connectivity is restored.

5.3.2.7.4.3.7 AS-SIP TDM Gateway Management Function

The following Generic Requirements for the NM function are applicable to the AS-SIP IP Gateway:

- Section 5.3.2.1.17, Management of Network Appliances

- Section 5.3.2.18.1, Management Requirements of the CCA Function

- Section 5.3.2.18.3, Management Requirements of the CCA Function excluding Section 5.3.2.18.3.1.1.2, SG-Related Data

- Section 5.3.2.18.5, Management Requirements of the MG Function, excluding requirements for analog lines, ISDN BRI interface parameters, and IDLC

The CCA interacts with the AS-SIP TDM Gateway Management function by:

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

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

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

5.3.2.7.4.3.8 AS-SIP TDM Gateway Transport Interface Functions

The AS-SIP TDM Gateway Transport Interface functions provide interface and connectivity with the ASLAN and its IP packet transport network. Examples of Transport Interface functions include the following:

- Network Layer functions: IP, IPSec where IPSec is used to protect NM IP packets

- Transport Layer functions: IP Transport Protocols TCP, UDP, TLS
- LAN Protocols

The CCA interacts with Transport Interface functions by using them to communicate with the EBC (and through the EBC to the MFSS) over the ASLAN. The following Local Domain elements are all IP end points on the ASLAN:

- The MG functional component
- The CCA/IWF/MGC itself
- The EBC

As an example, the CCA interacts with the AS-SIP TDM Gateway Transport Interface functions when it uses IP, TLS, TCP, and the native ASLAN protocols to exchange AS-SIP signaling messages with the EBC over the ASLAN.

The integrated MG controlled by the CCA interacts with the AS-SIP TDM Gateway Transport Interface functions when it uses IP, UDP, and the native ASLAN protocols to route SRTP media streams to and from the EBC over the ASLAN.

5.3.2.7.4.3.9 AS-SIP TDM Gateway-to-NMS Interface

The AS-SIP TDM Gateway MUST provide an interface to the DISA NMS. The interface MUST consist of a 10/100-Mbps Ethernet connection, as specified in Section 5.3.2.4.4, VVoIP NMS Interface Requirements.

5.3.2.7.4.3.10 No ASAC Requirements for AS-SIP TDM Gateway Related to Voice and Video

The AS-SIP TDM Gateway does NOT implement ASAC requirements. The TDM trunks between the connected TDM switch and the AS-SIP TDM Gateway MUST be engineered to limit the maximum traffic flow to fit the bandwidth constraints of the access link.

5.3.2.7.4.3.11 Additional Features

The AS-SIP TDM Gateway MUST support ITU-T Recommendation V.150.1 Modem Relay (See Section 5.3.4.13.9, Modem on IP Networks, and the NSA specification SCIP-216).

The AS-SIP TDM Gateway MUST support ITU-T Recommendation T.38 Fax Relay.

5.3.2.7.4.3.12 Specific Functions and Features NOT Supported

Specifically, the AS-SIP TDM Gateway does NOT support the following functions or requirements:

- A media server
- An RTS stateful firewall

- RTS Routing Database functions
- AS-SIP interfaces for voicemail and unified messaging

5.3.2.7.5 AS-SIP IP Gateway

5.3.2.7.5.1 Overview

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. The AS-SIP IP Gateway directly interfaces with only one IP-based UC signaling platform and does NOT support interworking of TDM-based signaling platforms and does NOT serve as a call manager for any TDM or IP EIs.

NOTE: Unlike the AS-SIP TDM Gateway, the AS-SIP IP Gateway is not an assured services appliance, and its placement in this section is for requirements grouping purposes and should not be interpreted as implying that the AS-SIP IP Gateway is an assured services appliance.

The AS-SIP IP Gateway SUT consists of the AS-SIP IP Gateway, the proprietary UC signaling platform, and the IP EIs served by the proprietary UC signaling platform.

As a precondition for testing at the JITC facilities the AS-SIP IP Gateway vendor MUST:

1. Establish a relationship with the UC signaling platform vendor whereby both vendors mutually agree that the AS-SIP IP Gateway vendor is to provide the interworking appliance that will enable interconnection and interoperation of the UC signaling platform and its IP EIs with the DISN UC system.

2. Conduct successful Interoperability testing of voice and video signaling and media between the AS-SIP IP Gateway and the proprietary UC signaling platform and its IP EIs.

3. Present a certificate signed by the UC signaling platform vendor that affirms that the AS-SIP IP Gateway and the proprietary UC signaling platform have undergone successful Interoperability testing for voice and video signaling and media

The AS-SIP IP Gateway interfaces to the enclave EBC in both the signaling plane and the bearer plane and is responsible for interworking AS-SIP voice and video signaling with the voice and video signaling of the proprietary UC signaling platform. and the AS-SIP Gateway is responsible for interworking UCR-compliant voice and video media packets with the voice and video media packets supported by the proprietary UC signaling platform's IP EIs. Interoperability of UC features and services other than non-assured voice and video services is outside the scope of the required functionality for the AS-SIP IP Gateway and will not be a part of AS-SIP IP Gateway SUT Interoperability testing.

From a signaling perspective, the AS-SIP IP Gateway MUST offer an AS-SIP-compliant signaling interface that provides end-to-end signaling Interoperability between the AS-SIP IP Gateway SUT and the AS-SIP signaling appliances of the DISN UC WAN.

From a media perspective, the AS-SIP IP Gateway MUST offer a UCR-compliant bearer interface that provides E2E Interoperability for voice and video media packets between the AS-SIP IP Gateway SUT and EBCs, IP EIs of LSC SUTs, MGs, and AS-SIP EIs. The AS-SIP IP Gateway MUST 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 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 proprietary UC signaling platform MUST be interworked by the AS-SIP IP Gateway into the proprietary media packets supported by the IP EIs.

Figure 5.3.2.7-6 depicts the AS-SIP IP Gateway SUT in relation to the UC WAN where the logical interface is between the AS-SIP IP Gateway and the EBC. The UCR does NOT mandate the connectivity, interface, or protocol requirements within the AS-SIP IP Gateway SUT and the internal signaling and media lines (in blue) represent notional connectivity options.

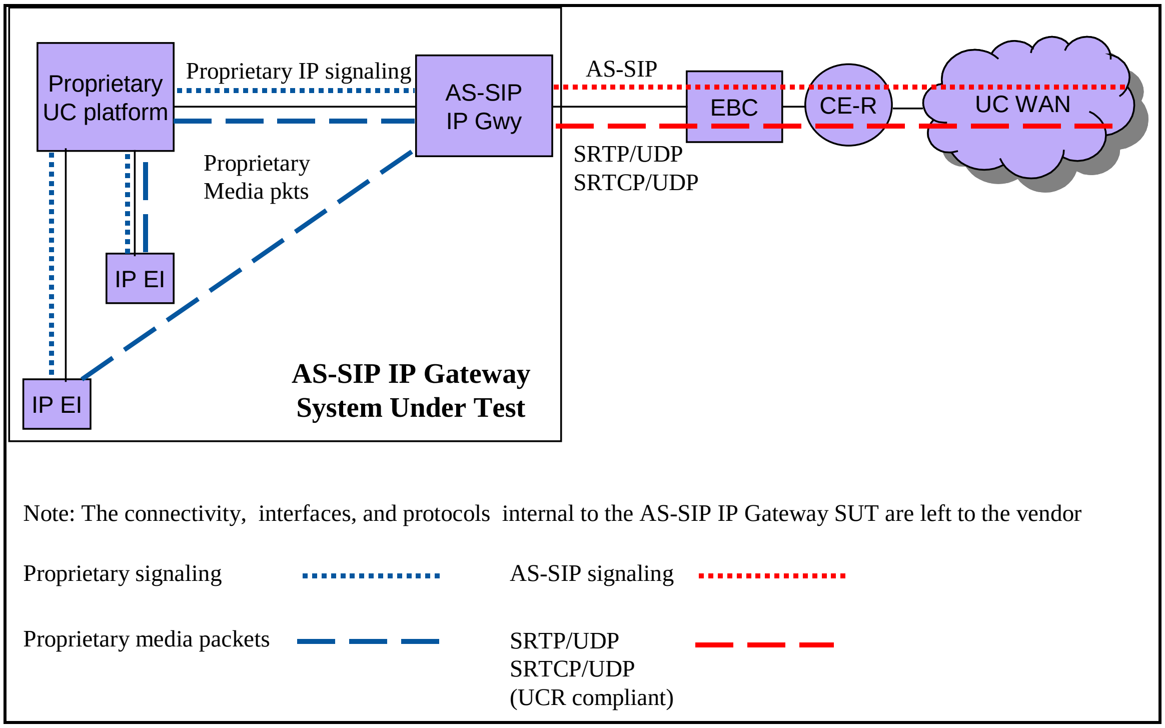


Figure 5.3.2.7-6. AS-SIP IP Gateway Topology

5.3.2.7.5.1.1 The AS-SIP IP Gateway MUST implement call count thresholds for voice sessions and for video sessions in order to perform Session Admission Control (SAC). See Section 5.3.2.7.5.3.1.4 Session Admission Control. for more details.

AS-SIP IP Gateway Call Request Processing Overview

5.3.2.7.5.1.2 When the AS-SIP IP Gateway receives a call request from the proprietary UC signaling platform then the AS-SIP IP Gateway MUST:

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:

    (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 EBC at the enclave, and the second Route header is the SIP URI for the EBC serving the WAN SS/MFSS.

    (5) Forwarding the INVITE message to the EBC at the enclave

- 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 MUST reject the call. NOTE: If the proprietary signaling interface is SIP, then the response message is 488 (Not Acceptable Here) and SHOULD include a Warning header field with warning code 370 (Insufficient Bandwidth).

5.3.2.7.5.1.3 When an AS-SIP IP Gateway receives an initial routine AS-SIP INVITE (i.e., not a re-INVITE) from the WAN SS/MFSS (via the EBC), then the AS-SIP IP Gateway MUST:

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 MUST reject the call. NOTE: The response message is 488 (Not Acceptable Here) and SHOULD include a Warning header field with warning code 370 (Insufficient Bandwidth)

5.3.2.7.5.1.4 The AS-SIP IP Gateway MUST support the following 2 methods for processing initial precedence AS-SIP INVITEs received from the WAN SS/MFSS via the EBC and the choice of method MUST 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 MUST 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.

WAN SS/MFSS Policing Requirements when Serving an AS-SIP IP Gateway

5.3.2.7.5.1.5 The AS-SIP IP Gateway only sends routine AS-SIP INVITEs to the WAN SS/MFSS, and the WAN SS/MFSS MUST apply the standard ASAC policing rules for outbound routine voice and video requests.

See UCR Requirements 5.3.4.11.1.8, 5.3.4.11.1.10, 5.3.4.11.1.11, and 5.3.4.11.1.12 for policing routine outbound telephony requests.

See UCR Requirements 5.3.4.11.2.9, 5.3.4.11.2.11, 5.3.4.11.2.12, and 5.3.4.11.2.13 for policing routine outbound video requests.

5.3.2.7.5.1.6 When a WAN SS/MFSS receives an initial "routine" AS-SIP INVITE intended for forwarding to a served AS-SIP IP Gateway, the WAN SS/MFSS MUST apply the standard ASAC policing rules for inbound routine voice and video requests.

See UCR Requirements 5.3.4.11.1.13, 5.3.4.11.1.13.1, 5.3.4.11.1.13.3, 5.3.4.11.1.13.4, 5.3.4.11.1.13.5, 5.3.4.11.1.14, 5.3.4.11.1.14.1, 5.3.4.11.1.14.2, 5.3.4.11.1.14.5, 5.3.4.11.1.14.6, 5.3.4.11.1.14.7, 5.3.4.11.1.14.8, 5.3.4.11.1.14.9, 5.3.4.11.1.14.10, 5.3.4.11.1.15, 5.3.4.11.1.15.1, 5.3.4.11.1.15.3, 5.3.4.11.1.15.4, and 5.3.4.11.1.15.5 for policing inbound routine telephony requests.

See UCR Requirements 5.3.4.11.2.14, 5.3.4.11.2.14.1, 5.3.4.11.2.14.3, 5.3.4.11.2.14.4, 5.3.4.11.2.14.5, 5.3.4.11.2.14.6, 5.3.4.11.2.15, 5.3.4.11.2.15.1, 5.3.4.11.2.15.3, 5.3.4.11.2.15.4, 5.3.4.11.2.15.5, and 5.3.4.11.2.15.6 for policing inbound routine video requests.

5.3.2.7.5.1.7 When a WAN SS/MFSS receives an initial precedence AS-SIP INVITE intended for forwarding to a served AS-SIP IP Gateway, the WAN SS/MFSS MUST implement one of the following two policing rules:

1. **[Preferred]** Forward the AS-SIP INVITE to the AS- 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 WAN SS/MFSS:

    a. Sends a 488 (Not Acceptable Here) response code to the remote initiating party of the AS-SIP INVITE that SHOULD include a Warning header field with warning code 370 (Insufficient Bandwidth).

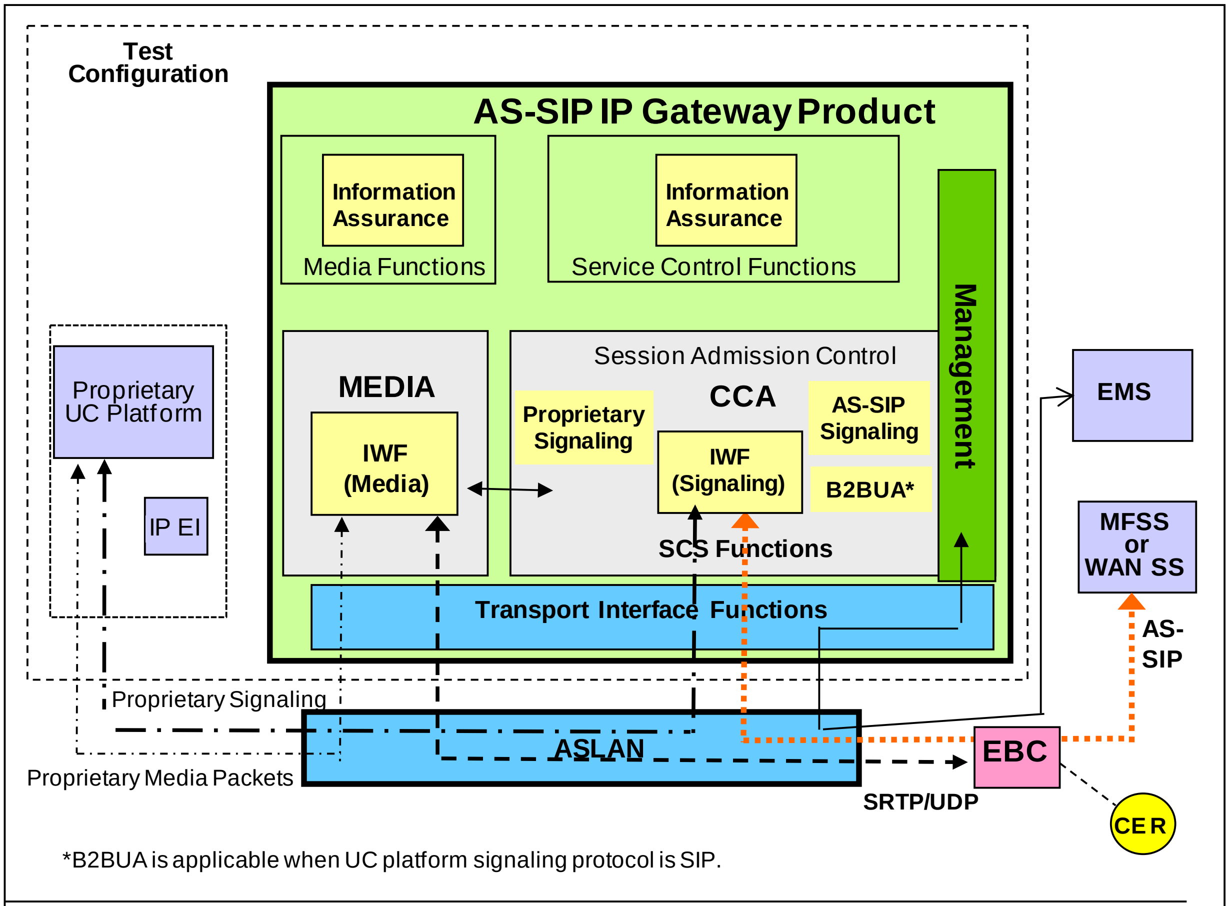
    b. Sends a CANCEL request (in the case of a 1xx response code) or a BYE request (in the case of a 2xx response code) to the local AS-SIP IP Gateway.

NOTE: This approach has the WAN SS/MFSS applying the standard ASAC policing rules for a ROUTINE request to a precedence request.

2. **[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 WAN SS/MFSS applies the standard ASAC policing rules for a precedence call request. That is, the WAN SS/MFSS 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 MUST 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 MFSS will forward the 1xx response greater than 100 or the 2xx response to the precedence inbound call request over the UC WAN.

5.3.2.7.5.2 AS-SIP IP Gateway Functional Reference Model and Assumptions

Table 5.3.2.7-7 shows the reference model for the AS-SIP IP Gateway. The AS-SIP IP Gateway consists of several SCS functions performed by the CCA, IWF (for signaling), and IWF (for media). These are connected via proprietary internal interface functions. Connectivity to other networks, long-haul transport systems (via an ASLAN), and DISA’s VVoIP NMS (ADIMSS) are provided by external interfaces.



*B2BUA is applicable when UC platform signaling protocol is SIP.

LEGEND:

ASLAN	Assured Services Local Area Network	IWF	Interworking Function
AS-SIP	Assured Services Session Initiation Protocol	MFSS	Multifunction Softswitch
B2BUA	Back-to –Back user Agent	MG	Media Gateway
CCA	Call Connection Agent	SCS	Session Control and Signaling
CE R	Customer Edge Router	SMEO	Small End Office
DoD	Department of Defense	SRTP	Secure Real Time Transport Protocol
EBC	Edge Border Controller	SS	Softswitch
EI	End Instrument	UDP	User Datagram Protocol
EMS	Element Management System	WAN	Wide Area Network

Figure 5.3.2.7-7. Functional Reference Model – AS-SIP IP Gateway

5.3.2.7.5.2.1 Assumptions – AS-SIP IP Gateway

The following assumptions are made based on the AS-SIP IP Gateway reference model:

1. The AS-SIP IP Gateway interfaces with only one proprietary UC signaling platform.

2. The proprietary UC signaling platform has no other connectivity to the UC WAN aside from the AS-SIP IP Gateway.

3. Each functional component in the AS-SIP IP Gateway has associated management-related functions for FCAPS management and audit logs.

4. The CCA interacts with the Service Control functions using internal interfaces and proprietary protocols that vary from one supplier's solution to another.

5. The AS-SIP IP Gateway interactions with its EBC are as follows:

   a. The EBC controls signaling streams between the AS-SIP IP Gateway (connected to an ASLAN) and a WAN SS/MFSS (where its separate ASLAN is connected to the DISN WAN). The AS-SIP IP Gateway accesses the UC WAN via the EBC and an associated AR on the UC WAN.

   b. The EBC controls media streams between the AS-SIP IP Gateway (connected to the ASLAN) and other AS-SIP IP Gateways, or the EIs and MGs of LSCs (whose separate ASLANs are connected to the DISN UC WAN).

5.3.2.7.5.3 Summary of AS-SIP IP Gateway Functions and Features

The AS-SIP IP Gateway provides interworking functions for the signaling and bearer planes (see Table 5.3.2.7-6, Summary of AS-SIP IP Gateway Functions).

Table 5.3.2.7-6. 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, 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 NMS.

LEGEND

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

5.3.2.7.5.3.1 AS-SIP IP Gateway SCS Requirements

Table 5.3.2.7-7 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 5.3.2.7-7. 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 (WAN SS/MFSS)	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	UC	Unified Capabilities
CCA	Call Connection Agent	WAN SS/MFSS	WAN Softswitch/Multifunction Softswitch
IP	Internet Protocol	VoIP	Voice over IP

5.3.2.7.5.3.1.1 CCA Function

The CCA is part of the SCS functions and includes the IWF (signaling) function. The scope of these CCA requirements covers the following areas:

1. AS-SIP signaling protocol implementation for voice and video calls

2. Proprietary signaling protocol implementation for voice and video calls (where signaling protocol implementation refers to the signaling being used by the proprietary UC signaling platform)

3. Control of sessions within the AS-SIP IP Gateway including:

   a. Proprietary (i.e., non-AS-SIP) sessions between the AS-SIP IP Gateway and the proprietary UC signaling platform

   b. AS-SIP sessions between the AS-SIP IP Gateway and the serving WAN SS/MFSS

4. Support for interactions with other network appliance functions including:

   a. Admission control
   b. Information Assurance
   c. Media interworking
   d. Appliance Management functions.

Figure 5.3.2.7-8 illustrates the relationship between the CCA and other functional components.

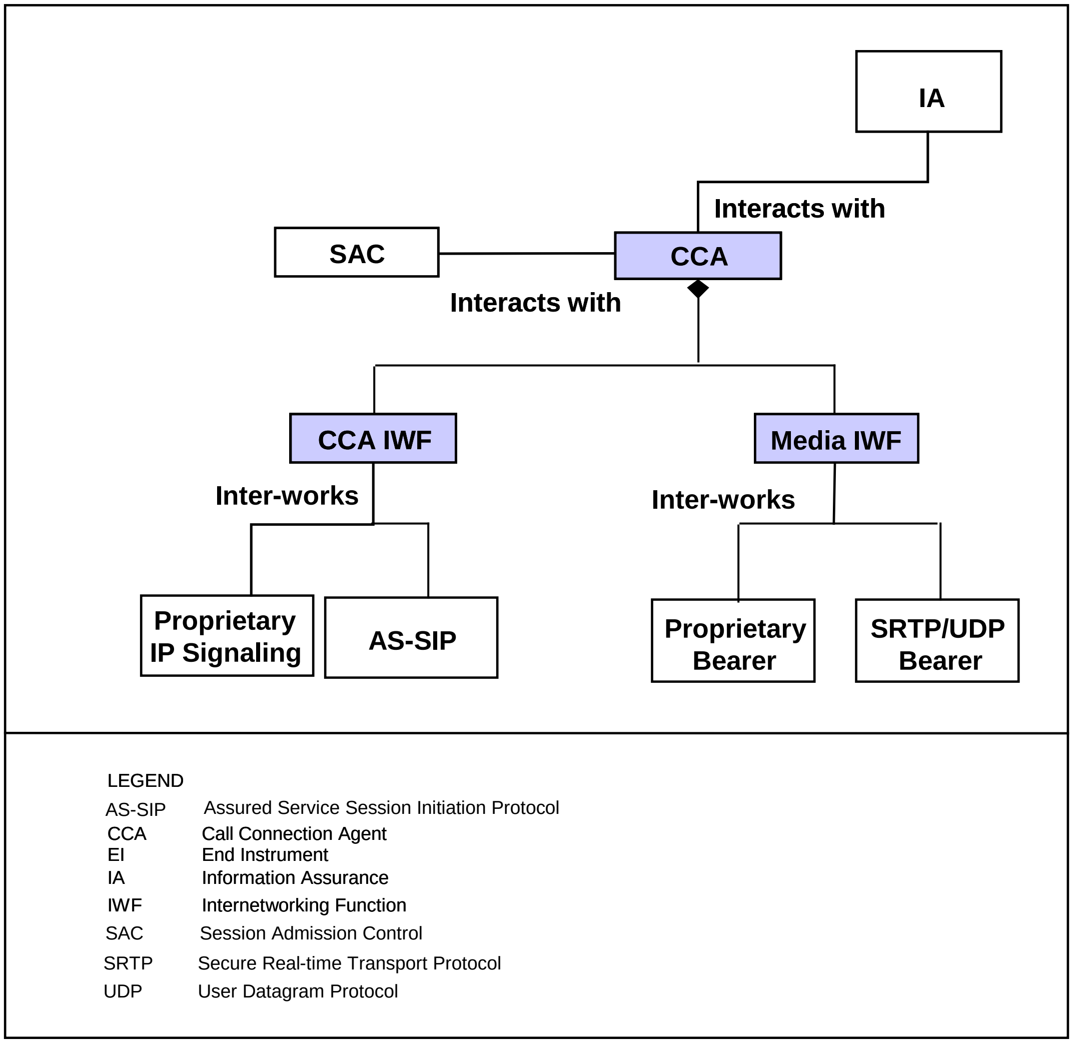

IA
Interacts with
SAC
CCA
Interacts with
CCA IWF
Media IWF
Inter-works
Inter-works
Proprietary IP Signaling
AS-SIP
Proprietary Bearer
SRTP/UDP Bearer
LEGEND
AS-SIP Assured Service Session Initiation Protocol
CCA Call Connection Agent
EI End Instrument
IA Information Assurance
IWF Internetworking Function
SAC Session Admission Control
SRTP Secure Real-time Transport Protocol
UDP User Datagram Protocol

Figure 5.3.2.7-8. CCA Relationships

The role of the AS-SIP IP Gateway CCA is to provide session control for all VoIP sessions and Video over IP sessions that are originated by, or terminated in, the DISN UC network and are interworked by the AS-SIP IP Gateway on behalf of the proprietary UC signaling platform. The proprietary signaling protocol used by the proprietary UC signaling platform is by definition an IP signaling protocol that is not compliant with the UCR AS-SIP requirements. When this proprietary IP signaling protocol is a SIP implementation, then the CCA in the AS-SIP IP Gateway takes on the role of the SIP Back-to-Back User Agent (B2BUA) in the traditional SIP architecture but with the addition of the SIP-to-AS-SIP Interworking function. When this IP signaling protocol is not SIP then the CCA performs a custom interworking role between the proprietary signaling protocol and AS-SIP.

In addition, the CCA interacts with the Media Interworking function to convey the IP addresses/UDP ports of the RTP streams of sessions established by the signaling plane as well as the SRTP master keys exchanged in the SDP bodies to the Media interworking function. When the sessions are terminated the CCA notifies the media interworking function so that the Media Interworking function ceases to interwork the media packets for the terminated sessions.

5.3.2.7.5.3.1.1.1 CCA IWF Component

As illustrated in Table 5.3.2.7-8, the role of the IWF within the CCA is to

1. Interwork the messages of the proprietary VoIP signaling protocol into AS-SIP signaling messages.

2. Interwork AS-SIP signaling messages into messages of the proprietary VoIP signaling protocol.

Table 5.3.2.7-8. IWF Signal Interworking Capabilities for AS-SIP IP Gateway

IWF INPUT PROTOCOL	IWF OUTPUT PROTOCOL	
	AS-SIP (TO AN EBC)	PV
AS-SIP (from an EBC)	*N/A*	Required
PV	Required	*N/A*

LEGEND:

AS-SIP	Assured Services Session Initiation Protocol	IWF	Inter Working Function
		N/A	Not Applicable
EBC	Edge Boundary Controller	PV	Proprietary VoIP

The CCA IWF MUST support the AS-SIP consistent with the detailed AS-SIP requirements in Section 5.3.4, AS-SIP Requirements.

The CCA IWF MUST secure the AS-SIP protocol using TLS, as described in UCR 2008, Section 5.4, Information Assurance Requirements.

The CCA IWF component of the AS-SIP IP Gateway MUST 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 proprietary UC signaling platform that the AS-SIP IP Gateway presents UCR-compliant call flows to the signaling appliances in the UC network per UCR Section 5.3.4.13.

5.3.2.7.5.3.1.2 AS Precedence Capability Requirements and Resource Priority Header

The AS-SIP IP Gateway does NOT conduct preemption.

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 MUST generate a Resource-Priority header having a ROUTINE priority level in accordance with Section 5.3.4.10.2 Precedence Level Communicated over SIP Signaling.

Whenever the AS-SIP IP Gateway receives an INVITE, UPDATE, or REFER request from the WAN SS/MFSS via the EBC, then the AS-SIP IP Gateway MUST process the Resource-Priority header to distinguish a ROUTINE call from a precedence call.

In the case of a ROUTINE call the AS-SIP IP Gateway follows the procedure in UCR requirement 5.3.2.7.5.1.3 above.

In the case of a precedence call, the AS-SIP IP Gateway follows the procedure in UCR requirement 5.3.2.7.5.1.4

5.3.2.7.5.3.1.3 SIP URI and Mapping of Telephone Number

When the AS-SIP IP Gateway receives a call request from the proprietary UC signaling platform, then the AS-SIP IP Gateway MUST map the telephony numbers received from the initial proprietary signaling message to SIP URIs in accordance with Section 5.3.4.14.3, SIP URI and Mapping of Telephony Number into SIP URI, and UCR Section 5.3.4.7.6 SIP URI and Mapping of Telephone Number into SIP URI.

5.3.2.7.5.3.1.4 Session Admission Control

5.3.2.7.5.3.1.4.1 The AS-SIP IP Gateway MUST conduct SAC as detailed in this section in place of the ASAC required of LSCs.

5.3.2.7.5.3.1.4.2 The AS-SIP IP Gateway MUST 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.

5.3.2.7.5.3.1.4.3 The AS-SIP IP Gateway MUST support code blocking. NOTE: Whenever the proprietary UC signaling platform supports code blocking then code blocking will be performed in the proprietary UC signaling platform and not in the AS-SIP IP Gateway.

5.3.2.7.5.3.1.4.4 The AS-SIP IP Gateway MUST support configuration of total voice call thresholds and total video call thresholds.
5.3.2.7.5.3.1.4.5 The AS-SIP IP Gateway MUST support configuration of outbound voice call thresholds, inbound voice call thresholds, outbound video call thresholds, and inbound video call thresholds.

5.3.2.7.5.3.1.4.6 Session Admission Control refers to the enforcement of voice and video session thresholds whereby the AS-SIP IP Gateway MUST:

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 WAN SS/MFSS that would exceed the appropriate (voice or video) call count threshold or inbound call count threshold.

c. Per Requirement 5.3.2.7.5.1.4, depending on the desired software configuration of the given AS-SIP IP Gateway either implement 5.3.2.7.5.1.4 a to divert all precedence INVITEs to the attendant or implement 5.3.2.7.5.1.4 b(1) if the INVITE would cause the appropriate (voice or video) call count threshold (or inbound call count threshold) to be exceeded and divert the precedence INVITE to the attendant.

5.3.2.7.5.3.1.4.7 Each time the AS-SIP IP Gateway receives a new voice call request the AS-SIP IP Gateway MUST conduct SAC as follows:

a. If the initial INVITE received from the WAN SS/MFSS via the EBC is “routine” and the AS-SIP IP Gateway is not enforcing directionalization,

   (1) If the voice call count is not at threshold, then increment the voice call count by one (the INVITE will be translated to proprietary signaling and sent to the proprietary UC signaling platform).

   (2) If the voice call count is at threshold then reject the INVITE.

b. If the initial INVITE received from the WAN SS/MFSS is “routine” and the AS-SIP IP Gateway is enforcing directionalization, then:

   (1) If the voice call count and inbound voice call count are not at threshold, then increment the voice call count by one and increment the inbound voice call count by one (the INVITE will be translated to proprietary signaling and sent to the proprietary UC signaling platform).

   (2) If either the voice call count or the inbound voice call count is at threshold, then reject the INVITE.

c. If the initial INVITE received from the WAN SS/MFSS is a precedence INVITE and the AS-SIP IP Gateway is not enforcing directionalization, then:

(1) If the AS-SIP IP Gateway is configured to divert all precedence INVITEs to the attendant per Requirement 5.3.2.7.5.1.4 a, then the INVITE is diverted to the attendant.

(2) If the AS-SIP IP Gateway is configured to process the precedence INVITE per 5.3.2.7.5.1.4 b, then:

(a) If the precedence INVITE would NOT cause the voice call count threshold to be exceeded, then increment the voice call count by one (the INVITE will be translated to proprietary signaling and sent to the proprietary UC signaling platform).

(b) If the precedence INVITE would cause the voice call count threshold to be exceeded then divert the precedence INVITE to the attendant

d. If the initial INVITE received from the WAN SS/MFSS is a precedence INVITE and the AS-SIP IP Gateway is enforcing directionalization, then:

(1) If the AS-SIP IP Gateway is configured to divert all precedence INVITEs to the attendant per 5.3.2.7.5.1.4 a, then the INVITE is diverted to the attendant

(2) If the AS-SIP IP Gateway is configured to process the precedence INVITE per 5.3.2.7.5.1.4 b, then

(a) If the precedence INVITE would NOT cause the voice call count threshold or the inbound voice call count threshold to be exceeded, then increment the voice call count by one and the inbound voice call count by one (the INVITE will be translated to proprietary signaling and sent to the proprietary UC signaling platform).

(b) If the precedence INVITE would cause the voice call count threshold or inbound voice call count threshold to be exceeded, then divert the precedence INVITE to the attendant.

e. If the call request is received from the proprietary UC signaling platform and the AS-SIP IP Gateway is not enforcing directionalization, then:

(1) If the voice call count is not at threshold, then increment the voice call count by one (the call request will be translated to an INVITE and sent to the WAN SS/MFSS).

(2) If the voice call count is at threshold then reject the INVITE.

f. If the call request is received from the proprietary UC signaling platform and the AS-SIP IP Gateway is enforcing directionalization, then:

(1) If the voice call count and outbound voice call count are not at threshold, then increment the voice call count by one and the outbound voice call count by one (the call request will be translated to an INVITE and sent to the WAN SS/MFSS).

(2) If either the voice call count or the outbound voice call count is at threshold, then reject the proprietary call request.

5.3.2.7.5.3.1.4.8 Each time the AS-SIP IP Gateway receives a new video session request, then the AS-SIP IP Gateway MUST conduct SAC as follows:

a. If the initial INVITE received from the WAN SS/MFSS is “routine” and the AS-SIP IP Gateway is not enforcing directionalization, then:

(1) If the video call count is NOT at threshold and the video bandwidth in the INVITE request would not cause the video call count to exceed threshold, then increment the video call count by the appropriate number of VSUs (the INVITE will be translated to proprietary signaling and sent to the proprietary UC signaling platform).

(2) If the video call count is at threshold or the video bandwidth in the INVITE request would cause the video call count to exceed threshold, then reject the INVITE.

b. If the initial INVITE received from the WAN SS/MFSS is “routine” and the AS-SIP IP Gateway is enforcing directionalization, then:

(1) If the video call count and inbound video call count are NOT at threshold and the video bandwidth in the INVITE request would not cause the video call count or the inbound video call count to exceed threshold, then increment the video call count and the inbound video call count by the appropriate number of VSUs (the INVITE will be translated to proprietary signaling and sent to the proprietary UC signaling platform).

(2) If the video call count or inbound video call count is at threshold or the video bandwidth in the INVITE would cause the video call count or inbound video call count to exceed threshold, then reject the INVITE.

c. If the initial INVITE received from the WAN SS/MFSS is a precedence INVITE and the AS-SIP IP Gateway is not enforcing directionalization, then:

(1) If the AS-SIP IP Gateway is configured to divert all precedence INVITEs to the attendant per Requirement 5.3.2.7.5.1.4 a, then the INVITE is diverted to the attendant.

(2) If the AS-SIP IP Gateway is configured to process the precedence INVITE per 5.3.2.7.5.1.4 b, then:

(a) If the video call count is NOT at threshold and the precedence INVITE would NOT cause the video call count threshold to be exceeded, then increment the video call count by the appropriate number of VSUs (the INVITE will be translated to proprietary signaling and sent to the proprietary UC signaling platform).

(b) If the precedence INVITE would cause the video call count threshold to be exceeded, then divert the precedence INVITE to the attendant.

d. If the initial INVITE received from the WAN SS/MFSS is a precedence INVITE and the AS-SIP IP Gateway is enforcing directionalization, then:

(1) If the AS-SIP IP Gateway is configured to divert all precedence INVITEs to the attendant per Requirement 5.3.2.7.5.1.4 a, then the INVITE is diverted to the attendant.

(2) If the AS-SIP IP Gateway is configured to process the precedence INVITE per Requirement 5.3.2.7.5.1.4 b, then:

(a) If the video call count and inbound video call count are NOT at threshold and the precedence INVITE would NOT cause the video call count threshold or the inbound video call count threshold to be exceeded, then increment the video call count and the inbound video call count by the appropriate number of VSUs (the INVITE will be translated to proprietary signaling and sent to the proprietary UC signaling platform).

(b) If the precedence INVITE would cause the video call count threshold or inbound video call count threshold to be exceeded, then divert the precedence INVITE to the attendant.

e. If the call request is received from the proprietary UC signaling platform and the AS-SIP IP Gateway is not enforcing directionalization, then:

(1) If the video call count is not at threshold and the video bandwidth in the call request would not cause the video call count to exceed threshold then increment the video call count by the appropriate number of VSUs (the call request will be translated to an INVITE and sent to the WAN SS/MFSS).

(2) If the video call count is at threshold or the video bandwidth in the call request would cause the video call count to exceed threshold then reject the call request.

f. If the call request is received from the proprietary UC signaling platform and the AS-SIP IP Gateway is enforcing directionalization, then:

(1) If the video call count and outbound video call count are not at threshold and the video bandwidth in the call request would not cause the video call count or the outbound video call count to exceed threshold, then increment the video call count and the outbound video call count by the appropriate number of VSUs (the call request will be translated to an INVITE and sent to the WAN SS/MFSS).

(2) If either the video call count or the outbound video call count is at threshold or the video bandwidth in the call request would cause the video call count or outbound video call count to exceed threshold, then reject the INVITE.

5.3.2.7.5.3.2 AS-SIP IP Gateway Media Interworking

Summary of Relevant Media Packet Requirements from other UCR Sections

The AS-SIP IP Gateway MUST support the audio Codecs in Section 5.3.2.6.1.2, Video Audio Codecs.

The AS-SIP IP Gateway MUST comply with Section 5.3.2.6.1.4, Voice over IP Sampling Standard, for the sampling rates.

The AS-SIP IP Gateway MUST support the audio and video Codecs as specified in Section 5.3.2.6.2.2, Video codecs (Including Associated Audio Codecs).

Media Interworking

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 MUST be interworked by the AS-SIP IP Gateway into UCR-compliant voice packets that MUST be sent to the EBC.

The enclave EBC MUST 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.

The AS-SIP IP Gateway MUST interwork the UCR-compliant voice media packets received from the EBC into the proprietary voice media packets used by the IP EIs, and then the proprietary voice media packets MUST 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 IP Gateway and the IP EIs.

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 MUST be interworked by the AS-SIP IP Gateway into UCR-compliant video packets that MUST be sent to the EBC.

The enclave EBC MUST 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.

The AS-SIP IP Gateway MUST interwork the UCR-compliant video media packets received from the EBC into the proprietary video media packets employed by the IP EIs and then the proprietary video media packets MUST 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 IP Gateway and the IP EIs.

5.3.2.7.5.3.3 Information Assurance Requirements

The AS-SIP IP Gateway MUST satisfy the Information Assurance requirements in Section 5.4 Information Assurance Requirements for a media gateway.

5.3.2.7.5.3.4 Service Requirements under Total Loss of WAN Transport Connectivity

Upon total loss of WAN transport the AS-SIP IP Gateway becomes incapable of exchanging signaling messages between the connected proprietary UC signaling platform and the UC WAN and incapable of exchanging interworked media packets between the EIs served by the proprietary UC signaling platform and the UC WAN. The immediate consequence is that the users on the existing voice and video sessions can no longer successfully send or receive media, and will go on-hook. The signaling termination messages (triggered by going on-hook) will fail to transit the WAN due to the loss of WAN transport. In addition, since the AS-SIP IP Gateway provides the only connectivity to the UC WAN for the proprietary UC signaling platform, the proprietary UC signaling platform loses the ability to establish new calls over the UC WAN until WAN connectivity is restored.

5.3.2.7.5.3.5 AS-SIP IP Gateway Management Function

NM Function

The following Generic Requirements for the NM function are applicable to the AS-SIP IP Gateway:

- Section 5.3.2.17.1, Voice and Video Network Management Domain
- Section 5.3.2.17.2, General Management Requirements

  NOTE: The AS-SIP IP Gateway MUST 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 IP Gateway MUST support at least one additional Ethernet interface for carrying signaling and media streams for VVoIP traffic.
- Section 5.3.2.17.3.1, Fault Management
- Section 5.3.2.17.3.2.1, Read-Write Access to CM Data by the RTS EMS
- Section 5.3.2.17.3.4.1, Near-Real-Time Network Performance Monitoring
- Section 5.3.2.17.3.4.2, Remote Network Management Commands (the LSC requirements apply to the AS-SIP IP Gateway with the exception of Section 5.3.2.17.3.4.2.6, Essential Service Protection and Section 5.3.2.17.3.4.2.14, PEI/GEI Origination Capability Control)
- Section 5.3.2.17.3.5, Security Management
- Section 5.3.2.17.4, Data Classification
- Section 5.3.2.17.5, Management of Appliance Software

- Requirement 5.3.2.18.1 and subrequirements

- Section 5.3.2.18.2, Management Requirements for the ASAC (use these requirements for SAC only)

- Section 5.3.2.18.3.1.1, CCA Support for Capacity Installation, but not including Section 5.3.2.18.3.1.1.1, MG-Related Configuration, and Section 5.3.2.18.3.1.1.2, SG-Related Data)

- Section 5.3.2.18.3.3, CCA Support for Fault Localization

- Section 5.3.2.18.3.4, CCA Support for Testing

5.3.2.7.5.3.6 AS-SIP IP Gateway Transport Interface Functions

The AS-SIP IP Gateway Transport Interface functions provide interface and connectivity functions with the ASLAN and its IP packet transport network. Examples of Transport Interface functions include the following:

- Network Layer functions: IP, IPSec where IPSec is used to protect NM IP packets

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

- LAN Protocols

The CCA interacts with Transport Interface functions by using them to communicate over the ASLAN with:

- The proprietary UC signaling platform
- The EBC (and through the EBC to the WAN SS/MFSS)

The Media interworking function interacts with Transport Interface functions to communicate over the ASLAN with:

- Each IP EI served by the proprietary UC signaling platform
- The EBC

5.3.2.7.5.3.7 AS-SIP IP Gateway-to-NMS Interface

The AS-SIP IP Gateway MUST provide an interface to the DISA NMS. The interface MUST consist of a 10/100-Mbps Ethernet connection as specified in Section 5.3.2.4.4, VVoIP NMS Interface Requirements.

5.3.2.7.5.3.8 Specific Functions/Features NOT Supported

Specifically noted, the AS-SIP IP Gateway does NOT support the following functions or requirements:

- A media server
- An RTS stateful firewall
- AS-SIP interfaces for voicemail and unified messaging

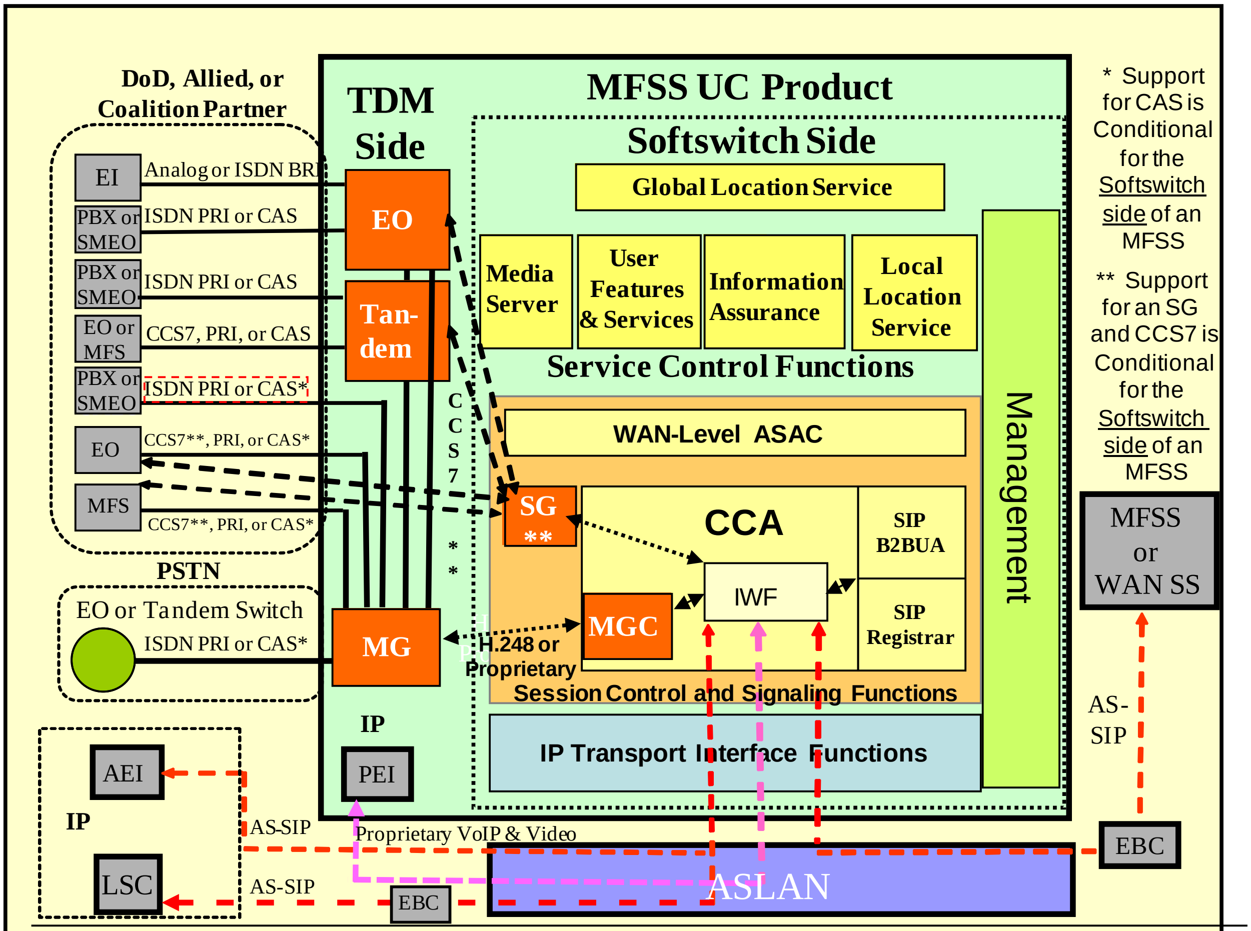
5.3.2.8 Network-Level Softswitches

The UC architecture defines the following two network-level SSs: the MFSS and the WAN SS. Network-level SSs are backbone devices that provide long-haul signaling between local service enclaves and other functions as described in Sections 5.3.2.8.1 through 5.3.2.8.4.

5.3.2.8.1 MFSS Functional Reference Model and Assumptions

The MFSS is a complex software-based call processing product that provides the full functionality of a TDM-based DSN MFS, and the full IP-based capabilities of an LSC with additional features, as required, to serve as a network-level SS. In summary, the MFSS consists of a TDM-based tandem function, a TDM-based EO function, and IP-based local and tandem functions.

Figure 5.3.2.8-1, Functional Reference Model – MFSS, shows the reference model for the MFSS. The boxes labeled “EO” and “Tandem” represent the TDM-based functions of the MFSS. The requirements for the TDM portion of the MFSS are entirely the same as for the MFS specified in UCR 2008, Section 5.2, Circuit-Switched Capabilities and Features.



LEGEND:

AEI	AS-SIP End Instrument
ASAC	Assured Service Admission Control
ASLAN	Assured Services Local Area Network
AS-SIP	Assured Services Session Initiation Protocol
BRI	Basic Rate Interface
B2BUA	Back-to-Back User Agent
CAS	Channel Associated Signaling
CCA	Call Connection Agent
CCS7	Common Channel Signaling No. 7
DoD	Department of Defense
EBC	Edge Border Controller
EI	End Instrument
EO	End Office
IA	Information Assurance
IP	Internet Protocol
ISDN	Integrated Services Digital Network
IWF	Interworking Function
LSC	Local Session Controller
MFS	Multifunction Switch
MFSS	Multifunction Softswitch
MG	Media Gateway
MGC	Media Gateway Controller
PBX	Private Branch Exchange
PEI	Proprietary End Instrument
PRI	Primary Rate Interface
PSTN	Public Switched Telephone Network
SCS	Session Control and Signaling
SG	Signaling Gateway
SIP	Session Initiation Protocol
SMEO	Small End Office
SS	Softswitch
SUT	System Under Test
TDM	Time Division Multiplexer
VoIP	Voice over Internet Protocol
WAN	Wide Area Network

Note: The PEI (using Proprietary VoIP and Video) is part of the MFSS UC Product; the AEI (using AS-SIP VoIP and Video) is not.

Figure 5.3.2.8-1. Functional Reference Model – MFSS

The IP functionality and features are provided by the MFSS component labeled “Softswitch Side.” The IP functionality is provided by several SCS functions performed by the CCA, IWF, MGC, MG, and SG. These are connected via proprietary internal interface functions.

Generic Requirements for the CCA, MG, and SG functions and NM are provided in separate sections of this documents as follows:

- Section 5.3.2.9, Call Connection Agent, including the CCA-associated IWF that applies to both the LSC and the MFSS
- Section 5.3.2.12, Media Gateway Requirements, including MG and MGC requirements
- Section 5.3.2.13, Signaling Gateway Requirements, including SG requirements
- Section 5.3.2.17, Management of Network Appliances, including NM requirements

5.3.2.8.1.1 Assumptions – MFSS

The following assumptions are made based on the MFSS reference model:

1. Interworking between the TDM side of the MFSS and the SS side of the MFSS is via proprietary internal interfaces. (The interfaces will require media conversion and may be implemented using any one of the MG options at the MFSS supplier's discretion.)

2. External connections from an MFSS APL product are as follows:

   a. Connections to other IP-based products (e.g., LSCs or MFSSs) use AS-SIP signaling

   b. Connections to other TDM-based products (e.g., MFS, EO, PBX, PSTN) use one of the following signaling interfaces: ISDN PRI, CCS7, or CAS

3. The role of the CCA in the MFSS is identical to the role of the CCA in the LSC (including the underlying assumptions, roles of the IWF and MGC, interactions with other LSC components, and VoIP and Video signaling interfaces), with the following exceptions and extensions:

   a. The CCA in the MFSS interacts with both LSC-Level ASAC and WAN-Level ASAC Policing. The MFSS supports LSC-Level ASAC for admission control for calls to and from PEIs and AEIs that it directly serves (through its internal LSC). The MFSS also supports WAN-Level ASAC Policing for admission control for calls to and from LSCs that it directly serves.

b. The CCA IWF in the MFSS is conditionally required to support interworking of the DoD CCS7 protocol with AS-SIP.

c. The CCA IWF in the MFSS is required to support interworking of the ISDN PRI protocol with AS-SIP.

4. The role of the MG in the MFSS is identical to the role of the MG in the LSC (including the underlying assumptions, roles of the MG and MGC, interactions with other LSC components, and VoIP signaling interfaces), with the following exceptions and extensions:

   a. The MG in the MFSS assists the MFSS CCA in providing call-denial treatments for CAC, and call-preemption treatments for LSC-Level ASAC and WAN-Level ASAC Policing.

   b. The MG in the MFSS is required to support ISDN PRI trunks.

   c. Support for CAS trunks is Conditional for the MG in the MFSS.

5. Figure 5.3.2.8-1, Functional Reference Model – MFSS, shows the MFSS supporting a single MG on a single ASLAN. A single MFSS also can support multiple MGs on multiple ASLANs, where those ASLANs are interconnected to form a MAN or COIN. In this arrangement, it is expected that the set of ASLANs forming the MAN or COIN can meet the single-ASLAN performance requirements in Section 5.3.1, Assured Services Local Area Network Infrastructure. In this case, the MFSS supports sessions between an MG on one ASLAN and a PEI, AEI, MG, or EBC on another ASLAN, as long as both ASLANs are part of the same MAN or COIN.

   Another way of stating this is that a single MFSS is able to support MGs at multiple physical locations. In some voice deployments, an MFSS in one location will serve ASLANs and EIs at distant locations, where both locations are part of the same regional MAN or COIN. In these cases, each distant ASLAN may want to have its own gateway to the local PSTN. In these cases, the MFSS supports MGs at multiple locations over MAN or COIN infrastructures that meet the ASLAN performance requirements in UCR 2008.

6. The MFSS and LSC are not required to support an SG. Support for an SG is Conditional for both the MFSS and LSC. As a result, the MFSS and LSC CCAs are not required to interact with the SG. As a result, support for an SG-CCA interface is Conditional for both the MFSS and LSC. The SG-CCA interface is viewed as an internal, unexposed interface within the MFSS or LSC, and can be based on proprietary protocols or on various SIGTRAN Protocols.

7. The TDM side of the MFSS provides Tandem and EO functions. Tandem functions in the MFSS provide circuit-switched network functions that terminate CCS7, PRI, and CAS type TDM trunks. The EO functions terminate ISDN and analog EIs. These EO and Tandem functions can interact with the SS side of the MFSS's CCA, MG, and SG through industry-standard external interfaces (e.g., CCS7 signaling links and TDM media trunks, as shown in Figure 5.3.2.8-1, Functional Reference Model – MFSS), or through internal interfaces that use protocols that are specific to a supplier's solution.

8. The MFSS supports Global Location Service functionality, and the LSC does not. The purpose of the Global Location Service is to provide the CCA with information on call routing and called address translation for calls that are directed outside of the MFSS (where a called address is contained within the SIP URI in the form of a called number). For example, the CCA uses the routing information stored in the Global Location Server (GLS) to:

    a. Route outgoing calls from MFSS EIs to other MFSSs and LSCs, and
    b. Route incoming calls from LSCs and other MFSSs to other LSCs and other MFSSs.

    However, the MFSS still uses the routing information stored in its LLS to route internal calls from one MFSS PEI or AEI to another, to route internal calls from an MFSS PEI or AEI to an MFSS MG (and vice versa), and to route incoming AS-SIP calls from another MFSS or LSC to local MFSS PEIs or AEIs.

9. The MFSS interactions with its EBC are different from the LSC interactions with its EBCs.

    a. In the LSC case, the EBC controls signaling streams between an LSC connected to an ASLAN and an MFSS where its separate ASLAN is connected to the DISN WAN. In this case, the EBC also controls media streams between LSC PEIs/AEIs and MGs connected to the ASLAN, and PEIs/AEIs and MGs on other LSCs where separate ASLANs are connected to the DISN WAN. The LSC accesses the DISN WAN via the LSC EBC and an associated PE Router on the DISN WAN. As a result, it is possible for an LSC MG to direct a VoIP media stream (interworked from a TDM media stream from the TDM side of that MG) through an EBC to the DISN WAN, and through the DISN WAN to a remote PEI, AEI, or MG.

    b. In the MFSS case, the EBC controls signaling streams between the MFSS where the EBC is connected to the DISN WAN and the LSCs that it serves, which are connected to the DISN WAN via their own EBCs and PE Routers. The MFSS EBC also controls signaling streams between the MFSS with its EBC connected to the DISN WAN and other MFSSs that it communicates with (with their own EBCs connected to the DISN WAN). As a result, the MFSS EBC is responsible for boundary control for both MFSS-LSC signaling and MFSS-MFSS signaling.

c. An LSC within an MFSS will serve a set of (MFSS-internal) LSC PEIs/AEIs and MGs. These LSC EIs and MGs will exchange media streams with EIs and MGs on other LSCs located elsewhere on the DISN WAN. In this case, the MFSS EBC also controls these media streams between the (MFSS-internal) LSC EIs and MGs connected to the MFSS ASLAN, and EIs and MGs on other LSCs where separate ASLANs are connected to the DISN WAN.

5.3.2.8.2 Summary of MFSS Functions and Features

The MFSS provides functions similar to the current DSN switching system referred to as an MFS, plus functions specified for an LSC with additional features, as required, to serve as a network-level SS.

5.3.2.8.2.1 TDM Side EO and Tandem Requirements

[Required: MFSS] The requirements for the TDM side of the MFSS are entirely the same as for the DSN MFS specified in UCR 2008, Section 5.2, Circuit-Switched Capabilities and Features.

The EO and Tandem functions allow the MFSS to support connectivity to existing TDM switches in DoD networks (i.e., continental United States (CONUS) and Global), allied and coalition networks, and the PSTN worldwide (i.e., CONUS and Global).

These functions allow the MFSS to connect via EO-based and Tandem-based TDM signaling links and TDM media trunks to DoD networks, allied and coalition networks, and PSTNs worldwide. These EO and Tandem functions extend the DoD CCS7, ISDN PRI, and CAS trunk capabilities for the MFSS CCA, MG, and SG.

In addition, the EO function of the MFSS supports both analog EIs and ISDN EIs (e.g., ISDN telephones served by ISDN BRIs, and ISDN PBXs served by ISDN PRIs). This allows the MFSS to support TDM users (i.e., analog and ISDN EIs) on its TDM EO side, and to separately support VoIP and Video users (i.e., AS-SIP and Proprietary VoIP/Video users) on its IP-based SS side.

5.3.2.8.2.2 Global Location Server

The GLS provides global location services and supports call routing where the called address points to a global destination (i.e., outside the MFSS) rather than a local destination (i.e., within the MFSS). A called address is contained within a SIP URI in the form of a called number. Section 5.3.2.10.9, CCA Interactions with Global Location Service, describes how the CCA uses routing information stored in the GLS to route calls between MFSS EIs and

- LSCs served by the MFSS
- Other MFSSs
- DoD TDM networks
- Allied TDM networks
- Coalition TDM networks
- PSTN (CONUS and Global)

However, the MFSS still uses the routing information stored in its LLS to

- Route internal calls from one MFSS PEI or AEI to another, and
- Route incoming calls to local MFSS PEIs or AEIs from
  - An LSC
  - Another MFSS
  - A DoD TDM network
  - An allied or coalition TDM network, or
  - The PSTN (CONUS and Global).

5.3.2.8.2.3 MFSS Signaling Interfaces

[Required: MFSS] The MFSS shall support PRI signaling for TDM communication with other systems.

[Required: MFSS] The TDM side of the MFSS shall support CCS7 signaling for communication with other TDM systems.

[Required: MFSS] The MFSS shall support AS-SIP signaling for IP communication with other MFSSs and LSCs.

[Required: MFSS] The MFSS shall provide internal signaling and media conversion for calls between the TDM side and SS side of the MFSS. The method used for the internal interface is left up to the supplier as long as all TDM-side MLPP and IP-side PBAS/ASAC requirements are met.

[Conditional: SS within the MFSS] The SS within the MFSS shall provide support for (and inclusion of) the SG. An SG supports CCS7 signaling. The condition here is that the interface between the TDM side and the SS side of the MFSS is considered internal to the MFSS product. The MFSS supplier may choose to include an SG as the internal interface between the TDM and SS sides in its MFSS product.

[Conditional: SS MG within the MFSS] The SS MG within the MFSS shall support CAS signaling as required by local implementations.

The MFSS supports the VoIP, Video, and CCS7 signaling interfaces shown in Table 5.3.2.8-1, MFSS Support for VoIP, Video, and CCS7 Signaling Interfaces.

Table 5.3.2.8-1. MFSS Support for VoIP, Video, and CCS7 Signaling Interfaces

FUNCTIONAL COMPONENT	VoIP AND VIDEO SIGNALING INTERFACES	VoIP AND VIDEO SIGNALING PROTOCOLS
CCA	CCA (MFSS) – to – CCA (LSC)	AS-SIP over IP
CCA	CCA (MFSS) – to – CCA (Other MFSS)	AS-SIP over IP
CCA	CCA (MFSS) – to – MFSS PEI (details outside the scope of this section)	Proprietary VoIP over IP (details outside the scope of this section)
CCA	CCA (MFSS) – to – MFSS AEI	AS-SIP over IP
CCA/MGC and MG	MFSS CCA (MGC) – to – MFSS MG	ITU-T H.248 over IP (used with DoD CCS7, ISDN PRI, and CAS trunks) **[Objective, not Required]**
CCA/MGC and MG	MFSS CCA (MGC) – to – MFSS MG	ISDN PRI over IP (North American National ISDN Version, used with ISDN PRI trunks only) **[Objective, not Required]**
CCA/MGC and MG	MFSS CCA (MGC) – to – MFSS MG	Proprietary Supplier Protocols (used with DoD CCS7, ISDN PRI, and CAS trunks)
CCA and SG (SG Conditional)	MFSS CCA – to – MFSS SG	DoD CCS7 over IP (used with DoD CCS7 trunks)
CCA and SG (SG Conditional)	MFSS CCA – to – MFSS SG	Proprietary Supplier Protocols (used with DoD CCS7 trunks)
CCA, SG, and EO (SG Conditional)	MFSS CCA – to – MFSS SG – to – MFSS EO	CCS7 ISUP and TCAP
CCA, SG, and Tandem (SG Conditional)	MFSS CCA – to – MFSS SG – to – MFSS Tandem	CCS7 ISUP and TCAP

LEGEND

AEI	AS-SIP End Instrument
AS-SIP	Assured Services Session Initiation Protocol
CAS	Channel Associated Signaling
CCA	Call Connection Agent
CCS7	Common Channel Signaling No. 7
DoD	Department of Defense
PEI	Proprietary End Instrument
EO	End Office
IP	Internet Protocol
ISDN	Integrated Services Digital Network
ISUP	ISDN User Part
ITU-T	International Telecommunications Union – Telecommunication
LSC	Local Session Controller
MFSS	Multifunction Softswitch
MG	Media Gateway
MGC	Media Gateway Controller
PEI	Proprietary End Instrument
PRI	Primary Rate Interface
SG	Signaling Gateway
TCAP	Transaction Capabilities Application Part
VoIP	Voice over IP

5.3.2.8.2.4 SG and MG Requirements for Interactions between the TDM Side and SS Side of the MFSS

[Required] The CCA/SG/MGC/MG complex in the SS side of the MFSS needs to interface and interact with the EO and Tandem functions in the TDM side of the MFSS. The interaction required to support intra-MFSS calls will be accomplished using the following requirements:

1. "MFSS internal connections" are used between the IP-based SS side and the TDM side of the MFSS to provide media conversion and signaling internal to the MFSS as an APL product SUT.

2. The MFSS will use one of the following MG/SG appliances for the internal MFSS connections:

    a. **[Required]** The MFSS MG must support internal MG connections that interconnect the SS side of the MFSS with the EO and Tandem functions on the TDM side of the MFSS.

    b. **[Required]** The MFSS MG shall interact with the MFSS MGC so that Internal MG connections between the SS and TDM sides of the MFSS support

        (1) Intra-MFSS calls between TDM EIs connected to the TDM side, and PEIs/AEIs connected to the SS side of the MFSS

        (2) Incoming and outgoing calls to/from systems external to the MFSS that require conversion between TDM and IP

[Conditional] When a DoD CCS7-based connection is used between the SS and TDM sides of the MFSS, the MFSS MG shall interact with the MFSS MGC so that DoD CCS7 signaling is used between the SS and TDM sides, and the CCS7 version of the MLPP feature operates correctly between the SS and TDM sides of the MFSS, for both VoIP-to-TDM calls and TDM-to-VoIP calls over this connection.

[Required] When a U.S. ISDN PRI-based connection is used between the SS and TDM sides of the MFSS, the MFSS MG shall interact with the MFSS MGC so that U.S. ISDN PRI signaling (National ISDN PRI signaling with the Precedence Level IE and related MLPP IEs included) is used between the softswitch and TDM sides, and the T1.619/T1.619a version of the ISDN PRI MLPP feature operates correctly between the SS and TDM sides of the MFSS, for both VoIP-to-TDM calls and TDM-to-VoIP calls over this trunk group.

[Conditional] When a U.S. CAS-based connection is used between the SS and TDM sides of the MFSS, the MFSS MG shall interact with the MFSS MGC so that

- U.S. CAS trunk signaling is used between the SS and TDM sides, and

- The DoD version of the CAS Trunk MLPP feature as specified in UCR 2008, Section 5.2, Circuit-Switched Capabilities and Features, operates correctly between the SS and TDM sides of the MFSS, for both VoIP-to-TDM calls and TDM-to-VoIP calls over this trunk group.

5.3.2.8.2.5 Requirements for External Connections between MFSS and Other Systems

Calls between the MFSS and a distant-end system will be either TDM based or IP based, as follows:

1. The TDM EO or TDM Tandem component of the MFSS will connect to another MFSS or EO using TDM-based trunks.

2. The SS side of an MFSS will connect to the SS side of a distant-end MFSS, or a distant-end (subtending) LSC using AS-SIP and IP transport.

5.3.2.8.2.6 Features of the SS Side of the MFSS

The following feature requirements apply to the SS side of the MFSS:

1. **[Required]** The SS side of the MFSS shall meet all the requirements for MLPP, as appropriate for VoIP and Video over IP services, as specified in Section 5.2.2, Multilevel Precedence and Preemption.

2. **[Required]** The SS side of the MFSS shall support CND as specified in UCR 2008, Section 5.2.3.5.1.8.2, Calling Number Delivery.

3. **[Required]** The requirements for SCS functions (i.e., CCA, IWF, MG, MGC, and SG) and NM are provided in separate sections of this document as follows:

   a. Section 5.3.2.9, Call Connection Agent, including the CCA-associated IWF that applies to both the LSC and the MFSS

   b. Section 5.3.2.12, Media Gateway Requirements, including MG and MGC requirements

   c. Section 5.3.2.13, Signaling Gateway Requirements, including SG requirements

   d. Section 5.3.2.17, Management of Network Appliances, including NM requirements

5.3.2.8.2.7 ASAC Requirements for the MFSS Related to Voice and Video

The ASAC requirements are specified in Section 5.3.2.2.2.3, ASAC – Open Loop.

5.3.2.8.3 Network Management Requirements for the MFSS

[Required] The NM requirements for the TDM side of the MFSS are specified in UCR 2008, Section 5.2.8, Network Management.

[Required] The NM requirements for the SS side of the MFSS are specified in UCR 2008, Section 5.3.2.17, Management of Network Appliances; Section 5.3.2.18, Network Management Requirements of Appliance Functions; and Section 5.3.2.19, Accounting Management.

5.3.2.8.3.1 Network Management System Interface

[Required: MFSS] The MFSS shall provide a single, common interface to the DISA NMS. The single interface shall provide access to MFSS features and functions for both the TDM and SS side of the MFSS.

[Required: MFSS] The MFSS-to-NMS interface shall be an Ethernet connection as specified in Section 5.3.2.4.4, VVoIP NMS Interface Requirements.

5.3.2.8.4 WAN-Level Softswitch

[Required: WAN SS] The WAN SS is a standalone APL product that acts as an AS-SIP B2BUA within the UC architecture. It provides the equivalent functionality of a commercial SS and has similar functionality to the SS component of an MFSS. Support for the functionality of the LSC is a Conditional requirement, and the support of an SG is not required. The inclusion of the product in the UC architecture allows the functionality of an MFSS to be achieved by interconnecting two separate appliances (e.g., MFS and WAN SS), possibly provided by different vendors. The creation of a WAN SS provides Government flexibility in the rollout of UC VVoIP capabilities and eases the migration of TDM technology-based services to IP technology-based services. The product shall provide the following functional components as shown in Figure 5.3.2.8-2, Functional Reference Model – WAN SS:

1. **[Required]** Section 5.3.2.8.2.2, Global Location Server.

2. **[Conditional]** Section 5.3.2.7, Local Session Controller.

3. **[Required]** Section 5.3.2.9, Call Connection Agent, including the CCA-associated IWF that applies to both the MFSS and the **[Conditional]** LSC.

4. **[Required]** Section 5.3.2.10.12, CCA Interactions with Service Control Functions that addresses media servers.

5. **[Required]** Section 5.3.2.2.2.3.1.2, ASAC Requirements for the MFSS Related to Voice, and Section 5.3.2.2.2.3.2, 5.3.2.2.2.3.2 ASAC Requirements for the LSC and the MFSS Related to Video Services. These sections address WAN-Level ASAC Policing requirements.

6. **[Required]** Section 5.3.2.12, Media Gateway Requirements, 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. **[Conditional: ISDN T1.619A PRIs; Required: Commercial PRIs (ANSI Version)]** the Non-Facility Associated Signaling (NFAS) feature of the U.S. National ISDN documents.

7. **[Required]** Section 5.3.2.17, Management of Network Appliances, including NM requirements.

8. **[Required]** Section 5.3.2.18, Network Management Requirements of Appliance Functions, including NM requirements for the CCA and the MG, but not for the SG.

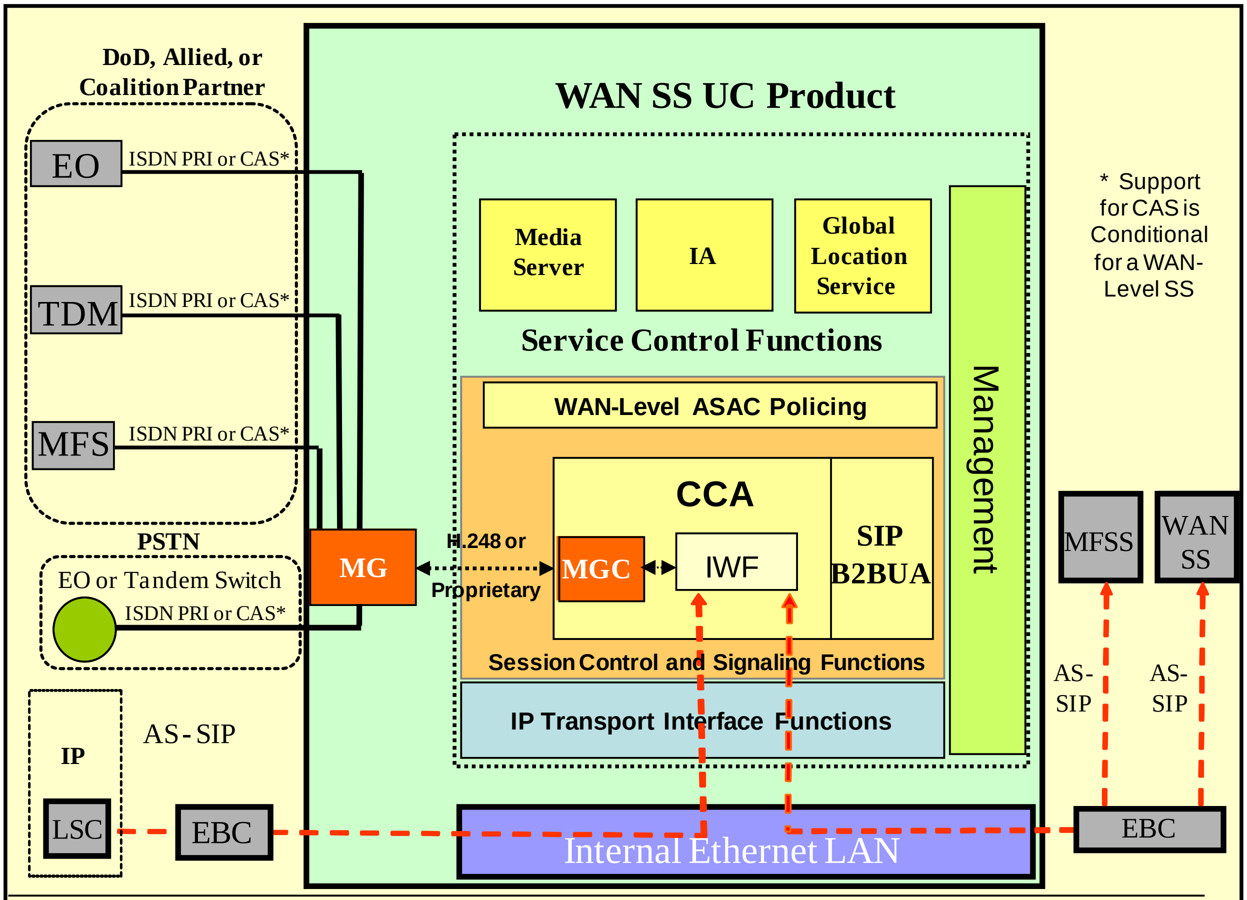
9. **[Required]** Section 5.3.2.7.2.7, LSC Transport Interface Functions, which addresses the IP Transport Interface functions.

10. **[Required]** Section 5.3.2.5.2, Product Quality Factors.

11. **[Required]** Section 5.3.4, AS-SIP Requirements.

12. **[Required]** Section 5.4, Information Assurance Requirements, for MFSS, MG, and **[Conditional]** LSC.

13. **[Conditional]** The MG of the WAN SS shall also support an OC-3 physical interface for transport of multiplexed PRI trunk groups between 1) the WAN SS and MFSs in the DISA TDM network, and 2) the WAN SS and EOs in the commercial TDM network (in the case where the WAN SS contains an LSC, and the LSC 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., National ISDN-2 (ni-2) PRI trunk groups in the US). 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.



LEGEND:

ASAC	Assured Service Admission Control	MFSS	Multifunction Softswitch
AS-SIP	Assured Services Session Initiation Protocol	MG	Media Gateway
B2BUA	Back-to-Back User Agent	MGC	Media Gateway Controller
CAS	Channel Associated Signaling	OC-3	Optical Carrier Level 3
CCA	Call Connection Agent	PBX	Private Branch Exchange
CCS7	Common Channel Signaling No. 7	PRI	Primary Rate Interface
DoD	Department of Defense	PSTN	Public Switched Telephone Network
EBC	Edge Border Controller	SCS	Session Control and Signaling
EO	End Office	SG	Signaling Gateway
IA	Information Assurance	SIP	Session Initiation Protocol
IP	Internet Protocol	SS	Softswitch
ISDN	Integrated Services Digital Network	SUT	System Under Test
IWF	Interworking Function	TDM	Tandem (Switch)
LAN	Local Area Network	UC	Unified Capabilities
LSC	Local Session Controller	WAN	Wide Area Network
MFS	Multifunction Switch		

Figure 5.3.2.8-2. Functional Reference Model – WAN SS

The major differences between the WAN SS and the SS part of the MFSS are:

1. The WAN SS does not need to contain an LSC, but may do so as a Conditional capability if the acquisition agent and vendor so desire.

2. The WAN SS does not require an SG (it is neither Required nor Conditional).

3. The WAN SS MG is only required to support ISDN T1.619A PRI trunks to the MFS. If the Conditional LSC is supported, the WAN 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).

4. The NM EMS for the WAN SS should be provided as a standalone EMS separate from the MFS EMS.

5. The WAN SS MG(s) may be remotely located from the MGC within the CCA of the WAN SS.

6. The WAN 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 Router via an EBC.

NOTE: When using and testing the requirements of the previous applicable sections (and throughout the entire UCR 2008), it is necessary to interpret them in light of the major differences between the WAN SS and the SS part of the MFSS from above. When requirements within these sections refer to the SS part of the MFSS, they are required for the WAN SS. When requirements refer to the MFS part of the MFSS, or interconnection/interoperation with the MFS (including the EO), they no longer apply to the WAN SS. The only connections required between the WAN SS MG and the MFS are ISDN T1.619A PRI and commercial PRI, in accordance with 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 a Conditional requirement for T1.619A PRIs and a Requirement for U.S. commercial PRIs.

5.3.2.9 Call Connection Agent

5.3.2.9.1 Introduction

This section provides Generic Requirements for the CCA function in the following network appliances:

- LSC
- MFSS
- WAN SS

Each of these appliances has a DISN-defined design that includes Session Control and Signaling functions. These functions include both a Signaling Protocol IWF and a Media Gateway Controller function.

The CCA described in the following requirements is part of the SCS functions, and includes both the IWF and the MGC. As a result, the scope of these CCA requirements covers the following areas:

1. Control of AS-SIP sessions within the network appliance, including:

   a. AS-SIP sessions from/to AEIs served by an LSC or MFSS appliance (NOTE: Proprietary protocol sessions from/to LSC PEIs and MFSS PEIs are supported also.)

   b. AS-SIP sessions from/to LSCs served by an MFSS appliance

   c. AS-SIP sessions between MFSS appliances (where sessions span multiple MFSSs)

2. Support for the following PSTN and VoIP signaling protocols:

   a. AS-SIP

   b. DoD CCS7, including MLPP

   c. ISDN PRI (North American National ISDN version), including MLPP

   d. PSTN CAS, for DTMF and MF trunks (North American version)

   e. Protocol interworking of the previous signaling protocols (for example, AS-SIP ⇔ DoD CCS7 interworking) through the CCA IWF

3. Control of MGs that link the network appliance with TDM NEs through the CCA MGC in the following:

   a. DoD networks
   b. Allied and coalition networks
   c. PSTN in CONUS
   d. PSTN Global (i.e., outside the continental United States (OCONUS))

4. CCA support for interactions with other network appliance functions, including:

   a. SG
   b. Admission control
   c. The following Service Control functions:

      (1) Media servers
      (2) UFS

(3) Information Assurance
(4) Local Location Service

d. Appliance Management functions
e. GLS (in the MFSS only)
f. EBCs

5. CCA support for voice calls and video calls

6. CCA support for Voice and Video services features and capabilities

[Required: LSC, MFSS] A CCA in an MFSS or LSC shall be able to support multiple MGs on a single ASLAN.

[Required: LSC, MFSS] A CCA in an MFSS or LSC shall be able to support multiple MGs on multiple ASLANs, where those ASLANs are interconnected to form a MAN or COIN. In this arrangement, it is expected that the set of ASLANs forming the MAN or COIN will meet the single-ASLAN performance requirements in Section 5.3.1, Assured Services Local Area Network Infrastructure. In this case, the LSC shall support sessions between an MG on one ASLAN and an PEI, AEI, MG, or EBC on another ASLAN, as long as both ASLANs are part of the same MAN or COIN.

[Required: LSC, MFSS] A CCA in an MFSS or LSC shall be able to support MGs at multiple physical locations. In some deployments, an LSC in one location will serve ASLANs and EIs at distant locations, where both locations are part of the same regional MAN or COIN. In these cases, each distant ASLAN may want to have its own gateway to the local PSTN. In these cases, the LSC shall support MGs at multiple locations over MAN or COIN infrastructures that meet the ASLAN performance requirements in the UCR 2008.

5.3.2.9.2 Functional Overview of the CCA

Figure 5.3.2.9-1, CCA Relationships, illustrates the relationship between the CCA and other functional components. As indicated in the figure, the IWF, MGC, and SG are contained within a CCA. However, it is permissible for the SG to be in an external network appliance.

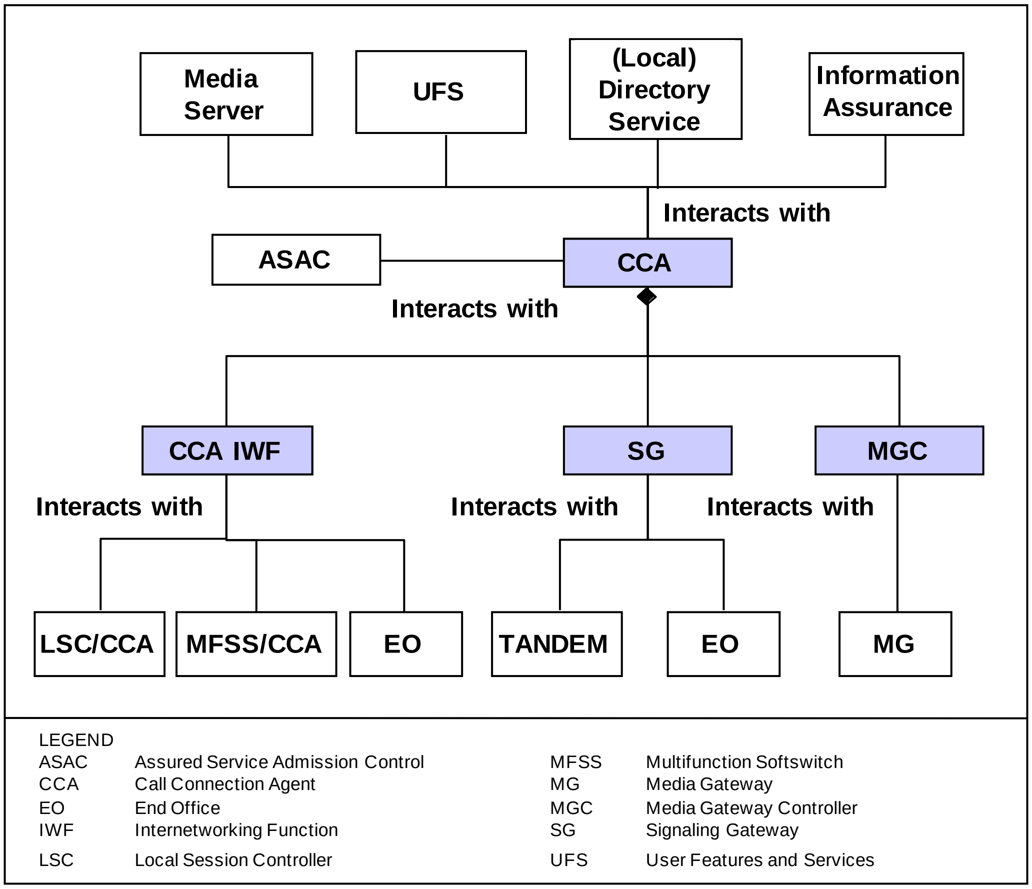

Media Server
UFS
(Local) Directory Service
Information Assurance
Interacts with
ASAC
CCA
Interacts with
CCA IWF
SG
MGC
Interacts with
Interacts with
Interacts with
LSC/CCA
MFSS/CCA
EO
TANDEM
EO
MG
LEGEND
ASAC Assured Service Admission Control
CCA Call Connection Agent
EO End Office
IWF Internetworking Function
LSC Local Session Controller
MFSS Multifunction Softswitch
MG Media Gateway
MGC Media Gateway Controller
SG Signaling Gateway
UFS User Features and Services

Figure 5.3.2.9-1. CCA Relationships

The role of a CCA is to provide session control for all VoIP sessions and Video over IP sessions that are originated by, or terminated in, the voice network. These VoIP and Video sessions can be established using SIP, a Proprietary VoIP protocol, AS-SIP, or some combination of these (e.g., SIP and AS-SIP on an PEI-or-AEI/LSC/EBC/MFSS session). The CCA takes on the role of the SIP B2BUA in the traditional SIP architecture.

In addition, the CCA takes on the role of a SIP Registrar for all PEIs, AEIs, MGs, and EBCs served by the LSC, allowing PEIs, AEIs, MGs, and EBCs 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 EBC that is active on the LSC at any moment in time.

In addition to acting as a SIP B2BUA, the CCA is responsible for providing call control and feature control for VoIP and Video over IP network-based calls and features. Most VoIP and Video over IP features that are provided to LSC PEI and AEI end users, on either a per-call basis or an all-calls basis, are controlled by the CCA.

5.3.2.9.2.1 CCA IWF Component

The role of the IWF within the CCA is to

- Support all the VoIP and TDM signaling protocols that the LSC supports for EIs, MGs, and EBCs, and

- Interwork all these various signaling protocols with one another.

Specifically, this section requires the CCA IWF to support the following VoIP and TDM signaling protocols:

- [Required: LSC, MFSS, AEI] AS-SIP

- **[Conditional: LSC]** Proprietary VoIP (for PEIs on the EI-LSC interface; this is conditional and may include supplier-specific SIP, supplier-specific H.323, and other supplier-proprietary protocols)

- **[Conditional: LSC, MFSS]** DoD CCS7, including MLPP (for SG/MG trunks; North America Version Conditional; and European or other foreign PRI version Conditional when required by the DoD user)

- **[Required: LSC, MFSS]** The ISDN PRI, including MLPP (for MG trunks; North American version Required; and European or other foreign PRI version Conditional when required by the DoD user)

- Facility Associated Signaling (FAS) is required for T1.619A PRIs, and NFAS is conditional for T1.619A PRIs.

- Both FAS and NFAS are Required for commercial PSTN PRIs, for access to the US PSTN.

- **[Conditional: LSC, MFSS]** CAS, including MLPP (for MG trunks; North American version Conditional; European or other foreign CAS trunk version Conditional when required by the DoD user)

5.3.2.9.2.2 CCA MGC Component

The role of the MGC within the CCA is to

1. Control all MGs within the LSC or MFSS.

2. Control all trunks (e.g., DoD CCS7, PRI, CAS) within each MG:

    a. **[Required: LSC, MFSS]** Support for DoD ISDN trunks
    b. **[Conditional: LSC, MFSS]** Support for CAS trunks

3. Control all signaling and media streams on each trunk within each MG.

4. Accept IP-encapsulated signaling streams from an SG or MG, and return IP-encapsulated signaling streams to the SG or MG accordingly.

    - This approach is used for CCS7 signaling to/from an SG **[Conditional in both the MFSS and LSC cases]**, and for PRI signaling to/from an MG.

5. Within the LSC, use either ITU-T Recommendation H.248 or a supplier-proprietary protocol to accomplish these controls.

The MGC and the MG that it controls are considered Conditional – Deployable for the LSC. The SG is considered Conditional for the LSC.

5.3.2.9.2.3 SG Component

The role of the CCA with respect to the SG in the network appliance is to

1. Control all SGs within the network appliance.

2. Control all signaling links (DoD CCS7) within each SG.

[Required: MFSS – Conditional: LSC] The CCA shall be responsible for controlling all the SGs within the MFSS and LSC. (This covers cases where there is a single SG within the network appliance, and cases that are more complex where there are multiple SGs within the network appliance.)

[Required: MFSS – Conditional: LSC] The CCA shall be responsible for controlling each signaling link within each SG within the MFSS or LSC.

[Required: MFSS – Conditional: LSC] The CCA shall be responsible for controlling the DoD CCS7 signaling stream(s) within each signaling link within each SG.

[Required: MFSS – Conditional: LSC] Within the network appliance (i.e., MFSS and LSC), the CCA shall use either an IETF-standard set of CCS7-over-IP protocols, or a supplier-proprietary protocol to accomplish the above SG, signaling link, and signaling stream controls.

5.3.2.9.3 CCA Requirements Assumptions

The following assumptions were used to develop VoIP and Video over IP requirements for the CCA:

1. Definitions of terms are given in Appendix A, Section A2, Glossary and Terminology Description.

2. The network supports voice and video services and features. Support for other services, such as messaging and unified messaging, is not required in the Voice and Video network design initially.

3. The network consists of voice and video APL products that are supported over a converged IP transport network. The APL products include the LSC, MFSS, EBC, CE Router, and terrestrial transport products. Intersystem communication between these products and associated appliance functions is accomplished by VoIP and Video communication (e.g., use of AS-SIP signaling packets and SRTP media packets) over an underlying IP network layer and IP-based transport layer, such as UDP or TCP.

4. The LSC is assumed to be a local APL product located in a local domain (B/P/C/S).

5. The EBC functions are assumed to be external to the LSC and MFSS. The EBC functions are Session Border Controller (SBC)-type functions and firewall-type functions that are provided by network appliances.

6. The CCA requirements in this section support voice and video call control for originating, terminating, and tandem calls, as well as the following end-user features: Call Hold, Call Waiting, Precedence Call Waiting, Call Forwarding, Call Transfer, Hotline Service, and Calling Party and Called Party ID (number only).

7. The CCA requirements in this section support PBAS/ASAC.

8. The CCA requirements in this section assume that CCA call routing decisions are based on call routing data provided by the LLSs and GLSs (other functional components within the LSC and MFSS). How this routing data is established within these Location Servers and/or obtained at these Location Servers is beyond the scope of these CCA requirements.

9. The MFSS is assumed to support AS-SIP connectivity for connections to other MFSSs and LSCs, and TDM connectivity for connections to other MFSSs and DoD TDM switches. The TDM connectivity can use CCS7, PRI, or CAS signaling.

10. The LSC is assumed to include an MGC and an MG **[Required: Fixed – Conditional: Deployable]**, and an SG (Conditional). This means that the TDM trunk groups that terminate on the LSC MG can use PRI, CAS, or CCS7 signaling.

11. The MFSS supports end users on both the SS side (i.e., VoIP end users using VoIP EIs), and on the TDM side (i.e., traditional end users with traditional DoD telephones).

12. The MFSS also supports TDM trunk group and CCS7 signaling links on both the VoIP side (through the MGC, MG, and SG [SG Conditional]) and the TDM side (through the EO and Tandem Switch).

13. The VoIP signaling protocol used between the VoIP EI and the LSC, and between the VoIP EI and the LSC part of an MFSS, can be vendor proprietary. The VoIP signaling protocol does not need to be AS-SIP between a VoIP PEI and LSC, or between the VoIP PEI and the LSC component of an MFSS. The VoIP signaling protocol used between the AEI and the LSC, and between the AEI and the LSC part of an MFSS, must be AS-SIP. The VoIP signaling protocol used between signaling appliances (i.e., LSC and MFSSs) is required to be AS-SIP.

14. The LSC and the MFSS will both use Location Services (Local or Global, as needed) to route calls to their intended destination. Location Services will be supported as an internal function of the LSC or MFSS, instead of an external function that the LSC or MFSS would have to access over an external interface using an industry-standard Location Services protocol.

15. It is assumed that route selections at the LSCs and the MFSS will be based on the originating call signaling type (i.e., either IP or TDM signaling). If the originating signaling is IP based, it is assumed that the call signaling will stay IP based for as long as possible as the signaling transits the network. Similarly, if the originating call signaling is TDM based, it is assumed that the call signaling will stay TDM based for as long as possible as the signaling transits the network.

16. The LSC and the MFSS will use SIP URIs for addressing and routing, and will not use “tel” URIs for this purpose. See Table 5.3.2.9-1, An E.164 and a DSN Number, Expressed as a SIP URI and a tel URI, for an example of an E.164 and a DSN number, expressed as a SIP URI and a tel URI.

Table 5.3.2.9-1. An E.164 and a DSN Number, Expressed as a SIP URI and a tel URI

TELEPHONE NUMBER	TELEPHONE NUMBER AS SIP URI	TELEPHONE NUMBER AS tel URI
+17327582000 (an E.164 number in the United States)	sip:+17327582000@uc.mil; user=phone	tel: +17327582000; user=phone
3144305353 (a DSN number at the Patch Barracks in Germany)	sip:3144305353; phone-context=uc.mil @uc.mil; user=phone (Support for the phone-context tag is an objective.)	tel: 3144305353; phone-context=uc.mil; user=phone (Support for the phone-context tag is an objective.)

17. Tones and announcements that are provided to VoIP end users will be provided from an internal media server, which is a functional component of the LSC or MFSS. An external media server that is separate from the LSC or MFSS is not envisioned.

18. See UCR 2008, Section 5.3.2.2.2.2, Public Safety Features, for a description of 911 call handling.

19. In some cases, a function like an MGC or MG will be labeled as Conditional – Deployable in this section. In these cases, Conditional – Deployable means that normally this function is not used in a Deployable environment, but may be used in that environment under certain conditions. When this function is used in that environment, the function should conform to the MGC requirements in this section. For example, an LSC deployed in one camp in a war zone overseas may not use an MGC or an MG, while another LSC deployed in another camp in the same zone may use both of them.

20. The CCA VoIP and Video over IP requirements in this section assume that all the functions within an individual appliance (i.e., LSC or MFSS) are provided by the same appliance supplier. Within a collection of network appliances, all the appliances may be provided by the same supplier, or some appliances may be provided by one supplier and other appliances may be provided by other suppliers.

21. Interoperability between LSCs and MFSSs is the goal of the UCR 2008 and the CCA requirements in this section. Integration between the functions within an individual LSC or MFSS is the responsibility of the network appliance supplier.

22. The LSC supports MGC and MG functionality, so that LSCs can support access to DoD TDM networks, allied TDM networks, coalition partner TDM networks, and the local PSTN, when this access is needed in both Fixed and Deployable environments. In addition, the LSC supports MGC and MG functionality to enable TDM connectivity (i.e., PRI, CAS, and CCS7 trunks and signaling links) to interconnecting MFSSs when it is needed.

23. “Voice and Video Assured Services” supports VoIP, Voice band FoIP, VBD MoIP, SCIP over IP, and Video over IP. The voice budgets used to manage end users’ VoIP calls will collectively manage those users’ VoIP calls, FoIP calls, MoIP calls, and SCIP-over-IP calls. The separate video budgets used to manage end users’ Video-over-IP calls will manage those users’ Video-over-IP calls only, and will not manage any VoIP, FoIP, MoIP, or SCIP-over-IP calls for those users. In short, VoIP budgets and Video-over-IP budgets are maintained and managed separately in Voice and Video Assured Services.

24. The LSCs and MFSSs providing Assured Services Voice and Video will support proprietary VoIP videophones (using the vendor’s version of SIP or H.323). The LSC and MFSS suppliers should also support AS-SIP videophones. The LSC and MFSS suppliers are required to support protocol interworking between their videophones (Proprietary VoIP and AS-SIP) and the AS-SIP protocol used on network-side interfaces between LSCs and MFSSs (and between LSCs and between MFSSs).

25. The VoIP signaling protocol used between the VoIP EI and the LSC (and between the VoIP EI and the LSC part of an MFSS) can be vendor proprietary. The VoIP signaling protocol does not need to be AS-SIP between a VoIP PEI and LSC (or between the VoIP PEI and the LSC component of an MFSS). The VoIP signaling protocol used between the AEI and the LSC, and between the AEI and the LSC part of an MFSS, must be AS-SIP. The VoIP signaling protocol used between signaling appliances (i.e., LSCs and MFSSs) is required to be AS-SIP.

5.3.2.9.4 Role of the CCA in Network Appliances

The role of the CCA is to provide session control for all VoIP sessions and Video over IP sessions that are originated by or terminated by EIs on the LSC. These VoIP and Video sessions can be established using either of the following:

- [Conditional] AS-SIP or
- **[Conditional]** A Proprietary VoIP protocol

The CCA takes on the role of a SIP B2BUA in the traditional SIP architecture.

The CCA takes on the role of a SIP Registrar for all EIs, MGs, and EBCs served by the LSC, allowing EIs, MGs, and EBCs to register their SIP URIs (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 EBC that is active on the LSC at any time.

The CCA is responsible for providing call control and feature control for all VoIP and Video–over-IP calls and features that the LSC provides. All VoIP and Video-over-IP calls that are originated by or answered by LSC PEI and AEI end users are controlled by the CCA. All VoIP and Video-over-IP features that are provided to LSC 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 LSC, the CCA includes an IWF and an MGC, and the MGC controls all the TDM interfaces served by the MG (DoD CCS7 trunks, ISDN PRI trunks, and CAS trunks (i.e., DTMF and MF)). This section reviews the role of the CCA in the LSC and MFSS reference models, and covers the role of the CCA, IWF, and MGC in each case.

5.3.2.9.5 CCA-IWF Signaling Protocol Support Requirements

This section describes the requirements for the CCA Signaling Protocol IWF to support the various VoIP and TDM signaling protocols used in the LSC and MFSS. In summary, the role of the IWF within the CCA is to support all the VoIP and TDM signaling protocols that are used by the EIs, MGs, and EBCs, and interwork all these various signaling protocols with one another.

5.3.2.9.5.1 CCA-IWF Support for AS-SIP

[Required: LSC, MFSS] The CCA IWF shall support the AS-SIP protocol consistent with the detailed AS-SIP protocol requirements in Section 5.3.4, AS-SIP Requirements.

[Required: LSC, MFSS] The CCA IWF shall use the AS-SIP protocol on LSC-MFSS and MFSS-MFSS sessions.

[Required: LSC, MFSS] When the CCA IWF uses the AS-SIP protocol over the Access Segment between the EBC and the DISN WAN, or over the DISN WAN itself, the CCA IWF shall secure the AS-SIP protocol using TLS, as described in Section 5.4, Information Assurance Requirements.

5.3.2.9.5.2 CCA-IWF Support for DoD CCS7 via an SG

[Conditional: LSC, MFSS] The CCA IWF shall support the DoD CCS7 protocol, consistent with the detailed DoD CCS7 protocol requirements in the following DoD and ANSI documents:

- UCR 2008, Section 5.2.2, Multilevel Precedence and Preemption, including
  - UCR 2008, Section 5.2.2.4.3, Common Channel Signaling Number 7
  - UCR 2008, Section 5.2.2.9, MLPP CCS7
  - UCR 2008, Section 5.2.4.6, Common Channel Signaling Number 7
- ANSI T1.619-1992 (R2005)

- ANSI T1.619a-1994 (R1999)

[Conditional: LSC, MFSS] When used in the European Theater and in other OCONUS ETSI-compliant countries, the CCA IWF shall support the ITU-T Recommendation Q.735.3 MLPP extensions to the ITU-T CCS7 protocol, consistent with the UCR 2008 and ITU-T Recommendation Q.735.3.

[Conditional: LSC, MFSS] The CCA IWF shall support reception of DoD CCS7 messages from the SG, and transmission of DoD CCS7 messages to the SG, as described in this document. The CCA IWF shall support securing of DoD CCS7 messages to and from the SG, as described in Section 5.4, Information Assurance Requirements.

[Conditional: LSC, MFSS] The CCA IWF shall be able to determine the DoD CCS7 signaling link that a CCS7 message was sent or received on (and the MG CCS7 trunk group associated with this signaling link), when processing a CCS7 message sent or received at the SG.

[Conditional: LSC, MFSS] The CCA IWF shall be able to support multiple DoD CCS7 signaling links at the SG, where each CCS7 signaling link is connected to a different CCS7 end point (i.e., to a different DoD Signaling Transfer Point (STP), a DoD TDM switch, another MFSS, or another LSC).

[Conditional: LSC, MFSS] The CCA IWF shall be able to differentiate between the individual DoD CCS7 signaling links at the SG. The CCA IWF shall know, as part of its configuration data, which DoD STP, DoD TDM switch, other MFSS, or other LSC each SG signaling link is connected to.

[Conditional: LSC, MFSS] In conjunction with the SG, the CCA IWF shall support DoD CCS7 signaling links to

- TDM switches and STPs in the DoD TDM network
- MFSSs and LSCs in the DoD network
- TDM switches and STPs in allied and coalition partners (when those STPs support DoD CCS7)
- TDM EO and Tandem switch components of the MFSS itself

[Conditional: LSC, MFSS] The CCA IWF shall be able to associate individual CCS7 link, ISDN User Part (ISUP), and Transaction Capabilities Application Part (TCAP) configuration data with each individual CCS7 link served by the SG and the CCA. The CCA IWF shall not require groups of CCS7 links served by the SG and the CCA to share “common” link, ISUP, and TCAP configuration data.

[Conditional: LSC, MFSS] As part of this CCS7 configuration data, the CCA IWF shall know the identity of the CCS7 device at the far end of each CCS7 signaling link. Specifically, the CCA IWF shall know the identity of each interconnected

- TDM switch and STP in the DoD TDM network
- MFSS and LSC in the DoD network
- TDM switch and STP in each allied and coalition partner
- TDM EO and Tandem switch component in the MFSS itself

5.3.2.9.5.3 CCA-IWF Support for PRI, via MG

[Required: LSC, MFSS] The CCA IWF shall support the U.S./National ISDN version of the ISDN PRI protocol, consistent with the detailed ISDN PRI protocol requirements in the following DoD and ANSI documents:

1. UCR 2008, Section 5.2.9, Integrated Services Digital Network, including Table 5.2.9-4, PRI Access, Call Control, and Signaling, and Table 5.2.9-5, PRI Features.

    a. The “MFS” column in these tables shall apply to the MFSS.
    b. The “PBX1” and “PBX2” columns in these tables shall apply to the LSC.

2. UCR 2008, Section 5.2.2, Multilevel Precedence and Preemption, including:

    a. UCR 2008, Section 5.2.4.2, Line Signaling
    b. UCR 2008, Section 5.2.2.7, ISDN MLPP PRI

3. ANSI T1.619-1992 (R2005).

4. ANSI T1.619a-1994 (R1999).

    a. Facility Associated Signaling is required for T1.619A PRIs, and NFAS is Conditional for T1.619A PRIs.

    b. Both FAS and NFAS are Required for commercial PSTN PRIs, for access to the U.S. PSTN.

[ETSI PRI: Required – Other Foreign PRIs: Conditional] The appliance supplier (i.e., LSC or MFSS supplier) has the option of supporting one or more foreign versions of the ISDN PRI protocol on 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 include:

1. ETSI standards on the use of ISDN PRI in European countries (and other countries that also support ETSI PRI standards)

2. Japanese Telecommunication Technology Committee (TTC) and South Korean Telecommunication Technology Association (TTA) standards on the use of ISDN PRI in Japan and South Korea, respectively

3. ITU-T standards on the use of ISDN PRI worldwide (in countries that only support ITU-T standards)

   NOTE: The ISDN-PRI/AS-SIP interworking requirements in this document only apply to the U.S. version of ISDN PRI. 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 LSC or MFSS is used in the European Theater or in other OCONUS ETSI-compliant countries.

[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 2008 and ITU-T Recommendation Q.955.3.

[Required: LSC, MFSS] The CCA IWF shall support reception of ISDN PRI messages from the MG and transmission of ISDN PRI messages to the MG.

[Required: LSC, MFSS] The CCA IWF shall be able to determine the ISDN PRI (and its D-Channel signaling link) that an incoming PRI message was received on, when processing an incoming PRI message from the MG.

[Required: LSC, MFSS] The CCA IWF shall be able to identify the ISDN PRI (and its D-Channel signaling link) that an outgoing PRI message will be sent on, when generating an outgoing PRI message to the MG.

[Required: LSC, MFSS] The CCA IWF shall be able to support multiple ISDN PRIs (and their D-Channel signaling links) at the MG, where each PRI is connected to a different PRI end point (e.g., to a different DoD PBX, DoD TDM switch, MFSS, LSC, PSTN PBX, or PSTN TDM switch).

[Required: LSC, MFSS] The CCA IWF shall be able to differentiate between the individual ISDN PRIs (and their D-Channel signaling links) at the MG. The CCA IWF shall know, as part of its configuration data, which DoD PBX, DoD TDM switch, MFSS, LSC, PSTN PBX, or PSTN TDM switch each ISDN PRI (and its D-Channel signaling link) is connected to.

[Required: LSC, MFSS] In conjunction with the MG, the CCA IWF shall support ISDN PRIs (and D-Channel signaling links) to

- TDM PBXs and switches in the DoD network (This includes the TDM EO and Tandem components of the local MFSS, in the MFSS CCA/MG case.)

- MFSSs and LSCs in the DoD network

- TDM PBXs and switches in the U.S. PSTN

- TDM PBXs and switches in allied and coalition partner networks (when those networks support U.S. “National ISDN” PRI)

[Required: LSC, MFSS] The CCA IWF shall support the full set of ISDN MLPP requirements in ANSI T1.619 and ANSI T1.619a, including the following from ANSI T1.619:

- Precedence level
- Cause
- Notification Indicator
- Signal
- Call Identity
- Information elements in ISDN PRI messages, on ISDN PRIs to

  – TDM PBXs in the DoD TDM network

  – TDM switches in the DoD TDM network (This includes the TDM EO and Tandem components of the local MFSS, in the MFSS CCA/MG case.)

  – MFSSs in the DoD network

  - LSCs in the DoD network

[Required: LSC, MFSS] The CCA IWF shall not support any of the ISDN MLPP requirements in ANSI T1.619 and ANSI T1.619a, on ISDN PRIs to TDM PBXs and switches in the U.S. PSTN.

In other words, the MLPP feature and its associated ISDN PRI signaling shall be supported on ISDN PRIs from the CCA/MG to PBXs and switches in the DoD TDM network (or to appliances in the network), but shall not be supported on ISDN PRIs from the CCA/MG to PBXs and switches in the U.S. PSTN.

[Required: LSC, MFSS] On ISDN PRIs from the CCA/MG to TDM PBXs and switches in allied and coalition partners (where those networks support U.S. "National ISDN" PRI), the CCA IWF shall support a DoD-user-configurable per-PRI option that allows the PRI to support or not support the ANSI T1.619/619a PRI MLPP feature on calls to and from that PRI.

[ETSI PRI: Required – Other Foreign PRIs: Conditional] When the appliance supplier supports a foreign ISDN PRI on 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

- TDM PBXs and switches in the PSTN in that foreign country

- TDM PBXs and switches in allied and coalition partner networks (where those networks support the ISDN PRI used in the home country of the allied or coalition partner)

Support for ETSI PRI is required when the LSC or MFSS is used in the European Theater or in other OCONUS ETSI-compliant countries.

[Required: LSC, MFSS] The CCA IWF shall be able to associate individual PRI configuration data with each individual PRI served by the MG and the CCA. The CCA IWF shall not require groups of PRIs served by the MG and the CCA to share "common" PRI configuration data.

5.3.2.9.5.4 CCA-IWF Support for CAS Trunks, via MG

[Conditional] The CCA IWF (with the MG) shall support the U.S. version of CAS trunks and trunk signaling, consistent with the CAS trunk and trunk signaling requirements in the following DoD documents:

- DoD UCR 2008, Section 5.2.4, Signaling, including

  - UCR 2008, Section 5.2.4.3, Trunk Supervisory Signaling
  - UCR 2008, Section 5.2.4.4, Control Signaling
  - UCR 2008, Section 5.2.4.5, Alerting Signals and Tones

- DoD UCR 2008, Section 5.2.2, Multilevel Precedence and Preemption, including

  - Section 5.2.2.4.1, Channel Associated Signaling

  - Section 5.2.2.9, MLPP CCS7, CAS-to-CCS7 trunk interworking in a mixed media network

[Conditional] The appliance supplier (i.e., LSC or MFSS supplier) has the option of supporting one or more foreign versions of CAS trunks and trunk signaling on 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:

- ETSI standards on the use of CAS trunks in European countries (and other countries that also support ETSI CAS trunk standards)

- Japanese TTC and South Korean TTA standards on the use of CAS trunks in Japan and South Korea, respectively

- ITU-T standards on the use of CAS trunks worldwide (in countries that only support ITU-T standards)

NOTE: The CAS trunk/AS-SIP interworking requirements in this document only apply to the U.S. version of CAS trunks. The CAS trunk/AS-SIP interworking requirements for foreign versions of CAS trunks (i.e., European, Japanese, South Korean) are outside the scope of this document.

[Conditional] The CCA IWF shall support reception of CAS signaling sequences (i.e., Supervisory, Control, and Alerting) from the MG, and transmission of CAS signaling sequences to the MG.

[Conditional] The CCA IWF shall be able to determine the MG CAS trunk and CAS trunk group that an incoming CAS signaling sequence was received on when processing an incoming CAS signaling sequence from the MG.

[Conditional] The CCA IWF shall be able to identify the MG CAS trunk and CAS trunk group that an outgoing CAS signaling sequence will be sent on when generating an outgoing CAS signaling sequence to the MG.

[Conditional] The CCA IWF shall be able to support multiple CAS trunk groups at the MG, where each CAS trunk group is connected to a different end point (e.g., to a different DoD PBX, DoD TDM switch, MFSS, LSC, PSTN PBX, or PSTN TDM switch).

[Conditional] The CCA IWF shall be able to differentiate between the individual CAS trunk groups at the MG. The CCA IWF shall know, as part of its configuration data, which DoD PBX, DoD TDM switch, MFSS, LSC, PSTN PBX, or PSTN TDM switch each CAS trunk group is connected to.

[Conditional] In conjunction with the MG, the CCA IWF shall support CAS trunk groups to

- TDM PBXs and switches in the DoD TDM network (This includes the TDM EO and Tandem components of the local MFSS, in the MFSS CCA/MG case.)

- MFSSs and LSCs in the DISN

- TDM PBXs and switches in the U.S. PSTN

- TDM PBXs and switches in allied and coalition networks (where those networks support U.S. CAS trunk groups)

[Conditional] The CCA IWF shall support the MLPP signaling requirements for CAS trunk groups in UCR 2008, Section 5.2.2.4.1, Channel Associated Signaling. This MLPP signaling support shall include the following four cases:

- Answered call, Trunk to be reused
- Unanswered call, Trunk to be reused
- Answered call, Trunk not to be reused
- Unanswered call, Trunk not to be reused

[Conditional] When the IWF is the appliance sending the preemption request over the CAS trunk group, the CCA IWF shall generate the measured supervisory signal (preemption signal) causing trunk circuit disconnect, with the following four variations:

- Answered call, Trunk to be reused
- Unanswered call, Trunk to be reused
- Answered call, Trunk not to be reused
- Unanswered call, Trunk not to be reused

[Conditional] When the IWF is the appliance receiving the preemption signal over the CAS trunk group, the CCA IWF shall be able to receive and act on the measured supervisory signal (preemption signal) causing trunk circuit disconnect, with the following four variations:

- Answered call, Trunk to be reused
- Unanswered call, Trunk to be reused
- Answered call, Trunk not to be reused
- Unanswered call, Trunk not to be reused

[Conditional] When the IWF is the appliance receiving the preemption request over the CAS trunk group, the CCA IWF shall generate the Preempt warning tone to the CCA-served party on the preempted call (e.g., a VoIP EI served by the CCA that is active on the preempted call).

[Conditional] When the IWF is the appliance receiving the preemption request over the CAS trunk group, the CCA IWF shall detect the Returned disconnect signal from the CCA-served party on the preempted call, and remove the Preempt warning tone from the party after this detection.

[Conditional] The CCA IWF shall support the CAS MLPP signaling as described earlier on CAS trunk groups to

- TDM PBXs and switches in the DoD TDM network (This includes the TDM EO and Tandem components of the local MFSS, in the MFSS CCA/MG case.) and

- MFSSs and LSCs in the DISN

[Conditional] The CCA IWF shall not use the CAS MLPP signaling described earlier on CAS trunk groups to TDM PBXs and switches in the U.S. PSTN.

In other words, the MLPP feature and its associated CAS signaling shall be supported on CAS trunk groups from the CCA/MG to PBXs and switches in the DoD TDM network (or to appliances in the network), but shall not be supported on CAS trunk groups from the CCA/MG to PBXs and switches in the U.S. PSTN.

[Conditional] On CAS trunk groups from the CCA/MG to TDM PBXs, and in allied and coalition partners (where those networks support U.S. CAS trunks), the CCA IWF shall support a DoD-user-configurable per-CAS trunk group option that allows the CAS trunk group to either

- Support the UCR 2008 CAS MLPP feature on calls to and from that trunk group, or
- Not support the UCR 2008 CAS MLPP feature on calls to and from that trunk group.

When the "Support" option is configured, the CCA IWF shall support the CAS MLPP feature for allied and coalition partner calls on that trunk group.

When the "Not Support" option is configured, the CCA IWF shall not support the CAS MLPP feature for allied and coalition partner calls on that trunk group.

[Conditional] When the appliance supplier supports foreign CAS trunk groups on its product, the CCA IWF, along with the MG, shall support CAS trunk groups to

- TDM PBXs and switches in the PSTN in a foreign country, and
- TDM PBXs and switches in allied and coalition partner networks (where those networks support the CAS trunk groups used in the home country of the allied or coalition partner).

[Conditional] The CCA IWF shall be able to associate individual CAS trunk group configuration data with each individual CAS trunk group served by the MG and the CCA. The CCA IWF shall not require groups of CAS trunk groups served by the MG and the CCA to share "common" CAS trunk group configuration data.

[Conditional] As part of this CAS trunk group configuration data, the CCA IWF shall know the identity of the CAS device at the far end of each CAS trunk group. Specifically, the CCA IWF shall know

- The identity of each interconnected TDM PBX and switch in the TDM portion of the network (This includes the TDM EO and Tandem components of the local MFSS, in the MFSS CCA/MG case.)
- The identity of each interconnected MFSS and LSC in the DISN
- The identity of each interconnected TDM PBX and switch in the U.S. PSTN

- The identity of each interconnected TDM PBX and switch in each allied and coalition partner network (when that network supports U.S. CAS trunk groups)

[Conditional] When the appliance supplier supports foreign CAS trunk groups on 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

- The identity of each interconnected TDM PBX and switch in the foreign PSTN

- The identity of each interconnected TDM switch in the foreign PSTN

- The identity of each interconnected TDM PBX and switch in each allied and coalition partner network (when that network supports the foreign CAS trunk group of the allied or coalition partner's home country)

NOTE: These "foreign" CAS trunk group requirements are included to support DoD users in interconnecting their MFSSs and LSCs with the networks of foreign PSTNs, U.S. Allies, and U.S. Coalition Partners using CAS trunk groups. Detailed requirements for support of foreign CAS trunk groups are outside the scope of this document.

5.3.2.9.5.5 CCA-IWF Support for PEI and AEI Signaling Protocols

[Required: LSC, MFSS] The CCA IWF shall support supplier-proprietary Voice and Video EIs and their associated proprietary EI signaling protocols. Proprietary EI signaling protocols, which may include a supplier's version of SIP or H.323, are permitted.

[Required] The CCA IWF shall support the following Voice and Video EIs, and their associated EI signaling protocols:

- **[Objective]** Voice and Video SIP EIs
- **[Objective]** Voice and Video H.323 EIs
- **[Required]** Voice and Video AS-SIP EIs

[Conditional] When the CCA IWF supports Voice and Video SIP EIs, the IWF shall support these EIs using the set of IETF SIP and SDP RFCs listed in Section 5.3.4, AS-SIP Requirements.

[Conditional] When the CCA IWF supports Voice and Video H.323 EIs, the IWF shall support these EIs using ITU-T Recommendation H.323.

NOTE: An LSC or MFSS ASLAN may support two different types of Voice and Video H.323 EIs:

- H.323 EIs that are served by an H.323 Gatekeeper, which is completely separate from the CCA and its IWF, and

- H.323 EIs that are served by the CCA and its IWF (where the CCA IWF is, effectively, an H.323 Gatekeeper for these EIs).

In the first case, the H.323 EIs are completely independent of the CCA, MG, SG, and EBC. It is possible in this case for an H.323 EI on the local ASLAN to set up an H.323 Voice or Video call with another H.323 EI on a remote ASLAN (located elsewhere on the DISN WAN), without using any AS-SIP, and without affecting any of the AS-SIP Voice or Video budgets that are used at LSCs or MFSSs.

This first case is an "H.323 Overlay Network" case and is outside the scope of this document.

In the second case, the H.323 EIs are dependent on the CCA, MG, SG, and EBC for interworking with TDM voice networks, for interworking with AS-SIP, and for gaining access to the DISN WAN. When an H.323 EI on the local ASLAN makes an H.323 Voice or Video call to another H.323 EI on a remote ASLAN in this case, the "calling LSC" does H.323/AS-SIP protocol conversion, the called LSC does AS-SIP/H.323 protocol conversion, and the call is treated as an AS-SIP session (with resulting Voice or Video budget impacts) between the calling LSC, the called LSC, and any intermediate MFSSs.

This second case, while unusual, is an "H.323/AS-SIP Interworking" case, and is within the scope of this document, with one major qualification. The CCA and IWF's use of AS-SIP in this interworking case is within the section's scope. The details on how the supplier's CCA and IWF perform the protocol interworking between EI H.323 and CCA AS-SIP are outside this section's scope.

[Conditional] When the CCA IWF supports Voice and Video AS-SIP EIs, the IWF shall support these EIs using the set of AS-SIP protocol requirements in UCR 2008, Section 5.3.4, AS-SIP Requirements (AS-SIP EIs are Required for 2010.).

5.3.2.9.5.6 CCA-IWF Support for VoIP and TDM Protocol Interworking

Per Section 5.3.2.9.2.1, CCA IWF Component, the role of the IWF within the CCA is to support all the VoIP and TDM signaling protocols that the appliance supports for PEIs, AEIs, MGs, and EBCs, and interwork all these various signaling protocols with one another.

The requirements in this section support the IWF's interworking of the various VoIP and TDM signaling protocols together. Table 5.3.2.9-2, Full IWF Interworking Capabilities for VoIP and TDM Protocols, summarizes the various interworking capabilities that the appliance is required to support.

Table 5.3.2.9-2. Full IWF Interworking Capabilities for VoIP and TDM Protocols

IWF INPUT PROTOCOL	IWF OUTPUT PROTOCOL					
	AS-SIP (TO AN AEI)	AS-SIP (TO AN EBC)	PV	DOD CCS7	ISDN PRI	CAS
AS-SIP (from an AEI)	*No interworking needed*	Required	Required if PV is supported	Conditional (for MFSS)	Required	Conditional
AS-SIP (from an EBC)	Required	*No interworking needed*	Required if PV is supported	Conditional (for MFSS)	Required	Conditional
PV	Required if PV is supported	Required if PV is supported	*No interworking needed*	Conditional if PV is supported	Required if PV is supported	Conditional
DoD CCS7	Conditional (for MFSS)	Conditional (for MFSS)	Conditional if PV is supported	*No interworking needed*	Conditional (for MFSS) (per UCR 2007)	Conditional
ISDN PRI	Required	Required	Required if PV is supported	Conditional (for MFSS) (per UCR 2007)	*No interworking needed*	Conditional
CAS	Conditional	Conditional	Conditional	Conditional	Conditional	*No interworking needed*

LEGEND:

AEI	Generic End Instrument	ISDN	Integrated Services Digital Network
AS-SIP	Assured Services Session Initiation Protocol	MFSS	Multifunction Softswitch
CAS	Channel-Associated Signaling	PRI	Primary Rate Interface
CCS7	Common Channel Signaling No. 7	PV	Proprietary VoIP
DoD	Department of Defense	SG	Signaling Gateway
EBC	Edge Boundary Controller	UCR	Unified Capabilities Requirements

[Required: FY2011] This section covers the interworking of six VoIP and TDM "input" protocols (i.e., AS-SIP on AEIs, Proprietary VoIP on PEIs, AS-SIP on EBCs, DoD CCS7 on SGs, ISDN PRI on MGs, and CAS trunks on MGs) with six VoIP and TDM "output" protocols (i.e., AS-SIP on AEIs, Proprietary VoIP on PEIs, AS-SIP on EBCs, DoD CCS7 on SGs, ISDN PRI on MGs, and CAS trunks on MGs).

Ruling out cases where the "input" and "output" protocols are the same, and combining cases where interworking between input protocol "A" and output protocol "B" also covers interworking between input protocol "B" and output protocol "A", this leaves 15 separate protocol interworking cases that need to be addressed. The number of cases is further complicated because

1. Depending on whom they are connected to, ISDN PRIs can connect network appliances to either U.S. ISDN networks or foreign ISDN networks, and can either support or not support MLPP.

2. Depending on whom they are connected to, CAS trunks can connect network appliances to U.S. TDM networks or foreign TDM networks, and can either support or not support MLPP.

3. An ISDN PRI or CAS trunk may be used to connect a network appliance to the U.S. PSTN, a foreign PSTN, a point in the worldwide DoD TDM network or DoD network, an allied TDM network, or a coalition partner TDM network.

As a result, this section addresses a wide variety of protocol interworking cases. All cases included are believed to be relevant to DoD networks worldwide.

In the following requirements, interworking is only required where the network appliance supplier supports both the AS-SIP protocol and the other protocol in the requirement.

[Required] When they are present in the network appliance, the CCA IWF shall interwork the protocols for the following cases, which shall include support for both Voice and Video AEIs, unless noted otherwise:

- AS-SIP protocol via AS-SIP AEIs with the supplier's proprietary VoIP EI protocol

- **[Conditional: LSC, MFSS]** AS-SIP protocol via AS-SIP AEIs with the DoD CCS7 protocol

- AS-SIP protocol via AS-SIP AEIs with the U.S. ISDN PRI protocol

- **[Required: ETSI PRI – Conditional: Other Foreign PRIs]** AS-SIP protocol via AS-SIP AEIs with the appropriate foreign ISDN PRI protocol.

- **[Conditional]** AS-SIP protocol via AS-SIP AEIs with the U.S. CAS trunk protocol

- **[Conditional]** AS-SIP protocol via AS-SIP AEIs with the appropriate foreign CAS trunk protocol

[Required] When they are present in the network appliance, the CCA IWF shall interwork the protocols for the following cases, which shall include support for both VoIP and Video PEIs, unless noted otherwise:

- **[Conditional: LSC, MFSS]** Proprietary VoIP EI protocol with the DoD CCS7 protocol
- Proprietary VoIP EI protocol with the U.S. ISDN PRI protocol
- **[Required: ETSI PRI – Conditional: Other Foreign PRI]** Proprietary VoIP EI protocol with the appropriate foreign ISDN PRI protocol
- **[Conditional]** Proprietary VoIP EI protocol with the U.S. CAS trunk protocol
- **[Conditional]** Proprietary VoIP EI protocol with the appropriate foreign CAS trunk protocol

[Required] When they are present in the network appliance, the CCA IWF shall interwork the protocols for the following cases, which shall include both VoIP and Video PEIs, unless noted otherwise:

- AS-SIP protocol via EBCs with the supplier's Proprietary VoIP EI protocol
- **[Conditional: LSC, MFSS]** AS-SIP protocol via EBCs with the DoD CCS7 protocol
- AS-SIP protocol via EBCs with the U.S. ISDN PRI protocol
- **[Required: ETSI PRI – Conditional: Other Foreign PRI]** AS-SIP protocol via EBCs with the appropriate foreign ISDN PRI protocol
- **[Conditional]** AS-SIP protocol via EBCs with the U.S. CAS trunk protocol
- **[Conditional]** AS-SIP protocol via EBCs with the appropriate foreign CAS trunk protocol

5.3.2.9.6 CCA Preservation of Call Ringing State during Failure Conditions

[Required: LSC, MFSS, WAN SS] The CCA in the LSC, MFSS, and WAN SS shall not allow AS-SIP sessions that have reached the ringing state (i.e., an AS-SIP 180 (Ringing) message or 183 (Session Progress) has been sent from the called party to the calling party, and the calling party is receiving an audible ringing tone) to fail when an internal failure occurs within the CCA. (As used here, "internal failure" includes cases where one component of the CCA fails, and a failover occurs within the CCA so that a second redundant component is brought into service to replace the first failed component.) Instead, the CCA shall ensure that the "call ringing state" is preserved (rather than dropped) at both the calling party interface (where audible ringing tone is being returned to the caller) and the called party interface (where incoming call alerting is being provided to the called party).

5.3.2.10 CCA Interaction with Network Appliances and Functions

This section describes how the CCA interacts with network appliances and appliance functions. These other appliance functions include the following:

- ASAC
- Service Control functions
- NM (FCAPS and audit logs)
- Transport Interface functions
- EBC (not part of the LSC, but part of the local assured services domain).

5.3.2.10.1 CCA Interactions between the SS and TDM Sides of the MFSS

The CCA/SG/MGC/MG complex in the MFSS must provide Interoperability between the SS side and the TDM side in the MFSS (using connections based on CCS7, U.S. PRI, or U.S. CAS signaling at the discretion of the vendor). In this case, some high-level requirements for this interworking are needed. These high-level requirements are included in this section.

[Required] The MFSS CCA shall be able to support MG connections between the SS side of the MFSS and the EO and Tandem functions on the TDM side of the MFSS.

[Conditional] When a DoD CCS7 connection is used between the SS and TDM sides of the MFSS, the MFSS CCA shall control the MG function and its associated SG signaling link so that

- DoD CCS7 signaling is used between the SS and TDM sides, and

- The CCS7 version of the MLPP feature operates correctly between the SS and TDM sides of the MFSS for both VoIP-to-TDM calls and TDM-to-VoIP calls over this trunk group.

[Required] When a U.S. ISDN PRI connection is used between the SS and TDM sides of the MFSS, the MFSS CCA shall control the MG function so that

- U.S. ISDN PRI signaling (national ISDN PRI signaling, with the Precedence Level IE and related MLPP IEs included) is used between the SS and TDM sides, and

- The ANSI T1.619/T1.619a version of the ISDN PRI MLPP feature operates correctly between the SS and TDM sides of the MFSS for both VoIP-to-TDM calls and TDM-to-VoIP calls over this trunk group.

[Conditional] When a U.S. CAS connection is used between the SS and TDM sides of the MFSS, the MFSS CCA shall control the MG function so that

- U.S. CAS trunk signaling is used between the SS and TDM sides, and

- The UCR 2008 version of the CAS trunk MLPP feature operates correctly between the SS and TDM sides of the MFSS for both VoIP-to-TDM calls and TDM-to-VoIP calls over this trunk group.

[Required] The MFSS CCA shall use MG connections between the SS and TDM sides of the MFSS to support

- The TDM calls between the TDM EO/Tandem and IP EIs on the MFSS, allowing calls between EO lines and IP EIs, and calls between EO and Tandem trunks and MFSS EIs.

- The TDM calls between the TDM EO/Tandem and the EBC on the MFSS, allowing calls between EO lines and other appliances on the DISN WAN, and calls between EO and Tandem trunks and other appliances on the DISN WAN.

- The TDM calls between the TDM EO/Tandem and other MG trunk groups on the MFSS, allowing calls between EO lines and these trunk groups, and calls between EO and Tandem trunks and these trunk groups.

5.3.2.10.2 CCA Support for Appliance Management Functions

Requirements for CCA support for Appliance Management functions are found in UCR 2008, Section 5.3.2.18.1, Management Requirements of the CCA Function.

5.3.2.10.3 CCA Interactions with Transport Interface Functions

The Transport Interface functions in an appliance provide interface and connectivity functions with the ASLAN and its IP packet transport network. High-level requirements for these functions are outlined in this section. The detailed implementation methods for these requirements are left up to each vendor. Examples of Transport Interface functions include:

- Network Layer functions: IP and IPSec
- Transport Layer functions: TCP, UDP, Stream Control Transmission Protocol (SCTP), TLS
- LAN protocols

The CCA interacts with Transport Interface functions by using them to communicate with PEIs, AEIs, the EBC, the MGs, and the SG over the ASLAN. The following appliance elements are all IP end points on the ASLAN:

- Each PEI or AEI
- Each MG and SG (even though the MG or SG may be connected physically to the CCA over an internal proprietary interface, instead of being logically connected to the CCA over the ASLAN)
- The CCA/IWF/MGC itself
- The EBC (for LSC, PEI, AEI, and MG communication with other LSCs, MFSSs, PEIs, AEIs, and MGs over the DISN WAN)

As an example, the CCA interacts with the LSC Transport Interface functions when it uses IP, TLS, TCP, and the native ASLAN protocols to exchange SIP signaling messages with PEIs or AEIs and the EBC over the ASLAN.

The MGs controlled by the CCA interact with the LSC Transport Interface functions when they use IP, UDP, and the native ASLAN protocols to route SRTP media streams to and from PEIs, AEIs, other LSC MGs, and the EBC over the ASLAN.

[Required] The CCA shall support assignment of the following items to itself:

- Only one CCA IP address (this one IP address may be implemented in the CCA as either a single logical IP address or a single physical IP address),
- A CCA Fully Qualified Domain Name (FQDN) that maps to that IP address, and

- A CCA SIP URI that uses that CCA FQDN as its domain name, and maps to the “SIP B2BUA” function within the CCA itself.

[Required] The CCA shall support assignment of the following items to each SIP and AS-SIP PEI and AEI on the Appliance LAN:

- Only one PEI or AEI IP address,
- A PEI or AEI FQDN that maps to that IP address, and
- 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.

[Required] The CCA shall support assignment of the following items to each MG on the Appliance LAN:

- Only one MG IP address (this one IP address may be implemented in the MG as either a single logical IP address or a single physical IP address),
- An MG FQDN that maps to that IP address, and
- An MG SIP URI that uses that MG FQDN as its domain name, and maps to the “UC Signaling and Media End Point” function within the MG.

[Required: MFSS – Conditional: LSC] The CCA shall support assignment of the following items to each SG on the Appliance LAN:

- Only one SG IP address (this one IP address may be implemented in the SG as either a single logical IP address or a single physical IP address),
- An SG FQDN that maps to that IP address, and
- An SG SIP URI that uses that SG FQDN as its domain name, and maps to the “UC Signaling End Point” function within the SG.

[Required] The CCA shall support assignment of the following items to the EBC:

- Only one EBC IP address (this one IP address may be implemented in the EBC as either a single logical IP address or a single physical IP address),
- An EBC FQDN that maps to that IP address, and

- An EBC SIP URI that uses that EBC FQDN as its domain name, and maps to the “SIP B2BUA” function within the EBC.

5.3.2.10.4 CCA Interactions with the EBC

The EBC provides SBC and firewall capabilities for the ASLAN, the PEIs/AEIs, and the IP-based components of the LSC, including the CCA/IWF/MGC and the MGs.

The CCA interacts with the EBC by directing AS-SIP signaling packets to it (for signaling messages destined for an MFSS) and by accepting AS-SIP signaling packets from it (for signaling messages directed to the LSC from an MFSS).

The LSC EIs and MGs, which are controlled by the CCA, interact with the EBC by directing SRTP media streams to it (for call media destined for EIs and MGs on other LSCs), and by accepting SRTP media streams from it (for call media directed to the LSC PEIs/AEIs and MGs from EIs and MGs on other LSCs).

The AS-SIP signaling packets exchanged between the LSC and an MFSS must pass through the EBC. The SRTP media streams exchanged between LSC EIs /MGs and EIs/ MGs on other LSCs must also pass through the EBC.

The CCA in the MFSS and LSC needs to interact with AS-SIP functions in the EBC, which

- Mediates AS-SIP signaling between an LSC and an MFSS, and between two MFSSs,

- Supports SBC functions, such as NAT and Network Address and Port Translation (NAPT), and

- Supports IP firewall functions.

High-level CCA requirements are needed for interacting with an EBC. These requirements are as follows:

1. **[Required]** When directing VoIP sessions to other network appliances providing voice and video services across the DISN, the CCA shall direct these VoIP sessions to the EBC, so that the EBC can process them before directing them to the network appliances on the DISN WAN.

2. **[Required]** The CCA shall direct VoIP sessions to other network appliances through the EBC in the following cases:

a. When the CCA is part of an LSC and is directing VoIP sessions to an MFSS on the DISN WAN, which is the "primary" or "backup" MFSS for that LSC,

b. When the CCA is part of an MFSS and is directing VoIP sessions to an LSC on the DISN WAN, which is a "subtended" LSC for that MFSS,

c. When the CCA is part of an MFSS and is directing VoIP sessions to another MFSS on the DISN WAN

3. **[Required]** When accepting VoIP sessions from other network appliances on the DISN, the CCA shall accept these VoIP sessions from the EBC, because the EBC relays them from the network appliances on the DISN WAN.

4. **[Required]** The CCA shall accept VoIP sessions from other network appliances through the EBC in the following cases:

a. When the CCA is part of an LSC and is accepting VoIP sessions from an MFSS on the DISN WAN, which is the "primary" or "backup" MFSS for that LSC

b. When the CCA is part of an MFSS and is accepting VoIP sessions from an LSC on the DISN WAN, which is a "subtended" LSC for that MFSS

c. When the CCA is part of an MFSS and is accepting VoIP sessions from another MFSS on the DISN WAN

5.3.2.10.5 CCA Support for Admission Control

The CCA interacts with the ASAC component of the LSC and MFSS to perform specific functions related to ASAC, such as counting internal, outgoing, and incoming calls; managing separate call budgets for VoIP and Video over IP calls; and providing preemption.

Requirements for ASAC are handled in two categories: CAC and ASAC. Call Admission Call is defined as follows:

> "A process in which a call is accepted or denied entry (blocked) to a network based on the network's ability to provide resources to support the quality of service (QoS) requirements for the call."

Call Admission Control is also referred to as SAC, because in the network appliances a VoIP call is also a SIP Voice session, and a Video call is also a SIP Video session. Session Admission Control is limited as follows:

> "SAC is typically limited to managing the pre-populated session budgets for each Assured Service (voice and video)."

Assured Services Admission Control includes CAC/SAC and its support for call counting, voice call budgets, and video call budgets. In addition, ASAC includes capabilities for handling calls differently based on their precedence level (e.g., DSN ROUTINE, PRIORITY, IMMEDIATE, FLASH, or FLASH OVERRIDE), and for having calls of a higher precedence level preempt calls of a lower precedence level.

Two different levels of ASAC are LSC-Level ASAC (supported in the LSC and the MFSS) and WAN-Level ASAC Policing (supported in the MFSS only). The LSC and MFSS are responsible for maintaining the following:

- VoIP session budgets
- VoIP session counts
- TDM session budgets
- TDM session counts
- VSU budgets
- VSU counts

[Required] The LSC and MFSS CCA shall meet all the requirements in Section 5.3.2.2.2.3, ASAC – Open Loop.

[Required] The LSC and MFSS CCA shall meet all the requirements in Section 5.3.4.10, Precedence and Preemption.

[Required] The LSC and MFSS CCA shall meet all the requirements in Section 5.3.4.11, Policing of Call Count Thresholds.

5.3.2.10.6 CCA Support for UFS

The UFS Server is responsible for providing features and services to VoIP and Video PEIs/AEIs on an LSC or MFSS, where the CCA alone cannot provide the feature or service. In this section, no distinction is made between "features" and "services," and all features and services, such as Call Hold, Call Waiting, Precedence Call Waiting, Call Transfer, Call Forwarding, Hotline Service, and Calling Party and Called Party ID (number only), are called features. Examples of features that may require the use of a UFS Server are voice mail services; services that use TCAP queries and responses over CCS7 signaling links, such as toll-free 800/888 number services and calling name delivery services; and services that require screening of calling party numbers on incoming calls (e.g., block calls to this VoIP PEI/AEI from these numbers); and screening of called party numbers on outgoing calls (e.g., block calls from this VoIP PEI/AEI to these numbers).

The CCA interacts with UFS by relaying end-user requests for feature and service invocation to the UFS, and relaying UFS responses, such as text displays and message waiting indicators, back to PEIs/AEIs and end users. The CCA may relay feature information from the UFS to the EI/AEI and end user without a corresponding feature request from the PEI/AEI or the end user. Examples of this include the UFS text message that tells an PEI that a call waiting call is available, and the UFS indicator that tells a PEI that there is a message waiting for that PEI.

[Required] The CCA within a network appliance shall support the operation of the following features and capabilities, as listed in Table 5.3.2.2-1, Assured Services Product Features and Capabilities:

1. **[Required]** The CCA shall generate a redirecting number each time it forwards a VoIP or Video session request as part of a Call Forwarding feature.

2. The CCA supports the ability to direct VoIP and Video sessions and session requests to the UFS Server, so that the UFS Server can apply an Appliance VoIP or Video feature, when use of that feature is required by the calling party, 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.

5.3.2.10.7 CCA Support for Information Assurance

The Information Assurance function within the appliance ensures that end users, PEIs, AEIs, MGs, SGs, and EBCs 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 encrypted properly SIP/TLS.

[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 EBCs) to the Information Assurance function to support the Information Assurance function’s user, PEI, AEI, and EBC authentication capabilities, and its PEI, AEI, and EBC signaling stream encryption capabilities.

[Required: MG – Conditional: SG] The CCA MGC shall relay received H.248 and IPSec (or proprietary-protocol-equivalent) authentication credentials and encryption key information from sending end systems (i.e., MGs and SGs) to the Information Assurance function to support the Information Assurance function’s MG and SG authentication capabilities, and its MG and SG signaling stream encryption capabilities.

[Required] The CCA shall relay authentication credentials received in a SIP or AS-SIP REGISTER message from an PEI, AEI, or EBC to the Information Assurance function so the

Information Assurance function can validate those credentials and allow that PEI, AEI, or EBC to register with the appliance.

[Conditional] The CCA MGC shall relay authentication credentials received with an H.248 message in an IPSec packet from an MG to the Information Assurance function so the Information Assurance function can validate those credentials and allow that MG to register with the appliance.

[Conditional] The CCA MGC shall relay authentication credentials received in an IPSec packet from an SG to the Information Assurance function so the Information Assurance function can validate those credentials and allow that SG to register with the appliance.

[Required] The CCA shall relay TLS encryption key information received from 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.

[Required] The CCA shall relay TLS encryption key information received from an EBC 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 EBC.

[Required] The CCA within the appliance shall support all Information Assurance Appliance requirements in Section 5.4, Information Assurance Requirements, 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.

5.3.2.10.8 CCA Interactions with Local Location Service

The LLS provides information on called address translation in response to call routing queries from the CCA. The CCA sends call routing queries to the LLS for both outgoing calls from appliance PEIs or AEIs (i.e., LSC and MFSS) and incoming calls to appliance PEIs or AEIs (i.e., LSC and MFSS).

The CCA uses the information returned by the LLS to

- Route internal calls from one appliance PEI or AEI to another,

- Route outgoing calls from an appliance PEI or AEI to another appliance (via an EBC), or to a TDM network (via an Appliance MG), and

- Route incoming calls from another appliance (via an EBC), or from a TDM network (via an Appliance MG), to an LSC PEI or AEI.

The interface and protocols used to interconnect the CCA with the LLS are internal to the appliance and, therefore, are supplier specific.

5.3.2.10.9 CCA Interactions with Global Location Service

Like the LLS, the GLS provides information on call routing in response to call-routing queries from the CCA. The CCA sends call-routing queries to the GLS for calls where the CCA determines that the call's destination lies outside the MFSS.

Call routing/addressing will involve two basic scenarios: MFSS internal calls or external calls.

1. MFSS internal calls are defined as local calls within the MFSS. These calls are any combination of calls among and between IP instruments and TDM instruments served either by the TDM side or by the SS side of the MFSS. Calls between the TDM and SS sides of the MFSS are routed over internal, proprietary connections requiring an internal MG.

2. External calls are defined as calls to/from the MFSS and other distant-end systems and networks, including other MFSSs, DSN EOs, PBXs, and the PSTN. Calls to or from TDM-based distant-end systems will route through the TDM side of the MFSS; calls to IP-based distant-end systems (i.e., LSCs, MFSS) will route through the SS side of the MFSS using IP-bearer and AS-SIP signaling.

The CCA may determine call routing based on an analysis of the called address. For example, it does this by finding that this address did not contain a PSTN escape code as a prefix, and by finding that the first six digits of this called address (i.e., the NPA-NXX in the DoD dialing plan) pointed to a location in the DoD network outside the MFSS. The CCA may make this determination based on a previous call-routing response from the MFSS's LLS that indicated, "This address is not assigned to any PEI, AEI, or MG on the MFSS."

As in the LLS case, the query from the CCA to the GLS identifies the called address for the call in question. It may be embedded within a SIP URI, e.g., sip: +17327582000@uc.mil; user=phone, or sip: 3144305353@uc.mil; user=phone. The response from the GLS identifies either:

- A remote IP address that points to the next appliance (i.e., an LSC or an MFSS) that the call should be routed to, or

- The local IP address of an MFSS MG trunk group that the call should be routed to. (This case applies when the MG TG connects to a TDM destination outside the MFSS, which can be on the DoD TDM network, an allied or coalition partner TDM network, or on the PSTN (CONUS and Global)).

5.3.2.10.10 CCA Interactions with End Instrument(s)

The CCA in the MFSS or LSC needs to interact with VoIP PEIs and AEIs served by that MFSS or LSC. The VoIP interface between the PEI and the MFSS or LSC is left up to the network appliance supplier. The VoIP interface between the AEI and the MFSS or LSC is AS-SIP.

The following requirements on VoIP EIs are part of the CCA requirements for the MFSS or LSC:

1. **[Required]** The CCA shall support supplier-proprietary Voice and Video EIs, using EI-CCA protocols that are proprietary to the LSC or MFSS supplier.

2. **[Required]** The CCA shall support the following Voice and Video EIs and their associated EI signaling protocols:

    - **[Objective]** SIP Voice and Video EIs
    - **[Objective]** H.323 Voice and Video EIs
    - **[Required]** AS-SIP Voice and Video EIs

[Objective] When the CCA IWF supports H.323 Voice and Video EIs, the IWF shall support these EIs using ITU-T Recommendation H.323.

NOTE: An LSC or MFSS ASLAN may support two different types of H.323 EIs:

- "H.323 Overlay Network": H.323 EIs that are served by an H.323 Gatekeeper, which is completely separate from the CCA.

- "H.323/AS-SIP Interworking": H.323 EIs that are served by the CCA (where the CCA is effectively an H.323 Gatekeeper for these EIs).

The first case is outside the scope of this section.

The second case is within the scope of this section, with one qualification. The CCA's use of AS-SIP is within the section's scope, but the details on how the supplier's CCA performs the protocol interworking between EI H.323 and CCA AS-SIP are outside this section's scope.

[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 5.3.2.22, Generic AS-SIP End Instrument and Video Codec Requirements, and Section 5.3.4, AS-SIP Requirements.

5.3.2.10.11 CCA Support for Assured Services Voice and Video

[Required] The Appliance CCA (i.e., LSC or MFSS) shall support both assured Voice and Video services. The CCA shall support both assured Voice and assured Video sessions, and shall support these sessions from both VoIP EIs and Video EIs, as described in UCR 2008, Section 5.3.2.10.10, CCA Interactions with End Instrument(s).

[Required] The Appliance CCA shall support common procedures and protocol for VoIP and Video session control, with the following clarifications and exceptions:

1. The CCA is required to be able to support “single-rate” TDM video (i.e., 64-kbps TDM video calls) at MG trunk groups that are controlled by the CCA.

2. The CCA is not required to be able to support “multi-rate” TDM video (i.e., Nx64-kbps TDM video calls, where N runs from 2 to 24) at MG trunk groups that are controlled by the CCA.

The CCA is not required to support protocol interworking between TDM video calls and

- IP video sessions that originate from or terminate on local Video EIs that are served by the CCA, or

- IP video sessions that originate from or terminate on remote Video EIs, that reach the CCA via the EBC, the DISN WAN, and remote appliances.

[Required] The Appliance CCA shall support common procedures and protocol for feature control, for the features and capabilities given in Table 5.3.2.2-1, Assured Services Product Features and Capabilities.

[Required] On calls to and from Proprietary VoIP and Proprietary Video EIs, the CCA shall use the appropriate parameters within the appliance supplier’s Proprietary protocol messages to differentiate Proprietary VoIP sessions from Proprietary Video sessions.

[Conditional] When H.323 EIs are supported on calls to and from H.323 EIs, the CCA shall use the appropriate parameters within the H.323 protocol messages to differentiate H.323 VoIP sessions from H.323 Video sessions.

[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 ACK messages, as well as the SDP message bodies in AS-SIP 200 OK responses and earlier 1xx provisional responses, to differentiate AS-SIP Voice sessions from AS-SIP Video sessions. (NOTE: Support for AS-SIP EIs is Required for 2010.)

The CCA's use of these SDP bodies for VoIP and Video differentiation shall follow the detailed SDP requirements for VoIP and Video in Section 5.3.4, AS-SIP Requirements.

[Required] The CCA shall track VoIP sessions against corresponding Appliance VoIP budgets, and shall **separately track** Video sessions against corresponding Video budgets. The CCA shall maintain the Appliance's VoIP budgets separate from the Appliance's Video budget. The CCA shall perform this separate tracking of Appliance VoIP and Video calls and budgets consistent with the CAC/SAC requirements in Section 5.3.2.10.5, CCA Support for Admission Control.

[Required] As part of LSC-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 5.3.2.10.5, CCA Support for Admission Control.

[Required] The CCA shall allow an individual PEI (i.e., Proprietary, H.323, or SIP) to support both VoIP and Video sessions. The CCA shall allow an individual EI to have both VoIP and Video sessions active at the same time.

[Required] The CCA shall allow an individual AEI (i.e., AS-SIP) to support both VoIP and Video sessions. The CCA shall allow an individual AEI to have both VoIP and Video sessions active at the same time.

[Required] The CCA shall support the routing of both VoIP and Video session requests from LSCs to MFSSs, from MFSSs to LSCs, and from MFSSs to MFSSs, using AS-SIP. The CCA shall direct outgoing VoIP and Video session requests to EBCs, and shall accept incoming VoIP and Video session requests from EBCs, consistent with this LSC-to-MFSS routing, MFSS-to-LSC routing, and MFSS-to-MFSS routing.

5.3.2.10.12 CCA Interactions with Service Control Functions

[Required] The CCA shall support the ability to remove VoIP and Video sessions and session requests from the media server so the CCA can continue with necessary session processing once the media server has completed its functions. Examples include the following:

1. Removing a calling VoIP 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).

2. 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 LSC and MFSS and, therefore, supplier specific.

The Media Server function provides tones and announcements that the LSC "plays out" to local and remote end users on VoIP and Video calls. In addition, the media server may provide audio and video messages, or "clips," that the LSC can "play" to local and remote users on Video calls.

NOTE: It is possible that some tones and announcements may be generated locally by the end user's PEI or AEI, based on commands from the LSC to the PEI or AEI that mandate the "play" of the tones or announcements. (An example of this is the use of an LSC command that instructs a PEI to "play" dial tone to a calling end user, and then to automatically halt "playing" dial tone upon receipt of the first keypad digit from that end user.) In these cases, the use of a separate media server to provide tones and announcements to end user PEIs or AEIs is up to the LSC vendor.

The media server stores these tones, announcements, audio clips, and video clips locally, and "plays them out" to either local or remote end users in response to corresponding requests from the CCA. As part of this "play out" process, the media server may prompt the end users for information (e.g., entry of keypad digits, or vocal answers to media server questions). In this case, the media server collects that information and responds to the CCA indicating what the collected information was, or what action the CCA should take based on the collected information.

The CCA is responsible for asking the media server to "play out" tones, announcements, audio clips, and video clips, and for ensuring that the media from the media server is directed to the correct end user. In addition, the CCA is responsible for capturing collected information from the media server, such as the series of keypad digits entered by an end user in response to a media server prompt, and using that information appropriately for call processing or feature processing.

5.3.2.11 CCA Interworking between AS-SIP and DoD CCS7

5.3.2.11.1 Purpose and Scope

This section provides basic requirements for interworking call setup and release signaling between a DoD network using the AS-SIP and a network using DoD CCS7. The interworking is performed at a node with CCA (SIP/CCS7 IWF) functionality that processes/interworks incoming CCS7 messages to outgoing AS-SIP messages, and similarly, incoming AS-SIP messages to outgoing CCS7 messages.

All requirements in this section are **[Conditional: LSC, MFSS]**, unless otherwise indicated. This condition is illustrated in Figure 5.3.2.8-1, Functional Reference Model – MFSS.

The requirements in this section are defined in terms of functionality at a SIP/CCS7 IWF as follows:

1. Section 5.3.2.11.4, Interworking for a Call Originating in an AS-SIP Network toward an ISUP Network, reviews the protocols that are interworked at the SIP/CCS7 IWF, and includes their scope and their relationship to national standards and requirements documents.

2. Section 5.3.2.11.4.1.3.6.2, Generic Address, discusses the general principles of interworking between the protocols and provides an overview of the design and functionality required at the SIP/SCCS7 IWF.

3. Section 5.3.2.11.5, Interworking for a Call Originating in an ISUP Network toward an AS-SIP Network, provides detailed interworking requirements for a call that is initiated from an AS-SIP network toward a CCS7 network.

4. Section 5.3.2.11.5.1.3, Coding of SDP Media Description Lines from USI, provides detailed interworking requirements for a call that is initiated from a CCS7 network toward an AS-SIP network.

5. Section 5.3.2.12.9, MG Support for DoD CCS7 Trunks, defines conditions for connection of the bearer (voice) path through the MG, including the playing of tones and announcements by the SIP/CCS7 IWF toward the CCS7 network.

6. Section 5.3.2.11.5.3, Expiration of T_{OIW2} and Sending Early ACM, provides the requirements for the T_{OIW2} timer, which controls the sending of an early CCS7 Address Complete Message (ACM).

5.3.2.11.2 Background

This section applies to network nodes that meet the requirements for support of the DSN CCS7 and AS-SIP protocols as given in Section 5.3.2.9.5, CCA-IWF Signaling Protocol Support Requirements. In addition, operation of MLPP functionality at the SIP/CCS7 IWF is aligned with the specification of that functionality in ANSI T1.619 and ANSI T1.619a. The functionality described in this section is aligned with that functionality specified in ANSI T1.679.

It is assumed that the SIP/CCS7 IWF does not perform number portability (NP) queries for enabling service provider portability. However, the SIP/CCS7 IWF does map NP-related IEs, retaining any knowledge of a prior NP query performed to support service provider portability. Though not a requirement, the SIP/CCS7 IWF may support SIP and CCS7 signaling to enable service portability and geographic portability.

Every call at the SIP/CCS7 IWF will have an assigned MLPP priority level and domain assigned when the call was originated or when it entered the DoD network.

5.3.2.11.3 General Considerations

[Conditional] The following rules apply to the handling of unrecognized ISUP information:

1. Assuming that no ISUP encapsulation is used, the SIP/CCS7 IWF shall act as a Type A exchange for ISUP Compatibility procedures.

2. Only the procedures, methods, and elements of information (i.e., messages, parameters, indicators, headers) relevant to interworking are described. Therefore, the procedures, methods, and elements of information that are of local significance (i.e., only relevant to one of the signaling systems: AS-SIP or ISUP) are not interworked.

3. The SIP/CCS7 IWF combined with an ISUP exchange or an MG shall provide interworking between the bearer network connections into the AS-SIP and ISUP networks.

4. Before sending any information into the AS-SIP network, the SIP/CCS7 IWF shall consult its local trust policy (e.g., for authentication and authorization) to determine whether the subsequent node to which the outgoing message is directed is trusted to receive that information. If the adjacent SIP node is not trusted to receive that information, the SIP/CCS7 IWF shall take appropriate action (e.g., omit the information, provide another value, or release the call).

5. Before accepting any information from the AS-SIP network, the SIP/CCS7 IWF shall consult its local trust policy (e.g., for authentication and authorization) to determine whether the node from which the incoming message came is trusted to originate or pass on that information. If the adjacent SIP node is not trusted to provide that information, the SIP/CCS7 IWF shall take appropriate action (e.g., ignore the information, use a default value, or release the call).

[Conditional] The SIP/CCS7 IWF shall establish a one-to-one relationship between each AS-SIP dialog and the corresponding ISUP call/bearer control instance so the SIP/CCS7 IWF interworks all the signaling information associated with a given call.

[Conditional] For calls where AS-SIP-to-CCS7 interworking is required, when an AS-SIP message is received for that call, the SIP/CCS7 IWF shall construct an appropriate ISUP message for that call using the information received within the SIP message's header fields and SDP body, if present.

Section 5.3.2.11.4, Interworking for a Call Originating in an AS-SIP Network toward an ISUP Network, and Section 5.3.2.11.4.1.3.6.2, Generic Address, provide the interworking specifications for AS-SIP and ISUP networks.

5.3.2.11.4 Interworking for a Call Originating in an AS-SIP Network toward an ISUP Network

This section describes the interworking requirements for a call originating in an AS-SIP network toward an ISUP network.

5.3.2.11.4.1 Sending of Initial Address Message

If an AS-SIP INVITE request is received and the INVITE request cannot be associated with an existing call, the interworking procedures depend on whether the INVITE request contains an SDP offer. Section 5.3.2.11.4.1.1, INVITE Request Received without an SDP Offer, provides detailed interworking procedures for the case when an SDP offer is not contained. Section 5.3.2.11.4.1.2, INVITE Request Received with an SDP Offer, provides detailed interworking procedures for the case when an SDP offer is contained.

[Conditional] If an AS-SIP INVITE is received, the Initial Address Message (IAM) resulting from the interworking procedures in Section 5.3.2.11.4.1.1, INVITE Request Received without an SDP Offer, and Section 5.3.2.11.4.1.2, INVITE Request Received with an SDP Offer, as applicable, shall be sent into the CCS7 network. The IAM parameters shall be coded as specified in Section 5.3.2.11.4.1.3, IAM Parameters.

If an INVITE request is received that does not have enough digits to route to the CCS7 network, normal SIP procedures apply, and the INVITE request is not interworked.

5.3.2.11.4.1.1 INVITE Request Received without an SDP Offer

[Conditional] Upon receipt of an INVITE request without an SDP Offer, if the INVITE request indicates support for reliable provisional responses, then an SDP Offer including media description shall be sent backward into the AS-SIP network within the first reliable non-failure provisional response (1xx greater than 100):

1. If SIP preconditions are not in use, the IAM shall be sent into the CCS7 network upon receipt of the SDP answer with media description.

2. If SIP preconditions are in use, the IAM shall be sent into the CCS7 network by continuing on to the procedures in Section 5.3.2.11.4.1.2.2, Received INVITE Request with Preconditions.

[Conditional] Upon receipt of an INVITE request without an SDP offer, if the INVITE request indicates that reliable provisional responses are not supported, then the IAM shall be sent immediately into the CCS7 network.

5.3.2.11.4.1.2 INVITE Request Received with an SDP Offer

The following subparagraphs describe an INVITE request with an SDP offer with or without preconditions.

5.3.2.11.4.1.2.1 Received INVITE Request without Preconditions

[Conditional] Upon receipt of an INVITE request with an SDP offer, if SIP preconditions are not in use, then the IAM shall be sent immediately into the CCS7 network.

5.3.2.11.4.1.2.2 Received INVITE Request with Preconditions

[Conditional] Upon receipt of an INVITE request with an SDP offer, if SIP preconditions are in use, then

1. If outgoing CCS7 signaling supports the use of the Continuity Check procedure, the IAM shall be sent immediately into the CCS7 network. The Continuity Check Indicator in the Nature of Connection Indicators parameter shall be set to “continuity check performed on previous circuit,” or “continuity check required on this circuit.” The latter setting shall be used if the continuity check is to be performed on the outgoing circuit.

2. If outgoing ISUP signaling on the subsequent network does not support the use of the Continuity Check procedure, sending of the IAM shall be deferred until all preconditions have been met.

In all cases, Section 5.3.2.11.4.1.3, IAM Parameters, gives specific details related to the population of specific parameters of the IAM. Table 5.3.2.11-1, IAM Parameters Mapped from an INVITE Request, lists the parameters within the IAM message that are interworked from the INVITE message and the associated sections that describe the specific interworking procedures.

5.3.2.11.4.1.3 IAM Parameters

Table 5.3.2.11-1 indicates the IAM parameters that interwork from INVITE.

Table 5.3.2.11-1. IAM Parameters Mapped from an INVITE Request

PARAMETER	SECTION
Called Party Number	5.3.2.11.4.1.3.1
Calling Party's Category	5.3.2.11.4.1.3.2
Nature of Connection Indicators	5.3.2.11.4.1.3.3
Forward Call Indicators	5.3.2.11.4.1.3.4
User Service Information	5.3.2.11.4.1.3.5
Calling Party Number	5.3.2.11.4.1.3.6.1
Generic Address	5.3.2.11.4.1.3.6.2
Hop Counter	5.3.2.11.4.1.3.7
Transit Network Selection[1]	5.3.2.11.4.1.3.8
Precedence	5.3.2.11.4.1.3.9
NOTES: 1. The Transit Network Selection parameter is not applicable in the DoD network. See UCR 2008, Section 5.3.2.11.4.1.3.8, Transit Network Selection. • The Charge Number parameter may also be included in the IAM as a network option when AS-SIP is used.	
LEGEND AS-SIP Assured Services Session Initiation Protocol IAM Initial Address Message	

5.3.2.11.4.1.3.1 Called Party Number (Required)

In the Request-URI, the incoming INVITE request will contain a sip(s): URI with the user=phone parameter:

- The userinfo part of that URI is an E.164 number encoded as specified by the telephone-subscriber rule of RFC 3966.

To generate the outgoing IAM, the SIP/CCS7 IWF shall use the following principles:

1. If the routing number field is not present in the userinfo component of the Request-URI, then the geographical telephone number field contained in the userinfo component of the Request-URI shall be mapped to the Called Party Number parameter of the IAM.

2. If the routing number field is present in the userinfo component of the Request-URI, the routing number field contained in the userinfo component of the Request-URI shall be mapped to the Called Party Number parameter of the IAM. For the mapping of the geographical telephone number field contained in the userinfo component of the Request-URI, refer to Table 5.3.2.11-2, Mapping of INVITE Request-URI to IAM Called Party Number.

[Conditional] The SIP/CCS7 IWF shall map the information contained in the userinfo component of the Request-URI to the Called Party Number parameter of the IAM message. Table 5.3.2.11-2 summarizes this mapping.

Table 5.3.2.11-2. Mapping of INVITE Request-URI to IAM Called Party Number

INVITE REQUEST-URI	IAM CALLED PARTY NUMBER	CONDITIONS
Geographical number in userinfo	Address Signal	If the routing number field is not present in the userinfo component
Routing number in userinfo (following “rn=“)	Address Signal	If the routing number field is present in the userinfo component
LEGEND IAM Initial Address Message URI Universal Resource Identifier		

5.3.2.11.4.1.3.2 Calling Party’s Category (Required)

[Conditional] If the incoming INVITE request uses AS-SIP, the default coding of the Calling Party’s Category field shall be 0 (“binary 0000 0000,” “Calling party’s category unknown”).

Other codes such as “ordinary subscriber,” “NS/EP call,” or “emergency service call” may be used in the Calling Party’s Category parameter based on the interworking configuration and on additional information received in the SIP INVITE request.

5.3.2.11.4.1.3.3 Nature of Connection Indicators (Required)

[Conditional] The Nature of Connection Indicators parameter in the outgoing IAM shall be set as shown in Table 5.3.2.11-3, Nature of Connection Indicators Parameters.

Table 5.3.2.11-3. Nature of Connection Indicators Parameter

BITS	NATURE OF CONNECTION INDICATORS PARAMETER
AB	Satellite indicator
DC	Continuity Check indicator (ISUP)
E	Outgoing echo control device
LEGEND ISDN Integrated Services Digital Network ISUP ISDN User Part	

Other Nature of Connection Indicators shall use the values specified in ANSI T1.113.3.

The codes in Table 5.3.2.11-4, Coding of the Nature of Connection Indicators Parameter, shall be used as the default in the Nature of Connection Indicators parameter field.

Table 5.3.2.11-4. Coding of the Nature of Connection Indicators Parameter

BITS	CODES	MEANING	CONDITIONS
AB	01	One satellite circuit in the connection	If AS-SIP is not used
DC*	00	Continuity check not required	Without pending precondition request (all profiles)
	10	Continuity check performed on a previous circuit	With pending precondition request (all profiles)
E	1	Outgoing echo control device included	Use of this value assumes that the DoD network supports echo control
* The SIP/CCS7 IWF creates COT, as required. See UCR 2008, Section 5.3.2.13.4.2, SG and CCA Interactions.			

LEGEND

AS-SIP-T	Assured Services Session Initiation Protocol for Telephones	DoD	Department of Defense
CCA	Call Connection Agent	IWF	Interworking Function
CCS7	Common Channel Signaling System No. 7	SG	Signaling Gateway
COT	Customer Originated Trace	SIP	Session Initiation Protocol

5.3.2.11.4.1.3.4 Forward Call Indicators (Required)

[Conditional] The Forward Call Indicators (FCI) parameter and its default values in the outgoing IAM shall be set as shown in Table 5.3.2.11-5, Forward Call Indicators Parameter.

Table 5.3.2.11-5. FCI Parameter

BITS	INDICATORS IN FCI PARAMETER	DEFAULT CODE	MEANING
D	Interworking indicator	1	Interworking encountered
F	ISUP indicator	0	ISUP not used all the way
HG	ISUP Preference indicator	01	ISUP not required all the way
I	ISDN Access indicator	0	Originating access non-ISDN
M	Ported Number Translation indicator	See Table 5.3.2.11-1, IAM Parameters Mapped from an INVITE Request	

LEGEND

FCI	Forward Call Indicators	ISDN	Integrated Services Digital Network
IAM	Initial Address Message	ISUP	ISDN User Part

Other FCI should follow ANSI T1.113. The appropriate values of the FCIs are determined based on analysis of various parameters (i.e., signaling, internal states, or configurations) at the SIP/CCS7 IWF.

The value of the M bit is set depending on whether an NP Database Dip Indicator (npdi) parameter is present in the userinfo component of the Request-URI, as shown in Table 5.3.2.11-6, Bit M in the FCI Parameter.

Table 5.3.2.11-6. Bit M in the FCI Parameter

BIT	CODE	MEANING	CONDITIONS
M	0	Number not translated	LNP dip not performed (npdi not present)
M	1	Number translated	LNP dip performed (npdi present)

LEGEND
LNP Local Number Portability npdi Number Portability Database Dip Indicator

5.3.2.11.4.1.3.5 User Service Information (Required) and Higher Layer Compatibility IE within Access Transport Parameter (Optional)

[Conditional] If the incoming INVITE request uses AS-SIP, either

1. The User Service Information (USI) parameter is set to 3.1 kilohertz (kHz) audio and transcoding is applied when required, or

2. If SDP is received from the remote peer before the IAM is sent, and if transcoding is not supported by the SIP/CCS7 IWF, then the USI parameter shall be derived from SDP, as described in Table 4/T1.679 of ANSI T1.679. Otherwise, they shall be set in accordance with local policy.

Table 4/T1.679 in ANSI T1.679 reflects the following considerations:

1. The SDP Media Description Part received by the SIP/CCS7 IWF should indicate only one media stream.

2. Only the “m=“, “b=“, and “a=“ lines of the SDP Media Description Part are considered to interwork with the IAM USI and High Layer Compatibility (HLC) parameters.

3. The first subfield (i.e., <media>) of the “m=“ line will indicate one of the currently defined values: “audio”, “video”, “application”, “data”, “image”, or “control”.

5.3.2.11.4.1.3.6 Calling Line Identification Parameters

Table 5.3.2.11-7, Mapping of SIP From/P-Asserted-Identity/Privacy Headers to ISUP CLI Parameters, summarizes the cases for mapping from the SIP INVITE header fields to the ISUP Calling Line Identification (CLI) parameters.

Table 5.3.2.11-7. Mapping of SIP From/P-Asserted-Identity/Privacy Headers to ISUP CLI Parameters

HAS A "P-ASSERTED -IDENTITY" HEADER FIELD CONTAINING A URI[1] WITH AN IDENTITY IN THE FORMAT "+CC"+ "NDC"+ "SN" BEEN RECEIVED?	HAS A "FROM" HEADER FIELD[2] CONTAINING A URI WITH AN IDENTITY IN THE FORMAT "+CC"+ "NDC"+ "SN" BEEN RECEIVED?	CALLING PARTY NUMBER PARAMETER ADDRESS SIGNALS	CALLING PARTY NUMBER PARAMETER APRI	GENERIC ADDRESS (SUPPLEMENTAL USER PROVIDES CALLING ADDRESS – NOT SCREENED) ADDRESS SIGNALS	GENERIC ADDRESS PARAMETER APRI
No	No	Network option to either include a network-provided E.164 number (see Table 5.3.2.11-8) or omit the Address Signals.	If a Privacy header field was received, set APRI as indicated in Table 5.3.2.11-9; otherwise, Network option to set APRI to "presentation restricted" or "presentation allowed."	Parameter not included.	Not applicable.
No	Yes	Network option to either include a network-provided E.164 number (see Table 5.3.2.11-8) or omit the Address Signals.	If a Privacy header field was received, set APRI as indicated in Table 5.3.2.11-9; otherwise, Network option to set APRI to "presentation restricted" or "presentation allowed."	Network option either to omit the parameter (if CgPN has been omitted) or derive from the "From" header (see Table 5.3.2.11-9)[3].	(See Table 5.3.2.11-10.)
Yes	No	Derive from P-Asserted-Identity (see Table 5.3.2.11-8).	APRI equals "presentation restricted" or "presentation allowed," depending on SIP Privacy header (see Table 5.3.2.11-9).	Not included.	Not applicable.

HAS A "P-ASSERTED -IDENTITY" HEADER FIELD CONTAINING A URI[1] WITH AN IDENTITY IN THE FORMAT "+CC"+ "NDC"+ "SN" BEEN RECEIVED?	HAS A "FROM" HEADER FIELD[2] CONTAINING A URI WITH AN IDENTITY IN THE FORMAT "+CC"+ "NDC"+ "SN" BEEN RECEIVED?	CALLING PARTY NUMBER PARAMETER ADDRESS SIGNALS	CALLING PARTY NUMBER PARAMETER APRI	GENERIC ADDRESS (SUPPLEMENTAL USER PROVIDES CALLING ADDRESS – NOT SCREENED) ADDRESS SIGNALS	GENERIC ADDRESS PARAMETER APRI

NOTES

1. It is possible that the P-Asserted-Identity header field includes both a tel: URI and a sip: URI. The handling of this case is for further study.
2. The "From" header may contain an "Anonymous URI." An Anonymous URI includes information that does not point to the calling party. RFC 3261 recommends that the display-name component contain "Anonymous." RFC 3323 recommends that the Anonymous URI itself have the value anonymous@anonymous.invalid.
3. This mapping effectively gives the equivalent of Special Arrangement (Network Option) to *all* SIP UACs with access to the SIP/CCS7 IWF.

LEGEND

APRI	Address Presentation Restricted Indicator	RFC	Request for Comments
CCS7	Common Channel Signaling System No. 7	SIP	Session Initiation Protocol
CgPN	Calling Party Number	UAC	User Agent Client
IWF	Interworking Function	URI	Universel Resource Identifier

5.3.2.11.4.1.3.6.1 Calling Party Number

Table 5.3.2.11-8, Setting of the Network-Provided ISUP CgPN Parameter with a CLI, provides details for when the Calling Party Number (CgPN) is given a network-provided value.

Table 5.3.2.11-8. Setting of the Network-Provided ISUP CgPN Parameter with a CLI

ISUP CgPN PARAMETER FIELD	VALUE
Screening Indicator	*"network provided"*
Number Plan Indicator	*"ISDN (Telephony) numbering plan (Recommendation E.164)"*
Address Presentation Restricted Indicator	Presentation allowed/restricted (see Table 5.3.2.11-7)
Nature of Address Indicator	If next ISUP node is located in the same country, set to "*national (significant) number*"; otherwise, set to "*international number*."
Address signals	If NOA is "*national (significant) number*," no country code should be included. If NOA is "*international number*," then the country code of the network-provided number should be included.
LEGEND CgPN Calling Party Number ISDN Integrated Services Digital Network	ISUP ISDN User Part NOA Nature of Address

Table 5.3.2.11-9, Mapping of P-Asserted-Identity and Privacy Headers to the ISUP CgPN Parameter, provides details for CgPN mapping in other cases.

Table 5.3.2.11-9. Mapping of P-Asserted-Identity and Privacy Headers to the ISUP CgPN Parameter

SOURCE SIP HEADER FIELD & COMPONENT	SOURCE COMPONENT VALUE	CgPN PARAMETER FIELD	DERIVED VALUE OF PARAMETER FIELD
–	–	Numbering Plan Indicator	“*ISDN (Telephony) numbering plan (Recommendation E.164)*”
P-Asserted-Identity header field, appropriate global number portion of the URI, assumed to be in the form of “+” CC+NDC+SN[1]	CC	Nature of Address Indicator	If CC is equal to the country code of the country where the SIP/CCS7 IWF is located, AND the next ISUP node is located in the same country, then set to “*national (significant) number”;* otherwise, set to “*international number.*”
Privacy, priv-value component[2]	Privacy header field absent	APRI	*“presentation allowed”*
	“none”		*“presentation allowed”*
	“header”		*“presentation restricted”*
	“user”		*“presentation restricted”*
	“id”		*“presentation restricted”*
–	–	Screening Indicator	*“network provided”*
P-Asserted-Identity header field, appropriate global number portion of the URI, assumed to be in the form of “+” CC+NDC+SN[1]	CC, NDC, SN	Address Signals	If NOA is “*national (significant) number*,” then set to NDC + SN. If NOA is “*internationa number*r,” then set to CC+NDC+SN.

NOTES

1. It is possible that the P-Asserted-Identity header field includes both a tel: URI and a sip: URI. The handling of this case is for further study.
2. It is possible to receive two priv-values, one of which is “*none*,” the other “*id.”* In this case, APRI shall be set to “*presentation restricted*.”

LEGEND

APRI	Address Presentation Restricted Indicator	IWF	Interworking Function
CCS7	Common Channel Signaling System No. 7	NOA	Nature of Address
CgPN	Calling Party Number	SIP	Session Initiation Protocol
ISDN	Integrated Services Digital Network	URI	Universal Resource Indicator
ISUP	ISDN User Part		

Table 5.3.2.11-10, Mapping of SIP from Header Field to ISUP Generic Address Parameter, provides details for mapping to a Generic Address, when this is possible.

[Conditional] The SIP/CCS7 IWF shall apply the mappings shown in Tables 5.3.2.11-7 through 5.3.2.11-10 when generating the ISUP CLI parameter. If any discrepancy occurs in privacy settings during the alignment process, the strongest privacy shall be used.

5.3.2.11.4.1.3.6.2 Generic Address

[Objective] The SIP/CCS7 IWF shall map the SIP From header field to the ISUP Generic Address parameter for supplemental CgPN, as shown in Table 5.3.2.11-10.

Table 5.3.2.11-10. Mapping of SIP “From” Header Field to ISUP Generic Address Parameter (Supplemental Calling Party Number Parameter)

SOURCE SIP HEADER FIELD & COMPONENT	SOURCE COMPONENT VALUE	GENERIC ADDRESS PARAMETER FIELD	DERIVED VALUE OF PARAMETER FIELD
–	–	Type of Address	“supplemental user provided calling address – not screened”
From, userinfo component of URI assumed to be in the form of “+” CC+NDC+SN	CC	Nature of Address Indicator	If CC is equal to the country code of the country where I-IWU is located, AND the next ISUP node is located in the same country, then set to *“national (significant) number”;* otherwise, set to *“international number.”*
–	–	Numbering Plan Indicator	*“ISDN (Telephony) numbering plan (Recommendation E.164)”*
–	–	APRI	Use same setting as for CgPN.
From, userinfo component assumed to be in the form of “+” CC+NDC+SN	CC, NDC, SN	Address Signals	If NOA is *“national (significant) number,”* then set to NDC + SN. If NOA is *“international number,”* then set to CC+NDC+SN.

NOTE: The “Geographical telephone number” in the userinfo component refers to the initial telephone number (immediately following “sip:”) in the Request-URI.

LEGEND

APRI	Address Presentation Restricted Indicator	ISUP	ISDN User Part
CgPN	Calling Party Number	NOA	Nature of Address
I-IWU	Incoming Interworking Unit	SIP	Session Initiation Protocol
ISDN	Integrated Services Digital Network	URI	Universal Resource Identifier

[Conditional] In the presence of the routing number and npdi fields in the userinfo component of the Request-URI, the geographical telephone number field contained in the userinfo component of the Request-URI shall be mapped to the GAP of the IAM. The coding of the GAP set by the SIP/CCS7 IWF is as specified in Table 5.3.2.11-11, Mapping of SIP Request-URI to ISUP Generic Address (Ported Number) Parameter.

Table 5.3.2.11-11. Mapping of SIP Request-URI to ISUP Generic Address (Ported Number) Parameter

SOURCE SIP HEADER FIELD & COMPONENT	SOURCE COMPONENT VALUE	GENERIC ADDRESS PARAMETER FIELD	DERIVED VALUE OF PARAMETER FIELD
–	–	Type of Address	“ported number”
– “+” CC+NDC+SN	–	Nature of Address Indicator	*“national (significant) number”*
–	–	Numbering Plan Indicator	“*ISDN (Telephony) numbering plan (Recommendation E.164)*”
Geographical number in userinfo component	+CC, NDC, SN from the URI	Address Signal	Set to NDC + SN

LEGEND
ISDN Integrated Services Digital Network SIP Session Initiation Protocol URI Universal Resource Identifier

5.3.2.11.4.1.3.7 Hop Counter

[Conditional] If the incoming INVITE request uses AS-SIP, the Hop Counter parameter shall be set to an integer equal to the value from the Max-Forwards header field value divided by a factor (F), rounded down. The value of F shall be derived by the SIP/CCS7 IWF using the following principles:

1. The Hop Counter parameter for a given message shall never increase, and shall decrease by at least one with each successive visit to an SIP/CCS7 IWF, regardless of intervening interworking. The same is true for Max-Forwards header field in the SIP domain.

2. The initial and successively mapped values of Max-Forwards header field should be large enough to accommodate the maximum number of hops that might be expected of a validly routed call.

3. The factor used to map from the Max-Forwards header field to the Hop Counter parameter for a given call will depend on call origin and call destination, and will be provisioned at the SIP/CCS7 IWF based on network topology, trust domain rules, and bilateral agreement.

5.3.2.11.4.1.3.8 Transit Network Selection

The DSN is the only transit network visible to the SIP/CCS7 IWF. Therefore, the SIP/CCS7 IWF does not expect to receive a Transit Network Selection parameter, and interworking for this parameter is not specified here.

5.3.2.11.4.1.3.9 Precedence

The modeling of the SIP/CCS7 IWF assumes that preemption of a call will occur at a node in the AS-SIP network or in the CCS7 network. The role of the SIP/CCS7 IWF is limited to interworking the signaling that indicates the relative priority of the calling party.

NOTE: If the SIP/CCS7 IWF controls the bearer path, it may perform preemption as described in Section 5.3.2.11.3, General Considerations.

[Conditional] If the incoming INVITE request uses AS-SIP, the RPH shall be used to derive the Precedence parameter, as shown in UCR 2008, Section 5.3.2.11.4, Interworking for a Call Originating in an AS-SIP Network toward an ISUP Network, or Section 7.1.1.2.1 of ANSI T1.619a in the outgoing IAM, as follows:

1. The network domain in the RPH is expected to be "uc." However, the Network Identity (NI) in the Precedence parameter shall be coded as "0000" (corresponding to the uc domain), independent of the received network domain.

2. The six-character precedence domain in the RPH shall be converted to binary to populate the MLPP service domain in the Precedence parameter.

3. If the received network domain in the RPH is "uc," then the SIP/CCS7 IWF shall map the received decimal value in the r-priority field in the RPH to the precedence level in the Precedence parameter. Some elements of this table are specified in Table 5.3.2.11-12, Mapping of RPH r-priority Field to IAM Precedence Level.

Table 5.3.2.11-12. Mapping of RPH r-priority Field to IAM Precedence Level

RECEIVED DECIMAL VALUE IN r-priority FIELD IN RPH	CALL PRIORITY	PRECEDENCE LEVEL IN IAM
0	ROUTINE	0 1 0 0
2	PRIORITY	0 0 1 1
4	IMMEDIATE	0 0 1 0
6	FLASH	0 0 0 1
8	FLASH OVERRIDE	0 0 0 0
LEGEND IAM Initial Address Message RPH Resource Priority Header		

4. If the received network domain is not "uc," the precedence level in the Precedence parameter shall be coded as "0100" ("routine").

[Conditional] For an incoming AS-SIP, the precedence level in the outgoing IAM shall be derived as follows:

[Objective] Network domains other than "uc" may be configured as valid domains in the SIP/CCS7 IWF. When the SIP/CCS7 IWF receives the AS-SIP message, it is an objective that the IWF check whether the network domain is recognized.

If the network domain is recognized, then the IWF shall map the network domain to the appropriate NI in the Precedence parameter according to configuration data, and shall translate the value of the r-priority field in the RPH to the precedence level bits in the Precedence parameter. The six-character precedence domain in the RPH shall be converted to binary to populate the MLPP service domain in the Precedence parameter.

If the network domain is not recognized, then the IWF shall populate the Precedence parameter according to configuration data.

5.3.2.11.4.2 Sending of Continuity Testing

[Conditional] When the preconditions on the incoming AS-SIP side have been met, and any continuity tests on the outgoing CCS7 side have been completed successfully, the SIP/CCS7 IWF shall send the Continuity Testing (COT) message coded as "Continuity check successful."

5.3.2.11.4.3 ACM Received

Table 5.3.2.11.13, Message Sent to AS-SIP Network upon Receipt of ACM from the CCS7 Network, provides a summary of how the ACM is interworked by the SIP/CCS7 IWF to be sent into an AS-SIP network.

Table 5.3.2.11-13. Message Sent to AS-SIP Network upon Receipt of ACM from the CCS7 Network

MESSAGE SENT TO AS-SIP NETWORK	ACM RECEIVED FROM CCS7 NETWORK: BCI PARAMETER, CALLED PARTY'S STATUS INDICATOR
183 Session Progress	00 – No indication
180 Ringing	01 – Subscriber free

LEGEND

ACM	Address Complete Message	BCI	Backwards Call Indicator
AS-SIP	Assured Services Session Initiation Protocol	CCS7	Common Channel Signaling No. 7

[Conditional] On receipt of the ACM, the backward SIP response sent by the SIP/CCS7 IWF depends on the value of the Called Party's Status Indicator in the Backwards Call Indicator (BCI) parameter of the ACM, as follows:

1. If the BCI (Called Party's Status Indicator) is set to "subscriber free," then a 180 (Ringing) SIP response code shall be sent.

2. If the BCI (Called Party's Status Indicator) is set to "no indication" or any value other than "subscriber-free," and if ISUP encapsulation is not used (i.e., interworking with an AS-SIP network), the ACM shall not be interworked.

NOTE: A backward path is available as soon as the IAM is sent and the appropriate SDP is received from the calling end.

NOTE: When the ACM is not interworked, protection against indefinite prolongation of the call is provided by timers specified in ANSI T1.113.

5.3.2.11.4.4 Call Progress Message Received

[Conditional] A Call Progress Message (CPG) with an Event Indicator of "progress" or "in-band information" shall not be interworked with AS-SIP. A CPG with an Event Indicator of "alerting" shall be interworked with AS-SIP, as shown in Table 5.3.2.11-14, Receipt of CPG at the SIP/CCS7 IWF.

Table 5.3.2.11-14. Receipt of CPG at the SIP/CCS7 IWF

MESSAGE SENT TO THE AS-SIP NETWORK	CPG EVENT INFORMATION PARAMETER RECEIVED EVENT INDICATOR RECEIVED	
180 Ringing	000 0001	(alerting)
Not interworked	000 0010 000 0011	(progress) or (in-band information or an appropriate pattern is now available)

LEGEND
AS-SIP Assured Services Session Initiation Protocol CPG Call Progress Message

5.3.2.11.4.5 Answer Message Received

[Conditional] On receipt of an Answer message (ANM), the SIP/CCS7 IWF shall send a 200 OK INVITE request to the AS-SIP network. If no offer was received in the initial INVITE request, and reliable provisional responses were not supported, the 200 OK INVITE request shall include an SDP offer consistent with the USI used on the CCS7 side.

5.3.2.11.4.6 Confusion Message Received

[Conditional] A received Confusion message shall be discarded by the SIP/CCS7 IWF.

5.3.2.11.4.7 Circuit Identification Code Query Response Message Received

[Conditional] After sending a Circuit Identification Code (CIC) Query message, the SIP/CCS7 IWF expects to receive a Circuit (CIC) Query Response message. The SIP/CCS7 IWF shall process the Circuit (CIC) Query Response message as described in ANSI T1.113.4, Clause 2.8.2A. The ISUP procedures may result in the release of a call.

5.3.2.11.4.8 Pass Along Message Received

On receipt of a Pass Along Message (PAM), the actions taken toward the CCS7 network are based on the contents of the PAM.

[Conditional] A received PAM shall be discarded by the SIP/CCS7 IWF.

5.3.2.11.4.9 Through Connection

Through connection of bearer path is applicable only to an SIP/CCS7 IWF that controls the bearer path.

[Conditional] Through connection at the SIP/CCS7 IWF shall follow the ANSI T1.113 through connection procedures for the originating exchange.

5.3.2.11.4.10 Suspend Message, Network Initiated Received

[Conditional] If the SIP/CCS7 IWF is the controlling exchange for the Suspend procedure, the actions taken toward the CCS7 network upon receipt of the Suspend message (SUS) shall be as described in ANSI T1.113, Clause 2.5.1.3. The SUS is not interworked, and no action is taken toward the AS-SIP network.

5.3.2.11.4.11 Resume Message, Network Initiated Received

[Conditional] If the SIP/CCS7 IWF is the controlling exchange for the Resume procedure, the actions taken toward the CCS7 network upon receipt of the Resume message (RES) shall be as described in ANSI T1.113, Clause 2.4.2c. The RES is not interworked, and no action is taken toward the AS-SIP network.

5.3.2.11.4.12 Release Procedures

5.3.2.11.4.12.1 Receipt of BYE or CANCEL

[Conditional] On receipt of an AS-SIP BYE or CANCEL message, the SIP/CCS7 IWF shall send an ISUP Release message (REL).

[Conditional] If AS-SIP is being used, and if the Reason header field is included in the BYE or CANCEL message, then the cause value may be mapped to the ISUP cause value field in the ISUP REL message, as shown in Table 5.3.2.11-15, Mapping of AS-SIP Reason Header Fields into Cause Indicators Parameter, depending on local policy. Table 5.3.2.11-16, Coding of Cause Value If Not Taken from the Reason Header Field, shows the coding of the cause value in the REL message if it is not available from the Reason header field. In all cases, the Location field shall be set to “network beyond interworking point.”

Table 5.3.2.11-15. Mapping of AS-SIP Reason Header Fields into Cause Indicators Parameter

COMPONENT OF AS-SIP REASON HEADER FIELD	COMPONENT VALUE	ISUP PARAMETER/FIELD	VALUE
protocol	“Q.850”	Coding standard	ITU-T Standard
protocol	“ANSI”	Coding standard	ANSI Standard
protocol-cause	“cause = XX” (Note)	Cause Value	“XX” (Note)
		Location	Network beyond interworking point
NOTE: “XX” is the cause value as defined in ITU-T Recommendation Q.850 or ANSI T1.113, depending on the value of the coding standard.			
LEGEND ANSI American National Standards Institute AS-SIP Assured Services Session Initiation Protocol		ISUP ISDN User Part ITU-T international Telecommunication Union – Telecommunications	

Table 5.3.2.11-16. Coding of Cause Value If Not Taken from the Reason Header Field

AS-SIP MESSAGE	REL CAUSE INDICATORS PARAMETER
BYE	Cause Value No. 16 (normal clearing)
CANCEL	Cause Value No. 31 (normal unspecified)
LEGEND AS-SIP Assured Services Session Initiation Protocol	REL Release Message

5.3.2.11.4.12.2 REL Message Received

[Conditional] On receipt of an ISUP REL message, if the SIP/CCS7 IWF is capable of bearer control, it immediately requests the disconnection of the internal bearer path. When the ISUP circuit is available for reselection, an ISUP Release Complete Message (RLC) is returned to the CCS7 network.

[Conditional] Depending on local policy, the received (ITU-T Recommendation Q.850 or ANSI T1.113) cause value of the REL message may be added to the AS-SIP final response or BYE message that is sent. The mapping of the Cause Indicators parameter to the Reason header field shall be as shown in Table 5.3.2.11-17, Mapping of Cause Indicators Parameter into AS-SIP Reason Header Fields.

Table 5.3.2.11-17. Mapping of Cause Indicators Parameter into AS-SIP Reason Header Fields

CAUSE INDICATORS PARAMETER FIELD	VALUE OF PARAMETER FIELD	COMPONENT OF AS-SIP REASON HEADER FIELD	COMPONENT VALUE
Coding standard	ITU-T Standard	protocol	“Q.850”
Coding standard	ANSI Standard	protocol	“ANSI”
Cause Value	“XX”[1]	protocol-cause	“cause= XX”[1]
		reason-text	Should be filled with the definition text as given in ITU-T Q.850 or ANSI T1.113[2]
NOTES 1. “XX” is the cause value as defined in ITU-T Recommendation Q.850 or ANSI T1.113. 2. Because the Cause Indicators parameter does not include the definition text as defined in ITU-T Recommendation Q.850 or ANSI T1.113, this is based on provisioning in the SIP/CCS7 IWF.			
LEGEND ANSI American National Standards Institute AS-SIP Assured Services Session Initiation Protocol ITU-T International Telecommunication Union – Telecommunications			

[Conditional] On receipt of a REL message before receiving an ANM, the SIP/CCS7 IWF shall send the appropriate SIP status code in an AS-SIP final response, as shown in Table 5.3.2.11-18, Receipt of the REL Message. The ISUP cause codes not appearing in the table shall have the same mapping as the appropriate ANSI T1.113 class defaults.

Table 5.3.2.11-18. Receipt of the REL Message

AS-SIP MESSAGE	REL CAUSE INDICATORS PARAMETER
Cause Values with Coding Standard Field Set to 00 (ITU-T Standard)[1]	
404 Not Found	Cause Value No. 1 (unallocated (unassigned) number)
500 Server Internal Error	Cause Value No. 2 (no route to network)
500 Server Internal Error	Cause Value No. 3 (no route to destination)
500 Server Internal Error	Cause Value No. 4 (send special information tone)
No Mapping (No procedure specified for this cause value in U.S. networks)	Cause Value No. 5 (misdialed trunk prefix) (No procedures specified for this cause value in U.S. networks)
See UCR 2008, Section 5.3.4, AS-SIP Requirements, which references RFCs 4411 & 3326	Cause Value No. 8 (preemption-circuit is not to be reused)
See UCR 2008, Section 5.3.4, AS-SIP Requirements, which references RFCs 4411 & 3326	Cause Value No. 9 (preemption-circuit is reserved for reuse)
486 Busy Here	Cause Value No. 17 (user busy)
480 Temporarily Unavailable	Cause Value No. 18 (no user responding)
480 Temporarily Unavailable	Cause Value No. 19 (no answer from the user)
480 Temporarily Unavailable	Cause Value No. 20 (subscriber absent)
480 Temporarily Unavailable	Cause Value No. 21 (call rejected)
410 Gone	Cause Value No. 22 (number changed)

AS-SIP MESSAGE	REL CAUSE INDICATORS PARAMETER
No Mapping (due to redirection procedures)	Cause Value No. 23 (redirect to a new destination)
502 Bad Gateway	Cause Value No. 27 (destination out of order)
484 Address Incomplete	Cause Value No. 28 (invalid number format) (address incomplete)
500 Server Internal Error	Cause Value No. 29 (facility rejected)
480 Temporarily Unavailable	Cause Value No. 31 (normal unspecified) (Class default)
480 Temporarily Unavailable	Cause Value in the Class 010 (resource unavailable, Cause Value No. 34)
500 Server Internal Error	Cause Value in the Class 010 (resource unavailable, Cause Value Nos. 38-47) (47 is class default)
500 Server Internal Error	Cause Value No. 50 (requested facility not subscribed)
500 Server Internal Error	Cause Value No. 57 (bearer capability not authorized)
500 Server Internal Error	Cause Value No. 58 (bearer capability not presently available)
500 Server Internal Error	Cause Value No. 63 (service option not available, unspecified) (Class default)
500 Server Internal Error	Cause Value in the Class 100 (service or option not implemented Cause Value Nos. 65-79) (79 is class default)
500 Server Internal Error	Cause Value No. 88 (incompatible destination)
404 Not Found	Cause Value No. 91 (invalid transit network selection)
500 Server Internal Error	Cause Value No. 95 (invalid message) (Class default)
500 Server Internal Error	Cause Value No. 97 (message type non-existent or not implemented)
500 Server Internal Error	Cause Value No. 99 (IE/parameter non-existent or not implemented)
480 Temporarily Unavailable	Cause Value No. 102 (recovery on timer expiry)
500 Server Internal Error	Cause Value No. 103 (parameter non-existent or not implemented, passed on)
500 Server Internal Error	Cause Value No. 110 (message with unrecognized parameter, discarded)
500 Server Internal Error	Cause Value No. 111 (protocol error, unspecified) (Class default)
480 Temporarily Unavailable	Cause Value No. 127 (interworking unspecified) (Class default)
Cause Values with Coding Standard Field Set to 01 (ANSI Standard) [1]	
404 Not Found	Cause Value No. 23 (unallocated destination number)
500 Server Internal Error	Cause Value No. 24 (unknown business group)
500 Server Internal Error	Cause Value No. 25 (exchange routing error)
404 Not Found[1]	Cause Value No. 26 (misrouted call to a ported number)
No Mapping (No procedure specified for this cause value in U.S. networks)	Cause Value No. 27 (NP QoR – number not found) (No procedures are specified for this cause value in U.S. networks.)

AS-SIP MESSAGE	REL CAUSE INDICATORS PARAMETER
Not Applicable	Cause Value in the Class 010 (resource unavailable, Cause Value Nos. 45 & 46) NOTE: Cause Value No. 45 is superseded by Cause Values 8 and 9 in codeset 0; Cause Value No. 46 is in codeset 1.
500 Server Internal Error	Cause Value in the Class 011 (service or option not available, Cause Value Nos. 51 & 54)
NOTE 1. The Coding Standard field in the Cause Indicators parameter in the received REL message may be set to either “ITU-T Standard” or “ANSI Standard.” This table is separated into two sections pertaining to each of these values of the Coding Standard field.	

LEGEND

ANSI	American National Standards Institute	ITU-T	International Telecommunication Union – Telecommunications	REL	Release Message
AS-SIP	Assured Services Session Initiation Protocol	NP	Number Portability	RFC	Request for Comment
IE	Information Element	QoR	Query on Release	UCR	Unified Capabilities Requirements

[Conditional] On receipt of a REL message after receiving an ANM, the SIP/CCS7 IWF shall send a BYE message.

5.3.2.11.4.12.3 Autonomous REL at SIP/CCS7 IWF

Table 5.3.2.11-19, Autonomous Release at SIP/CCS7 IWF, shows the trigger events at the SIP/CCS7 IWF and the release initiated by the SIP/CCS7 IWF when the call is traversing from AS-SIP to ISUP.

[Conditional] If an automatic repeat attempt initiated by the SIP/CCS7 IWF is unsuccessful (because the call is not routable), the SIP/CCS7 IWF shall send a 480 (Temporarily Unavailable) response code to the AS-SIP side. No actions on the ISUP side are required.

[Conditional] If, after answer, ISUP procedures result in an autonomous REL message from the SIP/CCS7 IWF, then a BYE message shall be sent on the AS-SIP side.

[Conditional] If the SIP/CCS7 IWF receives unrecognized backward ISUP signaling information and determines that the call needs to be released based on the coding, the SIP/CCS7 IWF shall send a 500 (Internal Server Error) response code on the AS-SIP side. Depending on local policy, a Reason header field containing the (ITU-T Recommendation Q.850 or ANSI T1.113) cause value of the REL message sent by the SIP/CCS7 IWF may be added to the AS-SIP message (BYE or final response) sent by the AS-SIP side of the SIP/CCS7 IWF.

Table 5.3.2.11-19. Autonomous Release at SIP/CCS7 IWF

AS-SIP SIDE	TRIGGER EVENT	REL ON THE CCS7 SIDE CAUSE PARAMETER
484 Address Incomplete	Determination that insufficient digits received	Not applicable
480 Temporarily Unavailable	Congestion at the SIP/CCS7 IWF	Not applicable
BYE	ISUP procedures result in release after answer	According to ISUP procedures
500 Server Internal Error	Call release due to the ISUP compatibility procedure	According to ISUP procedures
484 Address Incomplete	Call release due to expiry of T_7 within the ISUP procedures	According to ISUP procedures
480 Temporarily Unavailable	Other ISUP procedures result in release before answer	According to ISUP procedures

LEGEND

AS-SIP	Assured Services Session Initiation Protocol
CCS7	Common Channel Signaling No. 7
ISDN	Integrated Services Digital Network
ISUP	ISDN User Part
IWF	Interworking Function
REL	Release Message
SIP	Session Initiation Protocol

5.3.2.11.4.12.4 Reset Circuit, Circuit Group Reset, or Circuit Group Blocking Message Received

Table 5.3.2.11-20, Receipt of RSC, GRS, or CGB Messages, shows the AS-SIP message sent by the SIP/CCS7 IWF upon receipt of an ISUP Reset Circuit message (RSC), Circuit Group Reset message (GRS), or Circuit Group Blocking message (CGB) with the Circuit Group Supervision Message Type Indicator coded as “hardware failure oriented,” when at least one backward ISUP message relating to the call has already been received. The SIP/CCS7 IWF sends a BYE message if it has already received an ACK message for the 200 OK INVITE request it had sent. If it has sent a 200 OK INVITE request, but has not received an ACK message for the 200 OK INVITE request, then the SIP/CCS7 IWF shall wait until it receives the ACK message for the 200 OK INVITE request before sending the BYE message. Otherwise, it sends a 500 (Server Internal Error) response. On receipt of a GRS or CGB, one AS-SIP message is sent for each call association. Therefore, multiple AS-SIP messages may be sent on receipt of a single GRS or CGB message.

[Conditional] The SIP/CCS7 IWF shall process a received CCS7 RSC, GRS, or CGB message as shown in Table 5.3.2.11-20, Receipt of RSC, GRS, or CGB Messages.

Table 5.3.2.11-20. Receipt of RSC, GRS, or CGB Messages

MESSAGE SENT TO AS-SIP NETWORK	MESSAGE RECEIVED FROM ISUP
500 Server Internal Error or BYE	RSC
500 Server Internal Error or BYE	GRS
500 Server Internal Error or BYE	CGB with the Circuit Group Supervision Message Type Indicator coded "*hardware failure oriented*"

LEGEND

AS-SIP	Assured Services Session Initiation Protocol	GRS	Circuit Group Reset Message	ISUP	ISDN User Part
CGB	Circuit Group Blocking Message	ISDN	Integrated Services Digital Network	RSC	Reset Circuit Message

5.3.2.11.5 Interworking for a Call Originating in an ISUP Network toward an AS-SIP Network

This section describes the interworking requirements for a call originating in an ISUP network toward an AS-SIP network.

5.3.2.11.5.1 Sending of INVITE

[Conditional] After performing the normal ISUP handling for a received IAM and choosing to route the call to the AS-SIP network, the procedures at the SIP/CCS7 IWF will depend on whether preconditions are used in the AS-SIP network as follows:

1. Procedures to send an INVITE request without precondition upon receipt of an ISUP IAM are given in UCR 2008, Section 5.3.2.11.5.1.1, Sending INVITE without Precondition for a Received ISUP IAM.

2. Procedures to send an INVITE request with precondition upon receipt of an ISUP IAM are given in UCR 2008, Section 5.3.2.11.5.1.2, Sending INVITE with Precondition for a Received ISUP IAM.

3. Coding of the IAM received and the INVITE request sent by the SIP/CCS7 IWF are specified in UCR 2008, Section 5.3.2.11.5.1.3, Coding of SDP Media Description Lines from USI.

4. Timer (T_{OIW2}) is started when the INVITE request is sent.

5. If timer (T_{OIW2}) expires, an early ACM is sent to the CCS7 network. See UCR 2008, Section 5.3.2.11.5.3, Expiration of T_{OIW2} and Sending Early ACM.

5.3.2.11.5.1.1 Sending INVITE without Precondition for a Received ISUP IAM

Normal outgoing AS-SIP procedures for when an INVITE request is sent apply with the following clarifications and exceptions:

1. **[Conditional]** An INVITE request shall be sent immediately when an ISUP IAM is received and the Continuity Check Indicator in the Nature of Connection Indicators parameter in the IAM is set to indicate "continuity check not required."

2. **[Conditional]** Sending of the INVITE request shall be delayed if the Continuity Check Indicator in the Nature of Connection Indicators parameter in the IAM is set to indicate either "continuity check required on this circuit" or "continuity check performed on previous circuit." The INVITE request shall be sent on receipt of the Continuity message with the Continuity Indicators parameter set to "continuity check successful." The INVITE request shall not be sent if the Continuity message is received with the Continuity Indicators parameter set to "continuity check failed," or the ISUP timer T8 expires.

5.3.2.11.5.1.2 Sending INVITE with Precondition for a Received ISUP IAM

[Conditional] An INVITE request with a precondition shall be sent on receipt of an ISUP IAM. Incoming ISUP procedures apply, with the following clarifications and exceptions about when a confirmation of the precondition being met is sent.

NOTE: Configured procedures may delay the INVITE request until local resources have been reserved on the outgoing bearer path.

1. **[Conditional]** The SIP/CCS7 IWF initiates the precondition signaling procedure using the SDP Offer in the INVITE request. The precondition signaling is concluded upon sending (within an SDP Offer-Answer exchange) the confirmation of a precondition being met. The SDP Offer or SDP Answer carrying the confirmation of a precondition being met shall be sent when the following occur:

   a. If the Continuity Check Indicator in the Nature of Connection Indicators parameter in the incoming IAM is set to indicate either "continuity check required on this circuit" or "continuity check performed on previous circuit," the Continuity message with the Continuity Indicators parameter set to "continuity check successful" shall be received.

   b. The requested preconditions are met in the SIP network.

      NOTE: As a network option, the signaling of a precondition being met may only occur within the SDP Offer in an UPDATE message.

2. **[Conditional]** A CANCEL or BYE message shall be sent if the Continuity message is received with the Continuity Indicators parameter set to “continuity check failed,” or if ISUP timer T8 expires.

3. **[Conditional]** The REL message with Cause Value No. 47 (resource unavailable, unspecified) shall be sent by the SIP/CCS7 IWF to the ISUP network, and a CANCEL or BYE message shall be sent to the AS-SIP network if internal resource reservation was unsuccessful.

Table 5.3.2.11-21, Mapping of IAM Information to an INVITE Message, provides a summary of how the header fields within the outgoing INVITE message are populated. When the coding of the received Calling Party Category (CPC) is “NS/EP call” or “emergency service call,” additional information may be sent in the INVITE request.

Table 5.3.2.11-21. Mapping of IAM Information to an INVITE Message

IAM	INVITE	REFERENCE
Called Party Number	Request-URI	5.3.2.11.5.1.4
	To	5.3.2.11.5.1.4
Calling Party Number	P-Asserted-Identity	5.3.2.11.5.1.5
	Privacy	5.3.2.11.5.1.5
	From	5.3.2.11.5.1.5
GAP (Supplemental User Provided Calling Address)	From	5.3.2.11.5.1.5
GAP (Ported Number)	Request-URI	5.3.2.11.5.1.4
FCI (ported Number Translation Indicator)	Request-URI	5.3.2.11.5.1.4
Hop Counter	Max-Forwards	5.3.2.11.5.1.6
USI	Message Body (application/SDP)	5.3.2.11.5.1.3
Precedence	Resource Priority Header	5.3.2.11.5.1.7

LEGEND

FCI	Forward Call Indicator	SDP	Session Description Protocol	USI	User Service Information
IAM	Initial Address Message	URI	Universal Resource Indicator		

5.3.2.11.5.1.3 Coding of SDP Media Description Lines from USI

[Conditional] If present, the USI parameter in the IAM indicates user-requested bearer service characteristics. The USI codes shall be mapped to the AS-SIP SDP information. ANSI T1.113.3 provides an exhaustive list of the available codes in the USI. In principle, any combination of those codes can be mapped into any SDP information as long as transcoding is available.

[Conditional] The SIP/CCS7 IWF, as a network option, may also encode the SDP for the Adaptive Multi-Rate (AMR) codec, which is specified in RFC 4867.

[Conditional] If ITU-T Recommendation G.711 encoding may be used, then the SIP/CCS7 IWF shall send an SDP Offer with both “G.711 µ-law” and “G.711 A-law” included in the media description, and “G.711 µ-law” shall take precedence over “G.711 A-law.”

[Conditional] If transcoding is not available at the SIP/CCS7 IWF, the SIP/CCS7 IWF shall use the mapping relations in Table 5.3.2.11-22, Coding of SDP Media Description Lines from USI: ISUP to AS-SIP, from USI codes to SDP media description lines.

Table 5.3.2.11-22. Coding of SDP Media Description Lines from USI: ISUP to AS-SIP

USI PARAMETER	USI PARAMETER	USI PARAMETER	USI PARAMETER	HLC IE IN ATP	M= LINE			B= LINE	A= LINE
Information Transfer Rate	Rate Multiplier	Information Transport Capability	User Information Layer 1 Protocol Indicator	High Layer Characteristics Identification	<media>	<transport>	<fmt-list>	<modifier>:<bandwidth-value>	rtpmap:<dynamic-PT> <encoding name>/<clock rate>[/encoding parameters>
speech		Speech	G.711 µ-law	“Ignore”	audio	RTP/AVP	0 (& possibly 8)[1]	AS:64	rtpmap:0 PCMU/8000(& possibly rtpmap:8 PCMA/8000)[1]
speech		Speech	G.711 µ-law	“Ignore”	audio	RTP/AVP	Dynamic PT (& possibly a 2nd Dynamic PT)	AS:64	rtpmap:<dynamic-PT> PCMU/8000(and possibly rtpmap:8 PCMA/8000)[1]
3.1 kHz audio		3.1 kHz audio	G.711 µ-law	Telephony or “HLC absent”	audio	RTP/AVP	0	AS:64	rtpmap:0 PCMU/8000
3.1 kHz audio		3.1 kHz audio		Facsimile Group 2/3	image	udptl	t38	AS:64	Based on T.38
3.1 kHz audio		3.1 kHz audio		Facsimile Group 2/3	image	tcptl	t38	AS:64	Based on T.38
64 kbps unrestricted		Unrestricted digital information with tone/ann	N/A	“Ignore”	audio	RTP/AVP	9	AS:64	rtpmap:9 G.722/8000
64 kbps unrestricted		Unrestricted Digital Information	N/A	“Ignore”	audio	RTP/AVP	Dynamic PT	AS:64	rtpmap:<dynamic-PT> CLEARMODE/8000[2]
2 x 64 kbps unrestricted	2	Unrestricted Digital Information	N/A	“Ignore”	Note 3	Note 3	Note 3	Note 3	Note 3
384 kbps unrestricted		Unrestricted digital Information	N/A	“Ignore”	Note 3	Note 3	Note 3	Note 3	Note 3

NOTES:
1. Both PCMA and PCMU required under the conditions stated in UCR 2008, Section 5.3.2.11.5.1.3.
2. CLEARMODE has not yet been standardized.
3. No standard is defined at this time.

USI PARAMETER	USI PARAMETER	USI PARAMETER	USI PARAMETER	HLC IE IN ATP	M= LINE	B= LINE	A= LINE

LEGEND

ATP	Acceptance Test Procedure/Plan	kbps	Kilobits per Second	PCMU	Pulse Code Modulation mu-law
AVP	Audio/Video Profile	kHz	Kilohertz	RTP	Real Time Protocol
HLC	High Layer Compatibility	N/A	Not Applicable	USI	User Service Information
IE	Information Element	PCMA	Paired Carrier Multiple Access		

5.3.2.11.5.1.4 Request-URI and To Header Field

The Called Party Number parameter of the IAM contains the forward address information to derive the userinfo component of the INVITE Request-URI. The SIP/CCS7 IWF follows existing ISUP procedures to select the outgoing route.

[Conditional] If a new Called Party Number parameter is derived for the outgoing route, then the newly derived Called Party Number parameter shall be mapped into the userinfo component of the INVITE Request-URI.

For a basic call, the address information contained in the Called Party Number parameter is considered as the identification of the called party. Therefore, this information is used to derive the addr-spec component of the To header field.

If the Request-URI or the To header field contains a sip uri, it shall include the “user=phone” URI parameter.

It is assumed that the SIP/CCS7 IWF does not perform NP queries. However, it does map NP-related IEs.

[Conditional] When the Called Party Number parameter is included in the received IAM and the GAP for the ported number is not present, the mapping of this parameter and of the FCI Ported Number Indicator to the Request-URI shall be as shown in Table 5.3.2.11-23, Mapping of Called Party Number and FCI Ported Number Translation Indicator.

Table 5.3.2.11-23. Mapping of Called Party Number and FCI Ported Number Translation Indicator

ISUP PARAMETER/ FIELD	VALUE	SIP COMPONENT	VALUE
Called Party Number	Digits	Request-URI	userinfo
Address Signal	Either NCD + SN (national number) or CC + NCD + SN (international number)	userinfo's geographical number	If national number, prepend +CC to Address signal digits, as in: "+CC" "NCD" "SN." If international number, prepend "+".
FCI	Ported Number Translation Indicator	userinfo's npdi parameter	If Ported Number Translation Indicator is equal to "1," append ";npdi" to userinfo.

LEGEND

ISDN	Integrated Services Digital Network	FCI	Forward Call Indicator	npdi	NP Database Dip Indicator
		NP	Number Portability	SIP	Session Initiation Protocol
ISUP	ISDN User Part				

[Conditional] When the Generic Address (ported number) and Called Party Number parameters are both included in the received IAM, the mapping of these parameters and of the FCI Ported Number Indicator to the Request-URI shall be as shown in Table 5.3.2.11-24, Mapping of Generic Address (Ported) and Called Party Number (When Both are Included), and FCI Ported Number to Request-URI.

NOTE: The ISUP Transit Network Selection parameter is not expected to be received at the SIP/CCS7 IWF. Therefore, this document does not specify interworking of the parameter.

Table 5.3.2.11-24. Mapping of Generic Address (Ported) and Called Party Number (When Both are Included), and FCI Ported Number to Request-URI

ISUP PARAMETER/ FIELD	VALUE	SIP COMPONENT	VALUE
Generic Address Type of Number	"ported number"	Request-URI	userinfo
Address Signal	Since NOA is "*national (significant) number,*" then the format of the address signals is NCD + SN	userinfo's geographical number	Add +CC to Address Signal digits, as in: "+CC" "NCD" "SN"
FCI	Ported Number Translation Indicator	userinfo's npdi parameter	";npdi" is added to userinfo
Called Party Number Address Signal	Since NOA is "*national (significant) number,*" then the format of the address signals is NCD + SN	userinfo's routing number	";rn=routing number" is added to userinfo, with +CC being prefixed to Address Signal's NCD+SN

LEGEND

FCI	Forward Call Indicator	ISUP	ISDN User Part	SIP	Session Initiation Protocol
ISDN	Integrated Services Digital Network	NOA	Nature of Address		

5.3.2.11.5.1.5 P-Asserted-Identity, From, and Privacy Header Fields

[Conditional] The SIP/CCS7 IWF shall follow the mapping in Table 5.3.2.11-25, ISUP CLI Parameters to AS-SIP Header Fields, when mapping from the ISUP Calling Party Number and Generic Address parameters to the AS-SIP P-Asserted-Identity, From, and Privacy header fields in the INVITE message.

Table 5.3.2.11-25. ISUP CLI Parameters to AS-SIP Header Fields

Has a CgPN Parameter with Complete E.164 Number, with Screening Indicator = UPPS or NP[1], and with APRI = "Presentation Allowed" or "Presentation Restricted" Been Received?	Has a Generic Address (Supplemental User Provided Calling Address – Not Screened) with a Complete E.164 Number, and with APRI = "Presentation Allowed" Been Received?	P-Asserted-Identity Header Field	From Header Field: display-name (Optional) and addr-spec	Privacy Header Field
No	No	Header field not included.	Unavailable@Hostportion	Header field not included.
No[2]	Yes	Header field not included.	display-name derived from Generic Address (supplemental calling address) if possible. addr-spec derived from Generic Address (supplemental calling address) address signals or uses network-provided value.	Header field not included.
Yes[1]	No	Derived from CgPN parameter address signals (see Table 5.3.2.11-27).	If APRI = "allowed," display-name derived from CgPN if possible. If APRI = "restricted," display-name is "Anonymous." If APRI = "allowed," addr-spec is derived from CgPN parameter address signals (see Table 5.3.2.11-28) or uses network-provided value. If APRI = "restricted," addr-spec is set to "Anonymous URI."[4]	If CgPN parameter APRI = "restricted," then priv-value =; "id." For other APRI settings, Privacy header is not included or, if included, "id" is not included (see Table 5.3.2.11-29).

Has a CgPN Parameter with Complete E.164 Number, with Screening Indicator = UPPS or NP[1], and with APRI = “Presentation Allowed” or “Presentation Restricted” Been Received?	Has a Generic Address (Supplemental User Provided Calling Address – Not Screened) with a Complete E.164 Number, and with APRI = “Presentation Allowed” Been Received?	P-Asserted-Identity Header Field	From Header Field: display-name (Optional) and addr-spec	Privacy Header Field
Yes[1]	No	Derived from CgPN parameter address signals (see Table 5.3.2.11-27).	display-name may be derived from Generic Address[3] addr-spec is derived from Generic Address address signals (see Table 5.3.2.11-26).	If CgPN parameter APRI = “restricted,” then priv-value =; “id”. For other APRI settings, Privacy header is not included or if included, “id” is not included (see Table 5.3.2.11-29).

NOTES
1. A network-provided CLI in the CgPN parameter may occur on a call from an analog access line. Therefore, to allow the “display” of this network-provided CLI, it must be mapped into the AS-SIP From header. It is also considered suitable to map into the P-Asserted-Identity header.
2. This combination of CgPN and supplemental calling address is an error case, but is shown here to ensure consistent mapping across different implementations.
3. It may be possible to derive the Display name from the Generic Address parameter.
4. The From header may contain an “Anonymous URI,” which would not point to the calling party. RFC 3261 recommends that the display-name component contain “Anonymous.” Anonymous URI itself has the value “anonymous@anonymous.invalid.”

LEGEND

APRI	Address Presentation Restricted Indicator	NP	Network Provided
AS-SIP	Assured Services Session Initiation Protocol	RFC	Request for Comment
CgPN	Calling Party Number	UPPS	User Provided Passed Screening
CLI	Calling Line Identification	URI	Universal Resource Identifier

[Objective] The SIP/CCS7 IWF shall follow the detailed mapping in Table 5.3.2.11-26, Mapping of GAP (Supplemental User Provided Calling Address) to AS-SIP From Header Fields, when mapping from the ISUP Generic Address parameter to the AS-SIP From header field.

Table 5.3.2.11-26. Mapping of GAP (Supplemental User Provided Calling Address) to AS-SIP From Header Fields

ISUP PARAMETER/ FIELD	VALUE	AS-SIP COMPONENT	VALUE
Generic Address Number Qualifier Indicator	"supplemental user provided calling address – not screened"	From header field	display-name (optional) and addr-spec
Nature of Address Indicator	*"national (significant) number"*	addr-spec	Add CC (of the country where the SIP/CCS7 IWF is located) to GAP address signals, then map to AS-SIP URI.
	"international number"		Map complete GAP address signals to AS-SIP URI.
Address Signal	If NOA is *"national (significant) number,"* then the format of the address signal is NDC + SN. If NOA is *"international number,"* then the format of the address signal is CC + NDC + SN.	display-name	display-name shall be mapped from address signal, if possible, and if network policy allows it.
		addr-spec	"+CC" "NDC" "SN" mapped to the appropriate global number portion of URI scheme used.

LEGEND

AS-SIP	Assured Services Session Initiation Protocol
CCS7	Common Channel Signaling System No. 7
ISDN	Integrated Services Digital Network
ISUP	ISDN User Part
IWF	Interworking Function
NOA	Nature of Address
SIP	Session Initiation Protocol
URI	Universal Resource Identifier

[Conditional] The SIP/CCS7 IWF shall follow the detailed mapping in Table 5.3.2.11-27, Mapping of CgPN Parameter to AS-SIP P-Asserted-Identity Header Fields, when mapping from the ISUP Calling Party Number parameter to the AS-SIP P-Asserted-Identity.

Table 5.3.2.11-27. Mapping of CgPN Parameter to AS-SIP P-Asserted-Identity Header Fields

ISUP PARAMETER/ FIELD	VALUE	SIP COMPONENT	VALUE
Calling Party Number		P-Asserted-Identity header field	display-name (optional) and addr-spec
Nature of Address Indicator	*"national (significant) number"*	addr-spec	Add CC (of the country where the SIP/CCS7 IWF is located) to CgPN address signals, then map to URI.
	"international number"		Map complete CgPN address signals to URI.
Address Signal	If NOA is *"national (significant) number,"* then the format of the address signals is NDC + SN. If NOA is *"international number,"* then the format of the address signals is CC + NDC + SN.	display-name	display-name shall be mapped from address signal, if possible, and if network policy allows it.
		addr-spec	"+CC" "NDC" "SN" mapped to the appropriate global number portion of URI scheme used.

LEGEND

CgPN	Calling Party Number	ISUP	ISDN User Part	SS7	Signaling System No. 7
CCS7	Common Channel Signaling System No. 7	IWF	Interworking Function	URI	Universal Resource Identifier
		NOA	Nature of Address		
ISDN	Integrated Services Digital Network	SIP	Session Initiation Protocol		

[Conditional] The SIP/CCS7 IWF shall follow the detailed mapping in Table 5.3.2.11-28, Mapping of ISUP CgPN Parameter to AS-SIP from Header Fields, when mapping from the ISUP CgPN parameter to the AS-SIP From header field.

Table 5.3.2.11-28. Mapping of ISUP CgPN Parameter to AS-SIP From Header Fields

ISUP PARAMETER/ FIELD	VALUE	SIP COMPONENT	VALUE
Calling Party Number		From header field	display-name (optional) and addr-spec
Nature of Address Indicator	*"national (significant) number"*	addr-spec	Add CC (of the country where the SIP/CCS7 IWF is located) to CgPN address signals, then map to user portion of URI scheme used.
	"international number"		Map complete CgPN address signals to user portion of URI scheme used.
Address Signal	If NOA is "*national (significant) number,*" then the format of the address signals is NDC + SN. If NOA is "*international number,*" then the format of the address signals is CC + NDC + SN.	display-name	display-name shall be mapped from Address Signal, if possible and network policy allows it.
		addr-spec	"+CC" "NDC" "SN" mapped to user portion of URI scheme used

LEGEND

CgPN	Calling Party Number
CCS7	Common Channel Signaling System No. 7
ISDN	Integrated Services Digital Network
ISUP	ISDN User Part
IWF	Interworking Function
NOA	Nature of Address
SIP	Session Initiation Protocol
URI	Universal Resource Identifier

[Conditional] The SIP/CCS7 IWF shall follow the detailed mapping in Table 5.3.2.11-29, Mapping of ISUP APRIs into AS-SIP Privacy Header Fields, when mapping from the ISUP Address Presentation Restricted Indicator (APRI) subfield of the Calling Party Number parameter to the AS-SIP Privacy header field.

[Conditional] If the From or the P-Asserted-Identity header field is sent with a sip uri, it shall include the "user=phone" URI parameter.

5.3.2.11.5.1.6 Hop Counter (Max-Forwards)

[Conditional] If the outgoing INVITE message uses AS-SIP, then the Max-Forwards header field value from the Hop Counter value shall be set to an integer equal to the received Hop Counter value multiplied by a factor (F) rounded down. The value of F should be derived by the SIP/CCS7 IWF using the following principles:

Table 5.3.2.11-29. Mapping of ISUP APRIs into AS-SIP Privacy Header Fields

ISUP PARAMETER/ FIELD	VALUE	SIP COMPONENT	VALUE
Calling Party Number		Privacy header field	priv-value
APRI	"presentation restricted"	priv-value	"id," but only included if the P-Asserted-Identity header is included in the AS-SIP INVITE request.
	"presentation allowed"	priv-value	Omit Privacy header or Privacy header without "id" if other privacy service is needed.
NOTE When the CgPN parameter is received, the P-Asserted-Identity header is always derived from it as shown in Table 5.3.2-34.			
LEGEND APRI Address Presentation Restricted Indicator AS-SIP Assured Services Session Initiation Protocol CgPN Calling Party Number		ISDN Integrated Services Digital Network ISUP ISDN User Part SIP Session Initiation Protocol	

1. The Max-Forwards header field for a given message shall never increase, and shall decrease by at least one with each successive visit to an SIP/CCS7 IWF, regardless of intervening interworking. The same is true for the Hop Counter value in the ISUP domain.

2. The initial and successively mapped values of the Max-Forwards header field should be large enough to accommodate the maximum number of hops that might be expected of a validly routed call.

Since the value of F must take into account the topology of the networks that are traversed, it will depend on call origin and destination, and it will be provisioned at the SIP/CCS7 IWF based on network topology, trust domain rules, and bilateral agreement.

5.3.2.11.5.1.7 Precedence

The modeling of the SIP/CCS7 IWF assumes that preemption of a call will occur at a node either in the AS-SIP network or in the CCS7 network. The role of the SIP/CCS7 IWF is limited to interworking the signaling that indicates the relative priority of the calling party.

NOTE: If the SIP/CCS7 IWF controls the bearer path, it may perform preemption as described in UCR 2008, Section 5.3.2.10.5, CCA Support for Admission Control.

[Conditional] The SIP/CCS7 IWF shall populate the RPH in the outgoing AS-SIP INVITE message as follows:

1. If the NI in the received Precedence parameter is “0000,” corresponding to “uc,” the network domain in the RPH shall be coded as “uc.”

2. If the NI in the received Precedence parameter is not “0000,” corresponding to “uc,” then the network domain in the RPH shall be coded as “uc.”

3. The binary MLPP service domain in the received Precedence parameter shall be converted to six characters (0-F, one character per half-octet) and shall be used to populate the precedence-domain in the RPH.

4. If the NI in the received Precedence parameter is “0000,” then the r-priority field in the RPH shall be populated as shown in Table 5.3.2.11-30, Mapping of IAM Precedence Level to RPH Precedence Subfield.

Table 5.3.2.11-30. Mapping of IAM Precedence Level to RPH Precedence Subfield

ISUP PARAMETER/ FIELD	VALUE	SIP COMPONENT	VALUE
Calling Party Number		Privacy header field	priv-value
	“presentation restricted”	priv-value	“id,” but only included if the P-Asserted-Identity header is included in the AS-SIP INVITE message.
	“presentation allowed”	priv-value	Omit Privacy header or Privacy header without “id” if other privacy service is needed.

LEGEND

AS-SIP	Assured Services Session Initiation Protocol	ISDN	Integrated Services Digital Network	ISUP SIP	ISDN User Part Session Initiation Protocol

5. If the NI in the received Precedence parameter is not “0000,” then the r-priority field inthe RPH shall be coded as “0” (“Routine”).

5.3.2.11.5.2 18X Response Received

[Conditional]
Section 5.3.2.11.5.2.1, Receipt of 180 (Ringing) Message, describes procedures on receipt of a 180 (Ringing) message.

Section 5.3.2.11.5.2.2, Receipt of 183 (Session Progress), describes procedures on receipt of a 183 (Session Progress) message.

Local ISUP procedures may generate a backward early ACM (no indication) based on timer expiry. Those procedures are independent of these AS-SIP interworking procedures.

5.3.2.11.5.2.1 Receipt of 180 (Ringing) Message

[Conditional] On receipt of a 180 (Ringing) message, timer T_{OIW2}, if running, is stopped. If a 180 (Ringing) message is received, the SIP/CCS7 IWF shall send either the ACM, if no ACM has previously been sent for this call, or a CPG message, if an ACM has been sent previously for this call.

5.3.2.11.5.2.1.1 Setting for ACM BCIs

[Conditional] Table 5.3.2.11-31, Indicators in the BCI Parameter, and Table 5.3.2.11-32, Default BCIs Values, list the bits of the BCI parameters that are set by the SIP/CCS7 IWF when an ACM is sent. Other BCI parameters are set according to ISUP procedures.

Table 5.3.2.11-31. Indicators in the BCI Parameter

BITS	INDICATORS IN BCI PARAMETER
DC	Called Party’s Status Indicator
I	Interworking Indicator
K	ISUP Indicator
M	ISDN Access Indicator

Table 5.3.2.11-32. Default BCIs Values

PARAMETER	BITS	CODES	MEANING
Interworking Indicator	I	1	Interworking Encountered
ISUP Indicator	K	0	ISUP/BICC not used all the way
ISDN Access Indicator	M	0	Terminating Access Non-ISDN
LEGEND BCI Backward Call Indicator BICC Bearer-Independent Call Control	ISDN Integrated Services Digital Network	ISUP ISDN User Part	

5.3.2.11.5.2.1.2 Settings for Event Information in CPG

[Conditional] On receipt of a 180 (Ringing) message, the SIP/CCS7 IWF shall send a CCS7 CPG message with the Event Indicator bits G F E D C B A set to “alerting” (0 0 0 0 0 0 1) in the Event Information parameter.

5.3.2.11.5.2.2 Receipt of 183 (Session Progress) Message

[Conditional] On receipt of an AS-SIP 183 (Session Progress) message, no ISUP message is sent backward, and ISUP procedures shall continue.

5.3.2.11.5.3 Expiration of T_{OIW2} and Sending Early ACM

[Conditional] When timer $T_{\mathbf{OIW2}}$ expires, the SIP/CCS7 IWF shall return an ACM to the CCS7 network. In the case where the continuity check is performed, the SIP/CCS7 IWF shall withhold sending an ACM until a successful continuity indication has been received.

[Conditional] When returning an ACM to the CCS7 network, the SIP/CCS7 IWF shall return an awaiting answer indication (e.g., ringing tone) toward the calling party.

[Conditional] The Called Party's Status Indicator (Bit DC) of the BCI parameter in the ACM shall be set to "no indication." The other BCI indicators shall be set as described in UCR 2008, Section 5.3.2.11.5.2.1.1, Setting for ACM BCIs.

5.3.2.11.5.4 Circuit (CIC) Query Response Message Received

[Conditional: SIP/CCS7 IWF] After sending a Circuit (CIC) Query message, the SIP/CCS7 IWF expects to receive a Circuit (CIC) Query Response message.

[Conditional] The SIP/CCS7 IWF shall process the Circuit (CIC) Query Response message as described in ANSI T1.113.4, Clause 2.8.2A. If the ISUP procedures result in release of a call, appropriate actions shall be taken on the AS-SIP side.

5.3.2.11.5.5 200 (OK) INVITE Message Received

[Conditional] On receipt of a 200 (OK) INVITE message, the SIP/CCS7 IWF shall stop Timer $T_{\mathbf{OIW2}}$ if it is running.

[Conditional] If the 200 (OK) INVITE message uses AS-SIP, the SIP/CCS7 IWF shall

1. Send an ANM as determined by ISUP procedures. If an ANM is sent as the first backward message on the CCS7 side, the BCI parameter shall be coded with the Called Party's Status Indicator (Bits DC) set to "no indication," and the other BCI parameter indicators shall be set as described in UCR 2008, Section 5.3.2.11.5.2.1.1, Setting for ACM BCIs.

2. Stop any existing "awaiting answer indication" (e.g., ringing tone).

5.3.2.11.5.6 Through Connection, Tones, and Announcements

Through connection of bearer path is applicable only to a SIP/CCS7 IWF that controls the bearer path.

[Conditional] For AS-SIP, through connection at the SIP/CCS7 IWF shall follow the ANSI T1.113.4 procedures for the destination exchange if this functionality is not available at the adjacent AS-SIP node. If the adjacent AS-SIP node does support the ANSI T1.113.4 procedures for through connection at a destination exchange, the SIP/CCS7 IWF shall follow these procedures:

1. Through connection of the bearer path shall be completed dependent on whether preconditions are in use on the AS-SIP side of the call.

2. The bearer path shall be connected in both directions on completion of the bearer setup on the AS-SIP side. This event is indicated by the receipt of an SDP Answer acceptable to the SIP/CCS7 IWF, and an indication that all mandatory preconditions, if any, have been met.

3. The bearer path shall be connected in the forward direction no later than on receipt of a 200 (OK) INVITE message.

[Conditional] For AS-SIP, the following conditions shall result in a ringing tone being played from the SIP/CCS7 IWF:

- 180 (Ringing) received

- ISUP procedures indicate that ringing tone can be applied

- The local arrangements assign the role of destination exchange to the SIP/CCS7 IWF rather than the associated AS-SIP entity

Ringing tone or a progress announcement may already be playing because of T_{OIW2} expiry. See UCR 2008, Section 5.3.2.11.5.3, Expiration of T_{OIW2} and Sending Early ACM.

[Conditional] In the case of ringing tones being played because of T_{OIW2} expiry, no additional ringing tone shall be played.

NOTE: If the associated AS-SIP entity performs the functions of the destination exchange, other tones or announcements may be received from the AS-SIP network.

5.3.2.11.5.7 Release Procedures

5.3.2.11.5.7.1 Receipt of Forward REL

[Conditional] Upon receipt of an ISUP REL message:

1. If a REL message is received before the INVITE request has been sent, the SIP/CCS7 IWF shall take no action on the AS-SIP side other than to terminate local procedures, if any, that are in progress.

2. If a REL message is received before any response has been received to the INVITE request, the SIP/CCS7 IWF shall hold the REL message until an AS-SIP response has been received. At that point, it shall take appropriate release actions.

3. If a REL message is received before a response has been received that establishes a confirmed dialog or early dialog, the SIP/CCS7 IWF shall send a CANCEL request. If the SIP/CCS7 IWF later receives a 200 (OK) INVITE request, then it shall send an ACK message for the 200 (OK) INVITE request and, later, send a BYE request after the ACK message has been sent.

4. If a REL message is received at the SIP/CCS7 IWF after a response has been received that establishes a confirmed dialog or early dialog, the SIP/CCS7 IWF shall send a BYE request. For cases in which no encapsulation is used, for an early dialog only, CANCEL may be used instead.

5. If a REL message is received after the 200 (OK) INVITE request, but before the outgoing side of the SIP/CCS7 IWF has sent the ACK message, then the SIP/CCS7 IWF shall send the ACK message before sending a BYE request.

NOTE: Depending on local policy, a Reason header field containing the received (ITU-T Recommendation Q.850 or ANSI T1.113) cause value of the REL message may be added to the CANCEL or BYE request. If the Coding Standard field of the Cause Indicators parameter is set to “ANSI Standard,” the Protocol parameter of the Reason header is set to “ANSI,” and if the Coding standard is set to “ITU-T Standard,” the Protocol parameter is set to “Q.850.” The mapping of the Cause Indicators parameter to the Reason header is shown in Table 5.3.2.11-20, Receipt of RSC, GRS, or CGB Messages.

5.3.2.11.5.7.2 Receipt of Backward BYE

[Conditional] On receipt of an AS-SIP BYE request, the SIP/CCS7 IWF shall send a CCS7 REL message.
[Conditional] For the AS-SIP case, if a Reason header with a Protocol parameter set to either “Q.850” or “ANSI” is included in the BYE request, then the appropriate cause value may be mapped to the cause value field in the REL message depending on the local policy. The mapping of the Reason header to the Cause Indicators parameter is shown in Table 5.3.2.11-15, Mapping of AS-SIP Reason Header Fields into Cause Indicators Parameter (see UCR 2008, Section 5.3.2.11.4.12.1, Receipt of BYE or CANCEL). In case a value is not available from the

Reason header field, the Cause Indicators parameter shall be encoded as "normal clearing" (Cause Value No. 16).

5.3.2.11.5.7.3 Autonomous REL at the SIP/CCS7 IWF

Table 5.3.2.11-33, Autonomous REL at SIP/CCS7 IWF, shows the trigger events at the SIP/CCS7 IWF and the release initiated by the SIP/CCS7 IWF when the call is traversing from ISUP to AS-SIP.

Table 5.3.2.11-33. Autonomous REL at SIP/CCS7 IWF

REL ON THE CCS7 SIDE CAUSE PARAMETER	TRIGGER EVENT	AS-SIP SIDE
As determined by ISUP procedure	COT received with the Continuity Indicators parameter set to "continuity check failed," or the ISUP timer T8 expires.	Send CANCEL or BYE request according to the rule described in Section 5.3.2.11.5.7.1.
REL message with Cause Value No. 47 (resource unavailable, unspecified)	Internal resource reservation unsuccessful.	As determined by AS-SIP procedure.
As determined by ISUP procedure.	ISUP procedures result in generation of autonomous REL message on the ISUP side.	Send CANCEL or BYE request, according to the rule described in Section 5.3.2.11.5.7.1.
Depending on the AS-SIP release reason	AS-SIP procedures result in a decision to release the call.	As determined by AS-SIP procedure.

LEGEND

AS-SIP	Assured Services Session Initiation Protocol	COT	Customer Originated Trace	ISUP	ISDN User Part
CCS7	Common Channel Signaling No. 7	ISDN	Integrated Services Digital Network	REL	Release

[Conditional] If, after answer, ISUP procedures result in autonomous REL message from the SIP/CCS7 IWF, then a BYE request shall be sent on the AS-SIP side.

5.3.2.11.5.7.4 Reset Circuit, Circuit Group Reset, or Circuit Group Blocking Message Received

Table 5.3.2.11-34, Receipt of RSC, GRS, or CGB Messages, shows the message sent by the SIP/CCS7 IWF upon receipt of an ISUP RSC message, GRS message, or CGB message with the Circuit Group Supervision Message Type Indicator coded as "hardware failure oriented." On receipt of a GRS or CGB message, one AS-SIP message is sent for each call association. Therefore, multiple AS-SIP messages may be sent on receipt of a single GRS or CGB message.

Table 5.3.2.11-34. Receipt of RSC, GRS, or CGB Messages

MESSAGE RECEIVED FROM ISUP	MESSAGE SENT TO AS-SIP NETWORK
RSC	CANCEL or BYE
GRS	CANCEL or BYE
CGB with the Circuit Group Supervision Message Type Indicator coded *"hardware failure oriented"*	CANCEL or BYE

LEGEND

AS-SIP	Assured Services Session Initiation Protocol	ISDN	Integrated Services Digital Network
CGB	Circuit Group Blocking Message	ISUP	ISDN User Part
GRS	Circuit Group Reset Message	RSC	Reset Circuit Message

[Conditional] The SIP/CCS7 IWF shall process received CCS7 RSC, GRS, or CGB messages as shown in Table 5.3.2.11-34, Receipt of RSC, GRS, or CGB Messages. The SIP/CCS7 IWF shall send a CANCEL or BYE message according to the rule described in Section 5.3.2.11.5.7.1, Receipt of Forward REL.

Depending on local policy, a Reason header field containing the (ITU-T Recommendation Q.850 or ANSI T1.113) cause value of the REL message sent by the SIP/CCS7 IWF may be added to the AS-SIP message (BYE or CANCEL).

5.3.2.11.5.7.5 3XX, 4XX, 5XX, or 6XX Response INVITE Received

[Conditional] The SIP/CCS7 IWF shall handle receipt of a 3XX Redirection message, if received in a response as part of a valid dialog, according to the AS-SIP protocol, resulting in invocation of the local routing function.

The remainder of this section applies only to the 4XX, 5XX, and 6XX response cases.

[Conditional] If a Reason header is included in a received 4XX, 5XX, or 6XX message, then the SIP/CCS7 IWF shall map the cause value of the Reason header to the ISUP Cause Value field in the CCS7 REL message. The mapping of the Reason header to the Cause Indicators parameter shall be as shown in Table 5.3.2.11-15, Mapping of AS-SIP Reason Header Fields into Cause Indicators Parameter.

[Conditional] If no Reason header is included in a received 4XX, 5XX, or 6XX message, then the SIP/CCS7 IWF shall use the mapping of the status code to cause value on receipt of a 4XX, 5XX, or 6XX final response to the INVITE request into the AS-SIP network side, as shown in Table 5.3.2.11-35, Mapping of 4XX, 5XX, or 6XX to REL Message.

Table 5.3.2.11-35. Mapping of 4XX, 5XX, or 6XX to REL Message

REL (CAUSE CODE)	4XX/5XX/6XX SIP MESSAGE	REMARKS

REL (CAUSE CODE)	4XX/5XX/6XX SIP MESSAGE	REMARKS
127 Interworking	400 Bad Request	
127 Interworking	401 Unauthorized	Note 1
127 Interworking	402 Payment Required	
127 Interworking	403 Forbidden	
1 Unallocated number	404 Not Found	
127 Interworking	405 Method Not Allowed	
127 Interworking	406 Not Acceptable	
127 Interworking	407 Proxy Authentication Required	Note 1
127 Interworking	408 Request Timeout	
22 Number changed (without diagnostic)	410 Gone	
127 Interworking	413 Request Entity Too Long	Note 1
127 Interworking	414 Request-URI Too Long	Note 1
127 Interworking	415 Unsupported Media Type	Note 1
127 Interworking	416 Unsupported URI Scheme	Note 1
127 Interworking	420 Bad Extension	Note 1
127 Interworking	421 Extension Required	Note 1
127 Interworking	423 Interval Too Brief	
20 Subscriber absent	480 Temporarily Unavailable	
127 Interworking	481 Call/Transaction Does Not Exist	
127 Interworking	482 Loop Detected	
127 Interworking	483 Too Many Hops	
28 Invalid Number format	484 Address Incomplete	Note 1
127 Interworking	485 Ambiguous	
17 User busy	486 Busy Here	
127 Interworking or no mapping (Note 3)	487 Request Terminated	Note 2
127 Interworking	488 Not Acceptable Here	
No mapping.	491 Request Pending	Note 2
127 Interworking	493 Undecipherable	
127 Interworking	500 Server Internal Error	
127 Interworking	501 Not Implemented	
127 Interworking	502 Bad Gateway	
127 Interworking	503 Service Unavailable	Note 1
127 Interworking	504 Server Timeout	
127 Interworking	505 Version Not Supported	Note 1
127 Interworking	513 Message Too Large	Note 1
127 Interworking	580 Precondition Failure	Note 1
17 User busy	600 Busy Everywhere	
21 Call rejected	603 Decline	
1 Unallocated number	604 Does Not Exist Anywhere	
127 Interworking	606 Not Acceptable	

NOTES
1. This response may be handled entirely on the AS-SIP side; if so, it is not interworked.
2. This response does not terminate an AS-SIP dialog, but only a specific transaction within it.
3. No mapping if the SIP/CCS7 IWF previously issued a CANCEL request for the INVITE.

LEGEND

AS-SIP	Assured Services Session Initiation Protocol	REL	Release

REL (CAUSE CODE)	4XX/5XX/6XX SIP MESSAGE	REMARKS
CCS7 Common Channel Signaling No. 7	SIP Session Initiation Protocol	
IWF Interworking Function	URI Universal Resource Identifier	

[Conditional] When the response to the INVITE request results in the sending of a REL message with a Cause Code No. 127, Interworking, the Location field shall be set to “network beyond interworking point.”

In all cases where AS-SIP itself or this section specifies additional AS-SIP behavior related to the receipt of a particular INVITE response, these procedures should be followed in preference to the immediate sending of a REL message to the CCS7 network.

[Conditional] If there are no AS-SIP procedures associated with this response, the REL message shall be sent to the CCS7 network immediately.

It is possible that receipt of certain 4XX, 5XX, and 6XX responses to an INVITE request will not result in any REL message being sent to the CCS7 network. For example, if a 401 (Unauthorized) response is received and the SIP/CCS7 IWF successfully initiates a new INVITE request containing the correct credentials, the call will proceed.

If no further reference is given in the Remarks column, then this means that the AS-SIP response is interworked to a CCS7 REL message sent on the ISUP side of the SIP/CCS7 IWF with the cause value indicated within the table. In cases where further reference is indicated, the behavior of the SIP/CCS7 IWF is described within the referred-to clause. However, Table 5.3.2.11-36, Interworking Timer, indicates the “eventual” behavior of the SIP/CCS7 IWF in the case that further measures taken on the AS-SIP side of the call (to try to sustain the call) fail, resulting in the requirement to send a REL message into the CCS7 network with the cause value indicated.

5.3.2.11.6 Interworking Timer

The SIP/CCS7 IWF requires one timer that is specific to its interworking functionality. Table 5.3.2.11-36, Interworking Timer, summarizes the timer T_{OIW2}. The value of T_{OIW2} is set between 4 and 14 seconds (with a default value of 4 seconds). The timer is started when an INVITE request is sent (unless an ACM has already been sent for this call). The timer is stopped on receipt of any of the following messages:

- 180 (Ringing)
- 183 (Session Progress) with an encapsulated ACM
- 200 (OK) INVITE

Table 5.3.2.11-36. Interworking Timer

TIME-OUT VALUE	CAUSE FOR INITIATION	NORMAL TERMINATION	AT EXPIRY
4-14 seconds (default of 4 seconds)	Sending of INVITE request unless the ACM has already been sent	On reception of 180 (Ringing), 183 (Session Progress) with encapsulated ACM, or 200 (OK) INVITE request	Send early ACM. For AS-SIP case, send the awaiting answer indication (e.g., ring tone) or appropriate progress announcement to the calling party.
LEGEND ACM Address Complete Message AS-SIP Assured Services Session Initiation Protocol			

[Conditional] The SIP/CCS7 IWF shall initiate the timer when an INVITE request is sent, unless an ACM has already been sent for this call.

[Conditional] At the expiry of the timer, the SIP/CCS7 IWF shall send an early ACM into the CCS7 network.

[Conditional] For the AS-SIP case only, the SIP/CCS7 IWF shall send the awaiting answer indication (e.g., ring tone) or appropriate progress announcement to the calling party.

5.3.2.12 Media Gateway Requirements

5.3.2.12.1 Introduction

This section provides GSRs for the MG function in the following network appliances:

- LSC
- MFSS
- WAN SS

The LSC and MFSS have defined designs that include an MGC function and one or more MG functions.

The scope of these MG requirements covers the following areas:

1. Physical interfaces and protocols supported on the TDM side of the MG include the following:

    a. DoD CCS7 trunks (The TDM media trunks terminate on the MG; the TDM signaling links terminate on the separate SG, which is discussed in Section 5.3.2.13, Signaling Gateway Requirements.)

b. ISDN PRI trunks (The TDM media (B channels) channels and the TDM signaling channels (D channels) both terminate on the MG.)

c. CAS trunks (Both DTMF and MF; the TDM channel that carries both the media and the signaling terminates on the MG.)

2. VoIP interfaces and protocols supported on the IP side of the MG include the following:

a. Interface to the IP router network and the LAN (ASLAN, LANs internal to a UC product) that the network appliance is connected to

b. VoIP protocol stacks supporting IP, IPSec, UDP, TCP, SCTP, and SRTP

c. Secure VoIP media streams, packetized using IP, UDP, and SRTP, IAW UCR 2008, Section 5.4, Information Assurance Requirements

d. Secure VoIP signaling messages, packetized using IPSec, and UDP or TCP or SCTP, IAW, Section 5.4, Information Assurance Requirements

(1) H.248 signaling messages, for MGC control of DoD CCS7, ISDN PRI, and CAS trunks, if the supplier supports ITU-T Recommendation H.248

(2) ISDN PRI signaling messages, for MGC control of ISDN PRI trunks

3. Support for the following VoIP codecs, at a minimum, on the IP side of the MG:

a. ITU-T Recommendation G.711 (uncompressed voice, both North American (μ-law and International A-law))

b. ITU-T Recommendation G.723.1

c. ITU-T Recommendation G.729

4. Support for FoIP on the IP side of the MG

5. Support for voiceband MoIP on the IP side of the MG. The following terms define "Modem over IP" traffic, as used in the UCR 2008. The terms are listed here to clarify that SCIP over IP streams are a subset of all possible modem relay streams. In the UCR 2008, the term SCIP over IP can be considered synonymous with the transmission of SCIP over V.150.1 Modem Relay. These terms also appear in Appendix A, Definitions, Abbreviations and Acronyms, and References.

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

b. Modem Relay. A subset of MoIP, in which modem termination is used at gateways, thereby allowing only the baseband data to reach the packet network.

c. Voiceband Data (Modem Pass-Through). A subset of MoIP in which modem signals are transmitted over the voice channel of a packet network.

d. SCIP over IP. The transport of SCIP information over an IP network. The SCIP traffic can be transmitted over an IP network in many ways, but currently, the U.S. Government requires SCIP devices to support transmission of SCIP on IP networks via V.150.1 Modem Relay.

6. Support for SCIP over IP on the IP side of the MG. As noted previously, SCIP over IP streams are a subset of all possible modem relay streams. In the UCR 2008, the term SCIP over IP is synonymous with the transmission of SCIP over V.150.1 Modem Relay. For SCIP over IP calls, the MG supports V.150.1 Modem Relay traffic IAW ITU Recommendation V.150.1 and NSA document SCIP 216 on the IP side of the MG.

7. Support for 64-kbps unrestricted digital information (clear channel) ISDN over IP on the IP side of the MG.

5.3.2.12.2 Overview of the MG and MGC Functions

Media Gateway is a generic term for a Trunk Gateway (TG) and for an Access Gateway (AG). Thus, MG requirements apply to TGs and to AGs.

Figure 5.3.2.12-1, MGC – MG Layered Interface, illustrates the relationship between the MGC, a component of the CCA, and a generic MG.

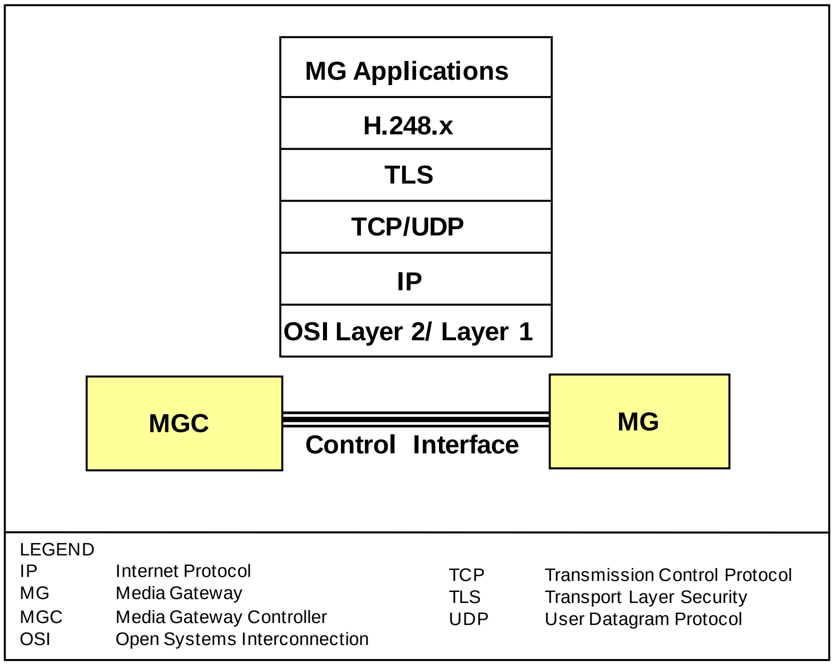

MG Applications
H.248.x
TLS
TCP/UDP
IP
OSI Layer 2/ Layer 1
MGC
Control Interface
MG
LEGEND
IP Internet Protocol
MG Media Gateway
MGC Media Gateway Controller
OSI Open Systems Interconnection
TCP Transmission Control Protocol
TLS Transport Layer Security
UDP User Datagram Protocol

Figure 5.3.2.12-1. MGC – MG Layered Interface

Figure 5.3.2.12-2, MG Trunk Function, illustrates the MG trunk function.

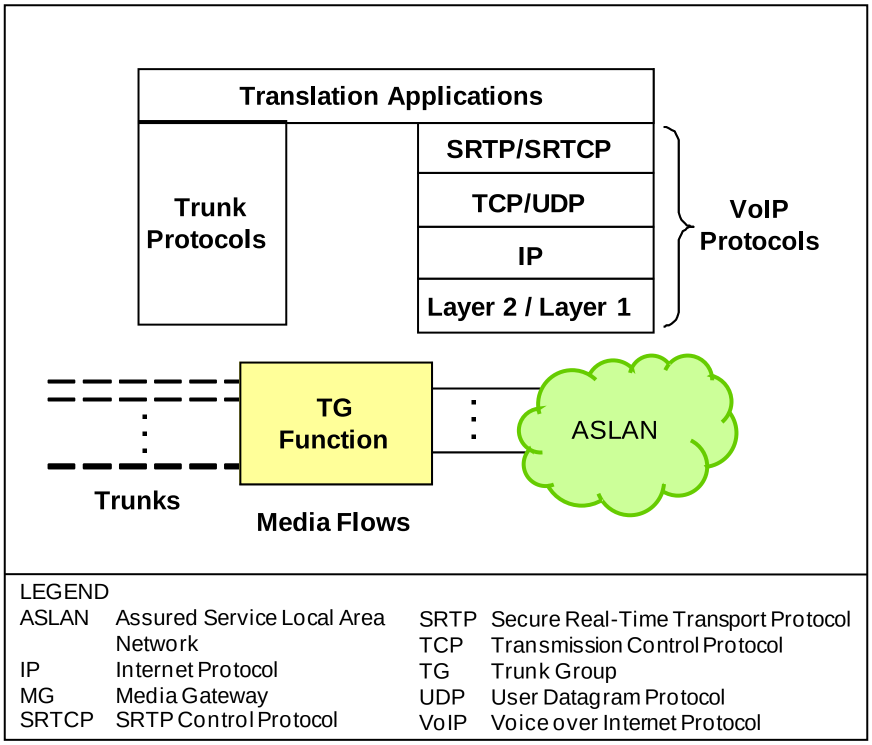

Translation Applications
Trunk Protocols
SRTP/SRTCP
TCP/UDP
IP
Layer 2 / Layer 1
VoIP Protocols
TG Function
ASLAN
Trunks
Media Flows
LEGEND
ASLAN Assured Service Local Area Network
IP Internet Protocol
MG Media Gateway
SRTCP SRTP Control Protocol
SRTP Secure Real-Time Transport Protocol
TCP Transmission Control Protocol
TG Trunk Group
UDP User Datagram Protocol
VoIP Voice over Internet Protocol

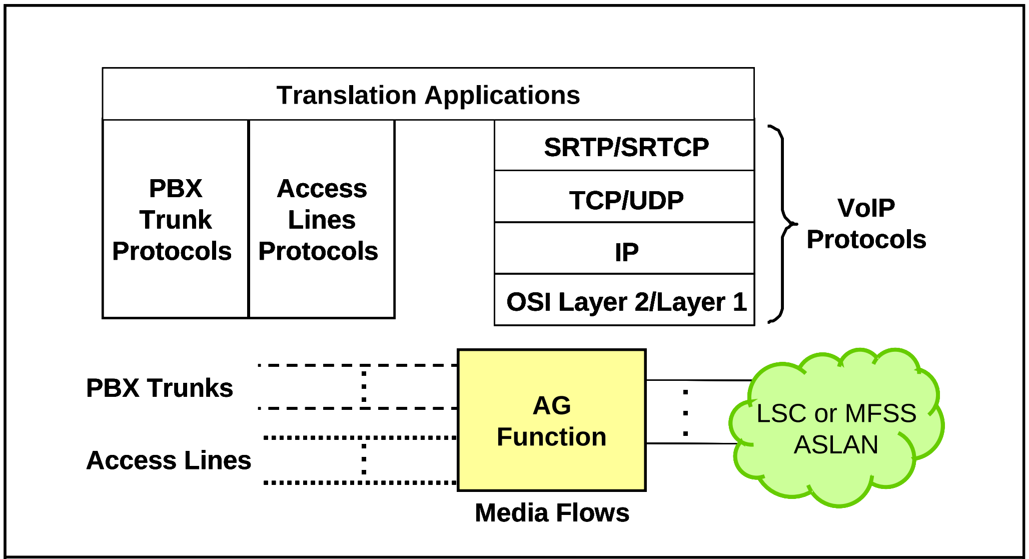
Figure 5.3.2.12-2. MG Trunk Function

5.3.2.12.2.1 Primary Trunk Functions and Interfaces

An MG may support a trunk-side interface to circuit-switched telephone networks. It terminates circuit-switched trunks in the circuit-switched networks and packet flows in the DISN Core network and, thus, provides functions such as media translation. The MG can set up and manage media flows through the Core network when instructed by the CCA. It is associated with a specific CCA that provides it with the necessary call control instructions.

5.3.2.12.2.2 Primary Access Functions and Interfaces

An MG may support line-side and trunk-side interfaces to the voice network end users. Traditional telephones and PBXs currently used in the PSTN, as well as ISDN BRI telephones, ISDN BRI terminals, and ISDN-capable PBXs using PRIs, can access the DISN Core network through the MG. The MG provides functions, such as packetization and echo control, for its end users' information streams, and is associated with a specific CCA that provides the necessary call control and service control instructions. On receiving the appropriate commands from its CCA, the MG provides Call Control functions such as audible ringing and power ringing, as well as Service Control functions. The MG also is capable of setting up transport connections through the DISN Core network when instructed to do so by the CCA (see Figure 5.3.2.12-3, MG Primary Access Functions and Interfaces).



LEGEND

AG	Access Gateway	PBX	Private Branch Exchange
ASLAN	Assured Service Local Area Network	SRTCP	SRTP Control Protocol
IP	Internet Protocol	SRTP	Secure Real-Time Transport Protocol
LSC	Local Session Controller	TCP	Transmission Control Protocol
MFSS	Multifunction Softswitch	UDP	User Datagram Protocol
OSI	Open Systems Interconnection	VoIP	Voice over Internet Protocol

Figure 5.3.2.12-3. MG Primary Access Functions and Interfaces

5.3.2.12.2.3 MGC Functions

The requirements in this section allow for two options for the Gateway Control Protocol in the MGC and the MG as follows:

1. An industry-standard Gateway Control Protocol, using an open interface between the MGC and the MG. This protocol assumes MG-to-MGC communication over IP and the LAN that the appliance is connected to. This LAN is the ASLAN for the LSC and MFSS. (In some cases, this LAN may be the Internal LAN of the UC product, where the UC product also contains the LSC or the MFSS. In these cases, the Internal LAN of the UC product is not an ASLAN.)

   The industry-standard Gateway Control Protocol used in these requirements is ITU-T Recommendation H.248.1.

2. A supplier-specific Gateway Control Protocol, using a closed (supplier-proprietary) interface between the MGC and the MG. This supplier-specific protocol may use MGC-to-MG communication over IP and the LAN that the appliance is connected to (ASLAN or Internal LAN for the UC product), or it may use separate physical, data link, and network layer interfaces that are also proprietary to the supplier.

   The MGC function is part of the CCA function in the LSC and MFSS, which in turn is part of the SCS functions in these appliances. The MG function is a standalone appliance function in the LSC and MFSS, and is not part of any other appliance function.

The role of the MGC within an LSC and MFSS is to

1. Control all MGs within the LSC and MFSS.

2. Control all trunks (e.g., DoD CCS7, PRI, or CAS) within each MG.

3. Control all signaling and media streams on each trunk within each MG.

4. Accept IP-encapsulated signaling streams from an SG or MG, and return IP-encapsulated signaling streams to the SG or MG accordingly.

The MGC and the MG that it controls are considered “Conditional – Deployable” for the LSC, and “Required” for the MFSS.

5.3.2.12.3 Role of the MG in Appliances

The MG provides circuit-switched trunk termination for DoD CCS7, PRI, and CAS trunks, and TDM/VoIP interworking. The MG is controlled by the MGC. The protocol that the MGC uses to control the MG can be ITU-T Recommendation H.248 (specifically, H.248.1) or a proprietary protocol chosen by the LSC supplier.

5.3.2.12.3.1 Role of the MG in the LSC

Figure 5.3.2.12-4, Functional Reference Model – LSC, illustrates the reference model for the LSC, including the VoIP MG and MGC.

The roles of the MG within the LSC are as follows:

1. The MG terminates all TDM trunks that interconnect the LSC with TDM networks, including the following:

    a. DoD TDM networks (e.g., DSN, including EO and Tandem switches within the DSN), both in the United States and worldwide

    b. PSTNs, both in the United States and worldwide

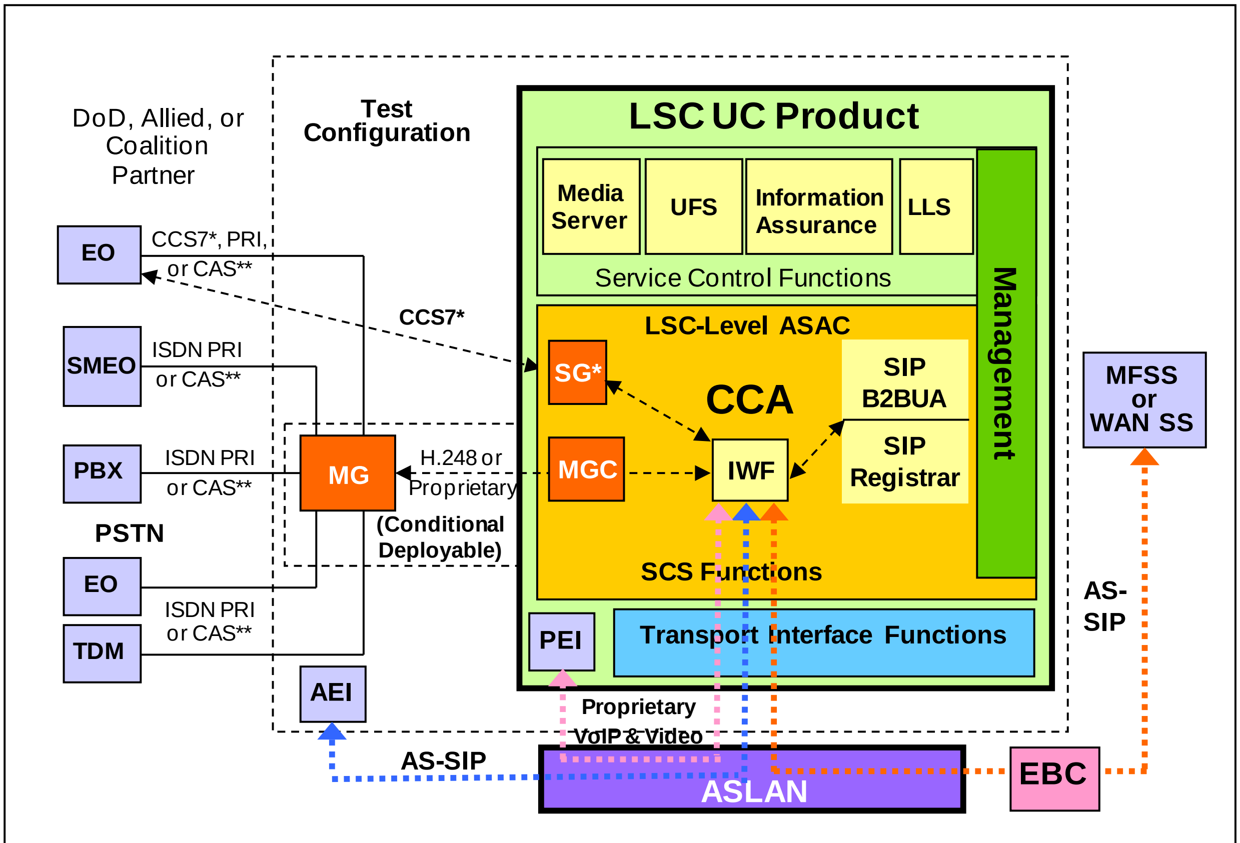
    c. Allied and U.S. coalition partner TDM networks

2. The MG terminates all TDM trunks that interconnect the LSC with TDM PBXs within the same DoD B/P/C/S.

3. The MG supports the physical interconnection of the following TDM trunk groups with the LSC:

    a. **[Conditional: LSC]** DoD CCS7 trunk groups
    b. ISDN PRI trunk groups (for both U.S. PRI and foreign country PRI)
    c. **[Conditional: U.S. and foreign country CAS]** CAS trunk groups

    Media gateway support for these TDM trunk groups is expected to be identical to the support for these trunk groups in DoD TDM PBXs, EOs, Tandem switches, and MFSs today, as specified in UCR 2008, Section 5.2, Circuit-Switched Capabilities and Features.



*Support for an SG & CCS7 is Conditional for an LSC.
**Support for CAS is Conditional for an LSC.

LEGEND:

AEI	AS-SIP End Instrument	MGC	Media Gateway Controller
ASAC	Assured Service Admission Control	PBX	Private Branch Exchange
ASLAN	Assured Services Local Area Network	PEI	Proprietary End Instrument
AS-SIP	Assured Services Session Initiation Protocol	PRI	Primary Rate Interface
B2BUA	Back-to-Back User Agent	PSTN	Public Switched Telephone Network
CAS	Channel Associated Signaling	SCS	Session Control and Signaling
CCS7	Common Channel Signaling No. 7	SG	Signaling Gateway
DoD	Department of Defense	SIP	Session Initiation Protocol
EBC	Edge Border Controller	SMEO	Small End Office
EO	End Office	SS	Softswitch
ISDN	Integrated Services Digital Network	TDM	Time Division Multiplexer
IWF	Interworking Function	UC	Unified Capabilities
LLS	Local Location Service	UFS	User Features and Services
LSC	Local Session Controller	VoIP	Voice over Internet Protocol
MFSS	Multifunction Softswitch	WAN	Wide Area Network
MG	Media Gateway		

Note: The PEI (using Proprietary VoIP and Video) is part of the LSC UC Product; the AEI (using AS-SIP VoIP and Video) is not.

Figure 5.3.2.12-4. Functional Reference Model – LSC

4. **[Conditional]** In the DoD CCS7 case , the MG is responsible for terminating the TDM media trunks (on the TDM side), and for terminating the VoIP/FoIP/MoIP media streams (on the VoIP side). In these cases, the separate SG is responsible for terminating the TDM CCS7 signaling links and the VoIP/FoIP/MoIP signaling streams.

5. In the PRI and CAS cases, the MG is responsible for terminating the TDM media trunks <u>and</u> signaling links on the TDM side, and for terminating the VoIP/FoIP/MoIP media streams <u>and</u> signaling streams on the VoIP side.

6. On calls that traverse the MG, the MG converts TDM media streams to VoIP, FoIP, or MoIP media streams, and converts VoIP, FoIP, or MoIP media streams to TDM media streams.

7. The MG supports interconnection of VoIP, FoIP, and MoIP media streams with the following LSC functions and end-user devices:

    a. **[Required: LSC MG]** The LSC media server, which provides tones and announcements for LSC calls and LSC features

    b. **[Conditional: LSC MG]** Proprietary VoIP, FoIP, and MoIP EIs on the LSC (when these EIs are supported on the LSC)

    c. **[Conditional: LSC MG]** Proprietary SIP EIs on the LSC (when these EIs are supported on the LSC)

    d. **[Conditional: LSC MG]** Proprietary H.323 EIs on the LSC (when these EIs are supported on the LSC)

    e. **[Required: LSC MG]** AS-SIP VoIP, FoIP, and MoIP AEIs on the LSC

8. On ISDN PRI calls that traverse the MG, the MG converts TDM signaling streams to VoIP signaling streams, and it converts VoIP signaling streams to TDM signaling streams. When H.248 control is used, the MG will send and receive encapsulated PRI signaling to and from the CCA.

9. On CAS trunk calls that traverse the MG, the MG converts TDM signaling streams to VoIP signaling streams, and it converts VoIP signaling streams to TDM signaling streams. When H.248 control is used, the MG will translate between CAS signaling and H.248 protocol messages to and from the CCA.

10. **[Conditional – Deployable: LSC MG]** The MG and the MGC that controls the MG are considered “Conditional – Deployable” for the LSC. Some LSC suppliers may include an MGC and MG in their Deployable LSC product, and other LSC suppliers may not. Those suppliers who do should follow the MG requirements defined in UCR 2008.

5.3.2.12.3.1.1 LSC MG VoIP Signaling Interfaces

The LSC MG supports the VoIP signaling interfaces shown in Table 5.3.2.12-1, LSC MG Support for VoIP Signaling Interfaces. The complete signaling requirements for the LSC are summarized in Table 5.3.2.7-2, LSC Support for VoIP and Video Signaling Interfaces.

Table 5.3.2.12-1. LSC MG Support for VoIP Signaling Interfaces

FUNCTIONAL COMPONENT	VoIP SIGNALING INTERFACES	VoIP SIGNALING PROTOCOLS
MG and MGC (CCA)	MG – to – MGC (CCA)	ITU-T H.248 over IP (used with DoD CCS7, ISDN PRI, and CAS trunks)
MG and MGC (CCA)	MG – to – MGC (CCA)	ISDN PRI over IP (North American National ISDN Version, used with ISDN PRI trunks only)
MG and MGC (CCA)	MG – to – MGC (CCA)	Proprietary Supplier Protocols (used as an alternative to ITU-T H.248 over IP and ISDN PRI over IP) (used with DoD CCS7, ISDN PRI, and CAS trunks)

LEGEND

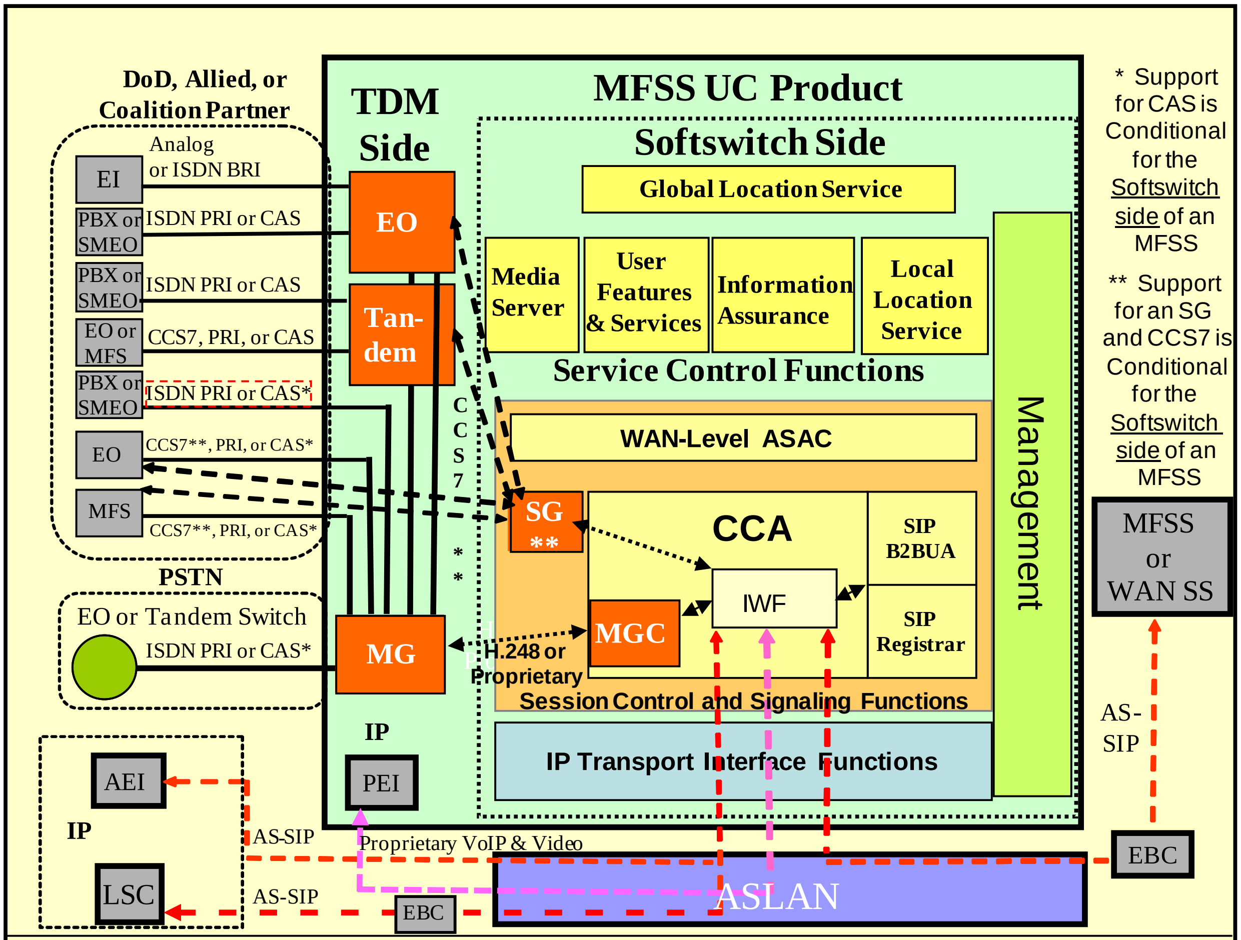
CAS	Channel Associated Signaling	ISDN	Integrated Services Digital Network
CCA	Call Connection Agent	MG	Media Gateway
CCS7	Common Channel Signaling No. 7	MGC	Media Gateway Controller
DoD	Department of Defense	PRI	Primary Rate Interface
IP	Internet Protocol	VoIP	Voice over IP
ITU-T	International Telecommunications Union – Telecommunication		

5.3.2.12.3.2 Role of the MG in the MFSS

Figure 5.3.2.12-5, Functional Reference Model – MFSS, provides the functional reference model of the MFSS. The role of the MG in the MFSS is identical to the role of the MG in the LSC (including the underlying assumptions, roles of the MG and MGC, interactions with other LSC components, and VoIP signaling interfaces), with the following exceptions and extensions:

1. The MG in the MFSS assists the MFSS CCA in providing call denial treatments for CAC, and call preemption treatments for LSC-Level ASAC and WAN-Level ASAC Policing. The MFSS supports LSC-Level ASAC for admission control for calls to and from EIs that it serves directly. The MFSS also supports WAN-Level ASAC Policing for admission control for calls to and from LSCs that it serves directly.

2. The MG in the MFSS supports DoD CCS7 trunks **[Conditional]**, in addition to supporting ISDN PRI **[Required]** and CAS trunks **[Conditional]**. Support for these DoD CCS7 trunks is a conditional requirement for the MFSS MG and the LSC MG.



LEGEND:

AEI	AS-SIP End Instrument
ASAC	Assured Service Admission Control
ASLAN	Assured Services Local Area Network
AS-SIP	Assured Services Session Initiation Protocol
B2BUA	Back-to-Back User Agent
BRI	Basic Rate Interface
CAS	Channel Associated Signaling
CCA	Call Connection Agent
CCS7	Common Channel Signaling No. 7
DoD	Department of Defense
EBC	Edge Border Controller
EI	End Instrument
EO	End Office
IA	Information Assurance
IP	Internet Protocol
ISDN	Integrated Services Digital Network
IWF	Interworking Function
LSC	Local Session Controller
MFS	Multifunction Switch
MFSS	Multifunction Softswitch
MG	Media Gateway
MGC	Media Gateway Controller
PBX	Private Branch Exchange
PEI	Proprietary End Instrument
PRI	Primary Rate Interface
PSTN	Public Switched Telephone Network
SCS	Session Control and Signaling
SG	Signaling Gateway
SIP	Session Initiation Protocol
SMEO	Small End Office
SS	Softswitch
SUT	System Under Test
TDM	Time Division Multiplexer
UC	Unified Capabilities
VoIP	Voice over Internet Protocol
WAN	Wide Area Network

Note: The PEI (using Proprietary VoIP and Video) is part of the MFSS UC Product; the AEI (using AS-SIP VoIP and Video) is not.

Figure 5.3.2.12-5. Functional Reference Model – MFSS

NOTE: An LSC within an MFSS will serve a set of (MFSS-internal) LSC EIs and MGs. These LSC EIs and MGs will exchange media streams with EIs and MGs on other LSCs located elsewhere on the DISN WAN. In addition, the MFSS EBC controls these media streams between the (MFSS-internal) LSC EIs and MGs connected to the MFSS ASLAN, and EIs and MGs on other LSCs, where separate ASLANs are connected to the DISN WAN.

5.3.2.12.3.2.1 MG Requirements for Interactions between the Softswitch and TDM Sides of the MFSS

The TDM side of the MFSS provides EO and Tandem functions that allow the MFSS to support connectivity to existing TDM switches in DoD networks (i.e., CONUS and Global), allied and coalition networks, and the PSTN worldwide (i.e., CONUS and Global). In addition, the EO function of the TDM side of the MFSS supports TDM users (i.e., analog and ISDN EIs). The softswitch side of the MFSS provides the IP-based features of an LSC with additional features as required to serve as a network-level softswitch.

The CCA/SG/MGC/MG complex in the MFSS must provide Interoperability between the softswitch side and TDM side in the MFSS, using connections based on CCS7, U.S. PRI, or U.S. CAS signaling. In this case, some high-level requirements for this interworking are needed. These high-level requirements are included in this section.

Internal MG connections are used when connecting the softswitch and the TDM sides of an MFSS.

An "external MG trunk group" is an MFSS trunk group that connects an MFSS MG with the following:

- The TDM EO or TDM Tandem component of another MFSS in the network
- The MGC/MG component of an LSC or another MFSS in the network
- A TDM PBX, SMEO, EO, Tandem, or MFS in a DoD TDM network
- A TDM PBX, EO, or Tandem in the U.S. PSTN or a foreign country PSTN

[Required] The MFSS MG shall be able to support MG trunk groups (referred to as internal MG connections) that either interconnect the SS (VoIP) side of the MFSS with the EO or Tandem functions on the TDM side of the MFSS.

[Conditional] When a DoD CCS7 connection is used between the SS and TDM sides of the MFSS, the MFSS MG shall interact with the MFSS MGC so that

- DoD CCS7 signaling is used between the S and TDM sides.

- The CCS7 version of the MLPP feature operates correctly between the SS and TDM sides of the MFSS for both VoIP-to-TDM calls and TDM-to-VoIP calls over this connection.

[Required] When a U.S. ISDN PRI connection is used between the SS and TDM sides of the MFSS, the MFSS MG shall interact with the MFSS MGC so that

1. U.S. ISDN PRI signaling (National ISDN PRI signaling, with the precedence level IE and related MLPP IEs included) is used between the SS and TDM sides.

2. The T1.619/T1.619a version of the ISDN PRI MLPP feature operates correctly between the SS and TDM sides of the MFSS for both VoIP-to-TDM calls and TDM-to-VoIP calls over this connection.

[Conditional] When a U.S. CAS trunk group is used between the SS and TDM sides of the MFSS, the MFSS MG shall interact with the MFSS MGC so that

1. U.S. CAS trunk signaling is used between the SS and TDM sides.

2. The UCR 2008, Section 5.2, Circuit-Switched Capabilities and Features, version of the CAS trunk MLPP feature operates correctly between the SS and TDM sides of the MFSS for both VoIP-to-TDM calls and TDM-to-VoIP calls over this trunk group.

[Required] The MFSS MG shall interact with the MFSS MGC so that internal MG connections between the SS and TDM sides of the MFSS support:

- TDM calls between the TDM EO/Tandem and VoIP PEIs/AEIs on the MFSS, allowing calls from EO lines to MFSS PEIs/AEIs, and calls from EO and Tandem trunks to MFSS PEIs/AEIs.

- TDM calls between the TDM EO/Tandem and the EBC on the MFSS, allowing calls from EO lines to the EBC (and other appliances on the DISN WAN), and calls from EO and Tandem trunks to the EBC (and other appliances on the DISN WAN).

- TDM calls between the TDM EO/Tandem and external MG trunk groups on the MFSS, allowing calls from EO lines to external MG trunk groups, and calls from EO and Tandem trunks to external MG trunk groups.

- TDM calls between the TDM EO/Tandem and local MG trunk groups on the MFSS, allowing calls from EO lines to local MG trunk groups, and calls from EO and Tandem trunks to local MG trunk groups. (This last case applies when the MFSS supports local MG trunk groups from its MG to subordinate PBX1s and PBX2s, when the subordinate PBX1s and PBX2s have not been migrated to VoIP.)

5.3.2.12.3.2.2 MFSS MG VoIP Signaling Interfaces

The MFSS MG supports the VoIP signaling interfaces shown in Table 5.3.2.12-2, MFSS MG Support for VoIP Signaling Interfaces.

Table 5.3.2.12-2. MFSS MG Support for VoIP Signaling Interfaces

FUNCTIONAL COMPONENT	VoIP AND VIDEO SIGNALING INTERFACES	VoIP AND VIDEO SIGNALING PROTOCOLS
MG and MGC	MFSS MG – to – MFSS MGC	ITU-T H.248 over IP (used with DoD CCS7, ISDN PRI, and CAS trunks)
MG and MGC	MFSS MG – to – MFSS MGC	ISDN PRI over IP (North American National ISDN Version, used with ISDN PRI trunks only)
MG and MGC	MFSS MG – to – MFSS MGC	Proprietary Supplier Protocols

LEGEND		MFSS	Multifunction Softswitch
CCS7	Common Channel Signaling No. 7	MG	Media Gateway
DoD	Department of Defense	MGC	MG Controller
ISDN	Integrated Services Digital Network	IP	Internet Protocol
ITU-T	International Telecommunications Union – Telecommunication	PRI	Primary Rate Interface
		VoIP	Voice over IP

Unless stated otherwise, all requirements for an “Appliance MG” are for both the LSC and the MFSS.

5.3.2.12.4 MG Interaction with NEs and Functions

The MG is responsible for interacting with elements and functions of the LSC and MFSS to support end-user calls, end-user features, and other operational capabilities needed by the DoD users (i.e., the Army, Navy, Air Force, and Marines). These other elements include the following:

- ASAC
- Service Control functions (Information Assurance and media server)
- Management (FCAPS and audit logs)
- Transport Interface functions
- EBC (not part of the LSC, but part of the Local Assured Services Domain)

5.3.2.12.4.1 MG Support for ASAC

The MG interacts with the CCA, which in turn interacts with the ASAC component of the LSC and MFSS to perform specific functions related to ASAC, such as providing denial treatments for calls that are denied admission to the LSC and/or MFSS, and preemption treatments for calls that are preempted by PBAS/ASAC.

Requirements for ASAC are handled in two categories: CAC and ASAC. In addition, this section covers two different levels of ASAC: LSC-Level ASAC, which is supported in the LSC and the MFSS, and WAN-Level ASAC Policing, which is supported in the MFSS only.

The MG assists the CCA in performing CAC (i.e., call blocking based on budget restrictions) for outgoing TDM calls at MGs and for incoming TDM calls at MGs.

The MG assists the CCA in performing ASAC (i.e., call preemption based on per-call precedence levels) for outgoing TDM calls at MGs and for incoming TDM calls at MGs.

In addition, please see Section 5.3.2.2.2.3, ASAC – Open Loop, and Section 5.3.4.10, Precedence and Preemption, for detailed requirements on how ASAC is supported by CCAs in LSCs and MFSSs.

5.3.2.12.4.1.1 MG Call Denial Treatments to Support CAC

When the CCA determines that a VoIP session request should be blocked because an Appliance CAC restriction applies (e.g., the VoIP session count equals the VoIP session limit for the type of session being requested), the CCA will deny the session request and apply a Call Denial treatment (i.e., a busy signal or call denial announcement) to the calling party on that request. If the calling party is a TDM calling party whose call enters the appliance at an MG trunk group, the MG is responsible for applying the Call Denial treatment also.

[Required] On incoming call requests to a TDM trunk group, where the CCA/MGC applies a CAC Call Denial treatment to that call request, the MG shall connect the TDM called party on the incoming call request to the appropriate CAC Call Denial tone or announcement when instructed to do so by the MGC.

5.3.2.12.4.1.2 MG Call Preemption Treatments to Support ASAC

When the CCA determines that an existing VoIP session or VoIP session request should be cleared because an Appliance ASAC preemption applies (e.g., a CAC limit applies and a call of a higher precedence level needs to complete within the appliance), the CCA will clear the existing session or session request and apply a Call Preemption treatment (i.e., a Call Preemption tone or announcement) to both the calling and called parties on that request. If the calling party is a TDM calling party whose call entered the appliance at an MG trunk group, or the called party is a TDM called party whose call left the appliance at an MG trunk group, the MG is responsible for applying the Call Preemption treatment also.

[Required] On incoming calls or call requests to a TDM trunk group, where the CCA/MGC applies an ASAC Call Preemption treatment to that call or call request, the MG shall connect the TDM calling party on the incoming call or call request to the appropriate ASAC Call Preemption tone or announcement when instructed to do so by the MGC.

[Required] On outgoing calls or call requests from a TDM trunk group, where the CCA/MGC applies an ASAC Call Preemption treatment to that call or call request, the MG shall connect the TDM called party on the outgoing call or call request to the appropriate ASAC Call Preemption tone or announcement when instructed to do so by the MGC.

5.3.2.12.4.2 MG and Information Assurance Functions

The MG interaction with Information Assurance function is consistent with the DoD Information Assurance requirements in Section 5.4, Information Assurance Requirements.

The Information Assurance function within the appliance ensures that end users, PEIs, AEIs, MGs, SGs, and EBCs that use 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 5.3.2.10.7, CCA Support for Information Assurance. These requirements, therefore, apply to the MG.

[Required] Each MG within an appliance shall support all the appliance requirements in Section 5.4, Information Assurance Requirements, that involve an Appliance MG.

The MG performs the following authentication and encryption functions in conjunction with the CCA and Information Assurance:

1. 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.

2. 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.

3. 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.

4. The MG also performs the following encryption functions in conjunction with PEIs or AEIs, and the media server in the LSC (NOTE: These functions may or may not use Information Assurance, depending on the internal design of the LSC.):

    a. 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.

    b. 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.

5.3.2.12.4.3 MG Interaction with Service Control Functions

The media server is responsible for playing tones and announcements to calling and called parties on VoIP calls, and for playing audio/video clips (similar to tones and announcements) to calling and called parties on video calls. In addition, the media server may provide “play announcement and collect digits” functionality to calling and called parties on VoIP and video calls when this functionality is required by certain features that the CCA supports. Depending on the complexity of those features, the media server may act as a full Interactive Voice Response (IVR) system for Appliance 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 LSC end users (e.g., VoIP or video EIs).

[Required] When instructed to do so by the MGC, the MG shall direct TDM calls and call requests to the media server, so that the media server can

1. Play tones and announcements to TDM parties on TDM calls and call requests (e.g., busy tone or announcement; call preemption tone or announcement).

2. Provide “play announcement and collect digits” functionality when required by an Appliance VoIP feature.

3. Provide full IVR-like functionality when required by an Appliance VoIP feature.

The interface and protocols used to interconnect the MG with the media server are internal to the appliance and are, therefore, supplier-specific.

5.3.2.12.4.4 Interactions with IP Transport Interface Functions

The Transport Interface functions in the LSC provide interface and connectivity functions with the ASLAN and its IP packet transport network. This section outlines high-level requirements for these functions. The detailed implementation methods for these requirements are left up to the vendor. Examples of Transport Interface functions include:

- Network Layer functions: IP, IPSec
- Transport Layer functions: IP Transport Protocols (e.g., TCP, UDP), TLS
- LAN protocols

The MG interacts with Transport Interface functions by using them to communicate with PEIs or AEIs and the EBC (and through the EBC to remote PEIs or AEIs and MGs served by other LSCs and MFSSs) over the ASLAN. The following LSC elements and Local Assured Services Domain elements are all IP endpoints on the ASLAN:

- Each PEI or AEI served by the LSC

- The MG itself

- Any other MGs that are served by the LSC (even though the other MGs may be connected physically to the CCA/MGC over an internal proprietary interface, instead of being logically connected to the CCA/MGC over the ASLAN)

- The CCA and its IWF and MGC
- The EBC

As an example, the MG interacts with the LSC Transport Interface functions when it uses IPsec, UDP/TCP/SCTP, and the native ASLAN protocols to exchange H.248 and PRI signaling messages with the CCA/MGC over the ASLAN.

The MG interacts with the LSC Transport Interface functions when it uses IP, UDP, and the native ASLAN protocols to route SRTP media streams to and from EIs, GEIs, other LSC MGs, and the EBC over the ASLAN.

[Required] Since each Appliance MG is an IP endpoint on the Appliance LAN, each MG shall support assignment of the following items to itself:

- Only one MG IP address (This one IP address may be implemented in the CCA as either a single logical IP address or a single physical IP address.)
- An MG FQDN that maps to that IP address
- An MG SIP URI that uses that MG FQDN as its domain name, and maps to a "SIP User Agent" function within the MG.

[Required] The MG shall interact with the Transport Interface functions in the appliances in the following cases:

- When the MG uses the native LAN protocols, IP, and UDP to exchange SRTP media streams with PEIs, AEIs, other MGs, and the EBC over the Appliance LAN
- **[Objective]** When the MG uses the native LAN protocols, IPSec, and UDP, TCP, or SCTP to exchange H.248 signaling messages with the MGC over the Appliance LAN
- **[Objective]** 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

5.3.2.12.4.5 MG – EBC Interaction

The EBC provides SBC and firewall capabilities for the ASLAN, the PEIs, AEIs, and the IP-based components of the LSC, including the CCA, and its IWF and MGC, and the MGs.

The MG interacts with the EBC by sending SRTP media streams to it (for call media destined for a PEI, AEI, or MG that is served by another appliance outside the LSC), 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 LSC).

The SRTP media streams exchanged between the LSC MG and a remote PEI, AEI, or MG must pass through the EBC. The EBC modifies these SRTP media streams by doing NAT / NAPT on them..

The VoIP MG in the MFSS or LSC needs to interact with VoIP Media Transfer functions in the EBC. The EBC

1. 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.

2. Supports SBC functions, such as NAT and NAPT.

3. Supports IP firewall functions.

High-level MG requirements are needed for interacting with an EBC. These requirements are as follows:

[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 EBC so the EBC can process them before sending them on to the remote PEIs or AEIs and MGs via the DISN WAN. The MG shall use the network-level IP addresses of the destination PEIs or AEIs and MGs, rather than the local IP address of the EBC, when directing the VoIP media streams through the EBC to the DISN WAN and the remote PEIs or AEIs and MGs.

[Required] The MG shall direct VoIP media streams to remote PEIs or AEIs and MGs through the EBC in the following cases:

- When the MG is part of an LSC and is directing VoIP media streams to PEIs or AEIs and MGs on another LSC on the DISN WAN

- When the MG is part of an LSC and is directing VoIP media streams to PEIs or AEIs and MGs on an MFSS on the DISN WAN

- When the MG is part of an MFSS and is directing VoIP media streams to PEIs or AEIs and MGs on an LSC on the DISN WAN

When the MG is part of an MFSS and is directing VoIP media streams to PEIs or AEIs and MGs on another MFSS on the DISN WAN.

[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 EBC, because the EBC 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 EBC from the DISN WAN and the remote PEIs or AEIs and MGs.

[Required] The MG shall accept VoIP media streams from remote PEIs or AEIs and MGs through the EBC in the following cases:

- When the MG is part of an LSC and is accepting VoIP media streams from PEIs or AEIs and MGs on another LSC on the DISN WAN

- When the MG is part of an LSC and is accepting VoIP media streams from PEIs or AEIs and MGs on an MFSS on the DISN WAN

- When the MG is part of an MFSS, and is accepting VoIP media streams from PEIs or AEIs and MGs on an LSC on the DISN WAN

- When the MG is part of an MFSS, and is accepting VoIP media streams from PEIs or AEIs and MGs on another MFSS on the DISN WAN

5.3.2.12.4.6 MG Support for Appliance Management Functions

The Management function in the EBC, LSC, and MFSS supports functions for EBC/LSC/MFSS FCAPS management and audit logs. Detailed requirements for the MG support of the Appliance Management functions are covered in Section 5.3.2.18.3, Management Requirements of the MG Function.

The MG interacts with the Appliance Management function by

1. Making changes to its configuration and to its trunks' configuration in response to commands from the Management function that request these changes.

2. Returning information to the Management function on its FCAPS in response to commands from the Management function that request this information.

3. Sending information to the Management function on a periodic basis (e.g., on a set schedule), keeping the Management function up-to-date on MG activity. An example of this update would be a periodic transfer of trunk media error logs from the MG to the Management function so that the Management function could either store the records locally or transfer them to a remote NMS for remote storage and processing.

5.3.2.12.4.7 IP-Based PSTN Interface Requirements

[Conditional] Voice and Video over IP interfaces from the UC network to the PSTN have not been defined. Therefore, the LSC and MFSS to PSTN interface will remain TDM as specified in UCR 2008, Section 5.2, Circuit-Switched Capabilities and Features. Interfaces from an LSC or MFSS to the PSTN will be via an MG with TDM interfaces as specified in UCR 2008, Section 5.2, Circuit-Switched Capabilities and Features.

5.3.2.12.4.8 MG Requirements: Interactions with VoIP EIs

The MG in the MFSS or LSC needs to interact with VoIP EIs served by that MFSS or LSC, and with VoIP EIs served by other MFSSs or LSCs. The VoIP signaling interface between the PEI and the MFSS or LSC is left up to the network appliance supplier. The VoIP signaling interface between the AEI and the MFSS or LSC is AS-SIP per Section 5.3.2.22, AS-SIP EI and Video Codec Requirements, 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 MFSS and LSC:

1. **[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. Supplier-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 AEIs

2. **[Conditional]** When the MG supports the exchange of voice media streams with voice H.323 EIs (both on the local network appliance and on remote network appliances), the MG shall support a mechanism for interworking the G.7xx/SRTP/UDP/IP-based VoIP media streams that the MG uses with the H.323-based VoIP media streams that the H.323 EI uses.

5.3.2.12.4.9 MG Support for User Features and Services

[Required] The MG shall support the operation of the following features for VoIP and Video end users, consistent with the operation of this feature on analog and ISDN lines in DoD TDM switches today:

- Call Hold
- Music on Hold
- Call Waiting
- Precedence Call Waiting
- Call Forwarding Variable
- Call Forwarding Busy Line
- Call Forwarding No Answer

- Call Transfer
- Three-Way Calling
- Hotline Service
- Calling Party and Called Party ID (number only)
- Call Pickup

5.3.2.12.5 MG Interfaces to TDM NEs in DoD Networks: PBXs, EOs, and MFSs

[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:

- PBXs
- SMEOs
- EOs
- MFSs

[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:

- **[Conditional: LSC, MFSS]** DoD CCS7 per UCR 2008, Section 5.2, Circuit-Switched Capabilities and Features, where the MG handles the media trunks and the SG handles the signaling links.

  – ANSI T1.619 and T1.619a support is required for CCS7 MLPP signaling, per UCR 2008, Section 5.2, Circuit-Switched Capabilities and Features.

- **[Required: LSC, MFSS]** U.S. National ISDN PRI per UCR 2008, Section 5.2, Circuit-Switched Capabilities and Features, where the MG handles both the media channels and the signaling channel.

  – ANSI T1.619 and T1.619a support is required for PRI MLPP signaling per UCR 2008, Section 5.2, Circuit-Switched Capabilities and Features.

  – Facility Associated Signaling is required for T1.619A PRIs, and NFAS is Conditional for T1.619A PRIs.

  – Both FAS and NFAS are required for commercial PSTN PRIs, for access to the US PSTN.

- **[Conditional: LSC, MFSS]** U.S. CAS trunks per UCR 2008, Section 5.2, Circuit-Switched Capabilities and Features, where the MG handles both media and signaling on the same channel.
  - CAS MLPP signaling is required per UCR 2008, Section 5.2, Circuit-Switched Capabilities and Features, when a U.S. CAS trunk is supported.

[Required] Media Gateway support for these TDM trunk groups shall be identical to the support for these trunk groups in DoD TDM PBXs, EOs, Tandem switches, and MFSs today, as specified in UCR 2008, Section 5.2, Circuit-Switched Capabilities and Features.

5.3.2.12.6 MG Interfaces to TDM 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.

[Conditional] The MG shall support foreign country CCS7 trunk groups where the MG handles the media trunks, and the SG handles the signaling links as follows:

1. For interconnection with an allied or coalition partner network, using foreign CCS7 from the network of the allied or coalition partner.

2. Support for MLPP using CCS7, per ITU-T Recommendation Q.735.3, is conditional on LSC and MFSS trunk groups when these trunk groups are used to connect to an allied or coalition partner from an OCONUS ETSI-compliant country.

[Required] The MG shall support foreign country ISDN PRI trunk groups where the MG handles both the media channels and the signaling channel as follows:

1. For interconnection with an allied or coalition partner network, using foreign ISDN PRI from the network of the allied or coalition partner.

2. Support for MLPP using ISDN PRI, per ITU-T Recommendation Q.955.3, is required on LSC trunk groups when these trunk groups are used to connect to an allied or coalition partner from a U.S. OCONUS ETSI-compliant country.

3. Support for MLPP using ISDN PRI, per ITU-T Recommendation Q.955.3, is required on MFSS trunk groups when these trunk groups are used to connect to an allied or coalition partner from a U.S. OCONUS ETSI-compliant country.

[Conditional] The MG shall support foreign country CAS trunk groups where the MG handles both media and signaling on the same channel as follows:

1. For interconnection with an allied or coalition partner network, using foreign CAS trunk groups from the network of the allied or coalition partner.

2. Support for MLPP using CAS trunk signaling is not required on these trunk groups.

[Conditional] When appliance suppliers support allied and coalition partner network TDM trunk groups on their MG, MG support for these trunk groups shall be identical to the support for these trunk groups in DoD TDM PBXs, EOs, Tandem Switches, and MFSs today, as specified in UCR 2008, Section 5.2, Circuit-Switched Capabilities and Features.

5.3.2.12.7 MG Interfaces to TDM NEs in the PSTN in the United States

[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.

[Required] Each appliance MG shall support TDM trunk groups that can interconnect with the U.S. PSTN, using the following types of trunk groups:

1. **[Required]** U.S. National ISDN PRI, where the MG handles both the media channels and the signaling channel:

   a. This is required for U.S. PSTN NEs nationwide.
   b. Support for MLPP using ISDN PRI is not required on these trunk groups.
   c. Support for both FAS and NFAS is required on these trunk groups.

2. **[Conditional]** U.S. CAS trunks, where the MG handles both media and signaling on the same channel:

   a. This is conditional for U.S. PSTN NEs nationwide.
   b. Support for MLPP using CAS trunk signaling is not required on these trunk groups.

[Required] Media Gateway support for these TDM trunk groups to the U.S. PSTN shall be identical to the support for these trunk groups in DoD TDM PBXs, EOs, Tandem Switches, and MFSs today, as specified in UCR 2008, Section 5.2, Circuit-Switched Capabilities and Features.

5.3.2.12.8 MG Interfaces to TDM NEs in OCONUS PTT Networks

The appliance supplier (i.e., LSC or MFSS supplier) should support TDM trunk groups on its MG product that can interconnect with NEs in foreign country PTT networks (OCONUS) worldwide.

[Required] The MG shall support foreign country ISDN PRI, where the MG handles both the media channels and the signaling channel:

1. For interconnection with a foreign country PSTN using foreign country ISDN PRI, from the country where the DoD user's B/P/C/S is located.

2. Support for ETSI PRI is required on LSC trunk groups when the LSC is used in OCONUS ETSI-compliant countries.

3. Support for ETSI PRI is required on MFSS trunk groups when the MFSS is used in OCONUS ETSI-compliant countries.

4. Support for MLPP using ISDN PRI is not required on the above trunk groups.

[Conditional] The MG shall support foreign country CAS trunks, where the MG handles both media and signaling on the same channel:

1. For interconnection with a foreign country PSTN, using foreign country CAS trunk groups from the country where the DoD user's B/P/C/S is located.

2. Support for MLPP using CAS trunk signaling is not required on foreign country CAS trunk groups.

[Conditional] If an appliance supplier supports foreign country PSTN TDM trunk groups on its MG, MG support for these trunk groups shall be identical to the support for these trunk groups in DoD TDM PBXs, EOs, Tandem Switches, and MFSs today, as specified in UCR 2008, Section 5.2, Circuit-Switched Capabilities and Features.

5.3.2.12.9 MG Support for DoD CCS7 Trunks

[Conditional: LSC, MFSS] The MG shall support TDM trunk groups that are controlled by a separate CCA-to-SG signaling link that carries DoD CCS7 protocol. The MG shall support these TDM trunk groups, and the SG shall support DoD CCS7 signaling, conformant with the detailed DoD CCS7 trunk and protocol requirements in the following DoD and ANSI documents:

- UCR 2008, Section 5.2.2, Multilevel Precedence and Preemption, including

- Section 5.2.2.4.3, Preempt Signaling, Common Channel Signaling Number 7 (CCS7)
- Section 5.2.2.9, MLPP Common Channel Signaling Number 7 (CCS7)
- UCR 2008, Section 5.2.4.6, Signaling – Common Channel Signaling Number 7 (CCS7)
- ANSI T1.619-1992 (R2005)
- ANSI T1.619a-1994 (R1999)

[Conditional: LSC, MFSS] When used in OCONUS ETSI-compliant countries, the MG shall also support DoD CCS7 trunk groups that support ITU-T Recommendation Q.735.3 for MLPP, consistent with UCR 2008, Section 5.2, Circuit-Switched Capabilities and Features.

[Conditional: LSC, MFSS] The MG shall support multiple CCS7 trunk groups based on the needs of the DoD user deploying the appliance. The MG shall allow each CCS7 trunk group at the MG to connect to a different DoD TDM or IP NE (i.e., LSC, MFSS) based on the interconnection needs of the DoD user.

The MG shall have knowledge of which DoD TDM NE (i.e., SMEO, EO, MFS, MFSS EO, MFSS Tandem) or DoD IP NE (i.e., LSC, MFSS) each CCS7 MG trunk group is connected.

5.3.2.12.10 MG Support for ISDN PRI Trunks

[Required] The MG shall support ISDN PRI trunk groups that carry the U.S./National ISDN version of the ISDN PRI protocol. The MG shall support these U.S. PRI trunk groups conformant with the detailed U.S. ISDN PRI requirements in the following DoD and ANSI documents:

1. UCR 2008, Section 5.2.9, Integrated Services Digital Network, including Table 5.2.9-4, PRI Access, Call Control, and Signaling, and Table 5.2.9-5, PRI Features.

    a. The “MFS” column in these tables shall apply to the MFSS.
    b. The “PBX1” column in these tables shall apply to the LSC.

2. UCR 2008, Section 5.2.2, Multilevel Precedence and Preemption, including

    a. Section 5.2.2.4.2, Primary Rate Interface

    b. Section 5.2.2.7, ISDN MLPP PRI

c. ANSI T1.619-1992 (R2005)

d. ANSI T1.619a-1994 (R1999)

e. FAS is required for T1.619 PRIs, and NFAS is conditional for T1.619 PRIs.

f. Both FAS and NFAS are required for commercial PSTN PRIs, for access to the U.S. PSTN.

[Required: MFSS, LSC for ETSI PRI – Conditional: MFSS, LSC for Other Foreign PRI] The appliance supplier (i.e., LSC or MFSS supplier) has the option of supporting one or more foreign versions of the ISDN PRI protocol on its product. As used here, the term "foreign version of ISDN PRI protocol" means the version of the PRI protocol that is used in the PSTN of a foreign country.

If an appliance supplier supports a foreign version of the ISDN PRI protocol on its product, the MG shall support ISDN PRI trunk groups that support the version of the PRI protocol that is used in the PSTN of a foreign country. The MG shall support these foreign PRI trunk groups conformant with the PRI protocol standards that are used in the PSTN of that foreign country. Examples of these standards include ETSI standards and ITU-T standards.

When used in OCONUS ETSI-compliant countries, the MG shall support ISDN PRI trunk groups that support ITU-T Recommendation Q.955.3 for MLPP, consistent with UCR 2008, Section 5.2, Circuit-Switched Capabilities and Features.

[Required] The MG shall support multiple U.S. PRI trunk groups based on the needs of the DoD user deploying the appliance. The MG shall allow each U.S. PRI trunk group at the MG to connect to: TDM EO and tandem components of the local MFSS; a different U.S. PSTN TDM NE (e.g., PBX, TDM switch); a different DoD TDM NE (e.g., PBX, TDM switch); or a different DoD IP NE (e.g., LSC, MFSS), based on the interconnection needs of the DoD user.

The MG shall have knowledge of which U.S. PSTN TDM, DoD TDM, and DoD IP NE each U.S. PRI trunk group is connected.

[Required: MFSS, LSC for ETSI PRI – Conditional: MFSS, LSC for Other Foreign PRI] When the appliance supplier supports foreign ISDN PRIs, the MG shall support multiple foreign PRI trunk groups based on the needs of the DoD user deploying the appliance. The MG shall allow each foreign PRI trunk group at the MG to connect to a different foreign PSTN TDM, a different allied network element, or a coalition partner TDM network element (e.g., PBX, switch) based on the interconnection needs of the DoD user.

The MG shall have knowledge of which foreign PSTN TDM, or allied or coalition partner TDM NE each foreign PRI trunk group is connected.

[Required] The MG shall support reception of ISDN PRI messages from the CCA MGC and transmission of ISDN PRI messages to the CCA MGC.

The mechanisms that the MG uses to exchange ISDN PRI messages with the CCA MGC (i.e., use of vendor-proprietary protocols with security protection, or use of ISDN User Adaptation Layer protocols over Transport Layer Protocols over IPSec) are described in Section 5.3.2.12.12.6, MG Support for VoIP Interworking for ISDN PRI Trunks.

5.3.2.12.11 MG Support for CAS Trunks

[Conditional: LSC, MFSS] The MG shall support CAS trunk groups that carry the U.S. version of the CAS protocol. The MG shall support these U.S. CAS trunk groups conformant with the detailed CAS trunk and CAS trunk signaling requirements in the following DoD documents:

- UCR 2008, Section 5.2.4, Signaling, including
  - Section 5.2.4.3, Trunk Supervisory Signaling
  - Section 5.2.4.4, Control Signaling
  - Section 5.2.4.5, Alerting Signals and Tones
- UCR 2008, Section 5.2.2, Multilevel Precedence and Preemption, including
  - Section 5.2.2.4.1, Channel Associated Signaling
  - Section 5.2.2.9.6, DSN MLPP CCS7 IAM Called Party Number Format, including CAS-to-CCS Trunk Interworking Matrix (Line-to-Trunk and Trunk-to-Line), and Table 5.2.2-14, CAS-to-CAS Trunk Interworking Matrix (Trunk-to-Trunk)

[Conditional] The appliance supplier (i.e., LSC or MFSS supplier) has the option of supporting one or more foreign versions of CAS trunks and trunk signaling on its product. As used here, the term “foreign version of CAS trunks and trunk signaling” means the version of CAS trunks and trunk signaling that is used in the PSTN of a foreign country.

If an appliance supplier supports a foreign version of CAS trunks and trunk signaling on its product, the CCA IWF shall support the version of CAS trunks and CAS trunk signaling that is used in the PSTN of a foreign country, conformant with the CAS trunk standards that are used in the PSTN of that foreign country. Examples of these standards include ETSI CAS trunk standards and ITU-T CAS trunk standards.

The MG shall support multiple U.S. CAS trunk groups based on the needs of the DoD user deploying the appliance. The MG shall allow each U.S. CAS trunk group at the MG to connect to: a TDM EO and Tandem components of the local MFSS; 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., LSC, MFSS), based on the interconnection needs of the DoD user.

The MG shall have knowledge of which U.S. PSTN TDM, DoD TDM, or DoD IP NE (i.e., LSC, MFSS) each U.S. CAS trunk group is connected.

[Conditional] When the appliance supplier supports foreign CAS trunk groups, the MG shall support multiple foreign CAS trunk groups based on the needs of the DoD user deploying the appliance. The MG shall allow each foreign CAS trunk group at the MG to connect to a different foreign PSTN, or allied or coalition partner TDM network element (e.g., PBX, TDM switch), based on the interconnection needs of the DoD user.

The MG shall have knowledge of which foreign PSTN TDM, or allied or coalition partner TDM network element each foreign CAS trunk group is connected.

[Conditional] The MG shall support reception of U.S. CAS trunk signaling sequences (i.e., Supervisory, Control, and Alerting) from the CCA MGC, and transmission of U.S. CAS trunk signaling sequences to the CCA MGC.

[Conditional: LSC, MFSS] The MG shall support the requirements for MLPP Trunk Selection (Hunting) in the following sections of the UCR 2008. The MG shall support these MLPP Trunk Selection requirements on MG CAS trunk groups to DSN EOs and DSN MFSs. The MG shall also support these requirements on MG CAS trunk groups to DSN SMEOs, PBX1s, and PBX2s (when supported).

- UCR 2008, Section 5.2.2.2.3, MLPP Trunk Selection (Hunting)
- UCR 2008, Section 5.2.2.2.3.1, Hunt Sequence for Trunks
- UCR 2008, Section 5.2.2.2.3.1.1, ROUTINE Precedence Calls
- UCR 2008, Section 5.2.2.2.3.1.2, Precedence Calls Above ROUTINE Precedence
- UCR 2008, Section 5.2.2.2.3.1.2.1, Method 1

- UCR 2008, Section 5.2.2.2.3.1.2.2, Method 2

To meet the above requirements, the MG shall support the definitions of Precedence Level/Calling Area (PL/CA), classmarks, voice-grade trunk groups, data-grade trunk groups, route digit, direct route, alternative route, preemptive search, and friendly search from UCR 2008, Section 5.2, Circuit-Switched Capabilities and Features.

5.3.2.12.12 MG Requirements: VoIP Interfaces Internal to an Appliance

The requirements in the following section assume that a supplier-specific Gateway Control Protocol is used 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 can be either industry standard (as described below) or supplier specific, which is outside the scope of this document.

When the H.248 Gateway Control Protocol is used over the open interface between the MG and the MGC, this open interface supports industry-standard protocol layers (i.e., physical, data link, network, and transport) below the application layer that carries the Gateway Control Protocol. The support for these protocol layers is identified as an Objective.

5.3.2.12.12.1 MG Support for VoIP Interconnection at the Physical and Data Link Layers

[Required] The MG shall connect to the ASLAN of the appliance using the physical layer and data link layer protocols of the ASLAN. In this case, the MG shall appear to the MGC, EBC, and appliance PEIs/AEIs as a physical layer and data link layer endpoint on a LAN switch in the ASLAN.

5.3.2.12.12.2 MG Support for VoIP Interconnection at the Network Layer

[Required] The MG shall connect to the ASLAN of the appliance using the IP as a Network Layer Protocol. In this case, the MG shall appear to the MGC, EBC, and appliance PEIs/AEIs as an IP endpoint on an IP router on the ASLAN.

[Required] The MG shall support IPv4 as a Network Layer Protocol, conformant with RFC 791.

[Required] The MG shall also support IPv6 as a Network Layer Protocol, conformant with RFC 2460.

[Required] Conformant with Section 5.3.5, IPv6 Requirements, the MG shall support dual IPv4 and IPv6 stacks (i.e., support both IPv4 and IPv6 in the same IP end point) as described in RFC 4213.

[Objective] When an open H.248 MGC-MG interface is used, the MG shall support IPSec for use with securing IP packets containing H.248 signaling messages and encapsulated ISDN PRI signaling messages. The MG support for IPSec shall be conformant with the appliance IPSec requirements in Section 5.4, Information Assurance Requirements.

NOTE: The MG is not required to support IPSec for use in IP packets containing SRTP media streams for VoIP, FoIP, and MoIP calls.

5.3.2.12.12.3 MG Support for VoIP Interconnection at the Transport Layer

The following requirements apply when an open MGC-MG interface, which is an objective, is supported:

[Objective] When an open MGC-MG interface is used, the MG shall support transport of H.248 signaling messages and encapsulated ISDN PRI signaling messages using the TCP as a Transport Layer Protocol. In this case, the MG shall support TCP conformant with RFC 793.

[Objective] When an open MGC-MG interface is used, the MG shall support transport of H.248 signaling messages and encapsulated ISDN PRI signaling messages using the UDP as a Transport Layer Protocol. In this case, the MG shall support UDP conformant with RFC 768.

[Objective] When an open MGC-MG interface is used, the MG shall support transport of H.248 signaling messages and encapsulated ISDN PRI signaling messages using the SCTP as a Transport Layer Protocol. In this case, the MG shall support SCTP conformant with RFC 4960.

[Objective] When an open MGC-MG interface is used, the MG shall support a per-MG parameter that controls which of the three Transport Layer Protocols (i.e., UDP, TCP, or SCTP) is used to exchange H.248 signaling messages and encapsulated PRI signaling messages with the MGC. This parameter shall support the following values:

1. When this parameter is set to “TCP,” the MG shall exchange application layer messages with the MGC using TCP.

2. When this parameter is set to “UDP,” the MG shall exchange application layer messages with the MGC using UDP.

3. When this parameter is set to “SCTP,” the MG shall exchange application layer messages with the MGC using SCTP.

NOTE: The MG is not required to support 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.

5.3.2.12.12.4 MG Support for VoIP Interconnection for Media Stream Exchange above the Transport Layer

[Required] The MG shall support exchange of VoIP media streams with appliance PEIs/AEIs, other appliance MGs, and the appliance EBC (and through the appliance EBC, with other PEIs/AEIs and MGs on other network appliances) using the following IETF-defined Media Transfer Protocols:

- SRTP, conformant with RFC 3711
- SRTCP, conformant with RFC 3711

[Required] The MG shall secure all VoIP media streams exchanged with appliance PEIs/AEIs, other appliance MGs, and the appliance EBC (and through the EBC, with PEIs/AEIs and MGs on other network appliances) using SRTP and SRTCP.

[Required] The MG shall use UDP as the underlying Transport Layer Protocol, and IP as the underlying Network Layer Protocol, when SRTP is used for media stream exchange.

5.3.2.12.12.5 MG Support for VoIP Interconnection for Signaling Stream Exchange above the Transport Layer

[Objective] When an open MGC-MG interface is used, the MG shall support exchange of VoIP signaling streams with the appliance MGC. When the VoIP signaling streams contain ISDN PRI signaling messages at the Application Layer, the MG shall use the ISDN User Adaptation (IUA) Protocol between the Transport Layer and the Application Layer (the ISDN PRI signaling). The MG shall support the IUA Protocol consistent with RFC 4233.

NOTE: 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.

[Required] When the VoIP signaling streams contain supplier-proprietary protocol messages instead of H.248 or ISDN PRI messages, the MG shall secure the proprietary protocol message exchange with the MGC using mechanisms that are as strong as, or stronger than, the use of IPSec to secure H.248 and PRI message exchange.

5.3.2.12.12.6 MG Support for VoIP Interworking for ISDN PRI Trunks

[Required] When an MG interworks a TDM call from an ISDN PRI trunk group with a VoIP session within the network appliance, the MG shall perform the following:

1. **[Required]** Convert between the ISDN media stream on the ISDN PRI B-Channel and the VoIP SRTP/Transport Layer/IP media stream within the appliance.

2. **[Objective]** Convert between ISDN signaling messages (ITU-T Recommendation Q.931 messages in Q.921 frames) on the ISDN PRI D-Channel and encapsulated ISDN signaling messages (ITU-T 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.

5.3.2.12.12.6.1 MG Support for VoIP Interworking for National ISDN PRI

[Objective] For U.S. ISDN PRI trunks carrying National ISDN PRI signaling, the MG shall interwork the National ISDN PRI Data Link Layer Protocol (the National ISDN version of ITU-T Recommendation Q.921) with the IETF IUA Protocol and the underlying Transport Layer and IPSec protocols.

5.3.2.12.12.6.2 MG Support for VoIP Interworking for CAS Trunks

The MG needs to read and understand incoming CAS signaling sequences before translating them into MGC messages and sending them to the MGC using IP. Similarly, the MG has to understand and generate outgoing CAS signaling sequences after receiving signaling messages from the MGC using IP and translating the signaling messages into the appropriate CAS signaling sequences. The method of converting CAS signaling into VoIP signaling and the method of conveying this information to and from the CCA are dependent on the MG control protocol used. The H.248 protocol provides a standard way of doing this.

5.3.2.12.12.6.3 MG Support for VoIP Interworking for U.S. CAS Trunks

[Conditional] When an MG interworks a TDM call from a CAS trunk with a VoIP session within the appliance, the MG shall perform the following:

1. Convert between the TDM media stream on the CAS trunk and the VoIP SRTP/Transport Layer/IP media stream within the appliance.

2. Convert between the CAS signaling sequences on the CAS trunk and the VoIP signaling sequences within the appliance.

5.3.2.12.12.6.4 MG Support for VoIP Interworking for Foreign CAS Trunks

[Objective] When the MG supplier supports foreign CAS trunks, an MG shall interwork a TDM call from a CAS trunk with a VoIP Session within the appliance and shall perform the following:

1. Convert between the TDM media stream on the foreign CAS Trunk and the VoIP SRTP/Transport Layer/IP media stream within the appliance.

2. Convert between the CAS signaling sequences on the foreign CAS trunk and the VoIP signaling sequences within the appliance.

5.3.2.12.12.6.5 MG Support for VoIP Codecs for Voice Calls

The MG must support a set of internationally standard and DISN-standard VoIP codecs for use in converting TDM media streams to VoIP media streams, and in converting VoIP media streams to TDM media streams.

[Required] The MG shall support TDM voice streams using the following:

- ITU-T 64 kbps G.711 μ-law PCM over digital trunks

- ITU-T 64 kbps G.711 A-law PCM over digital trunks

- North American 56 kbps G.711 μ-law PCM over digital trunks

- North American analog voice transmission over analog trunks on TDM trunk groups on the TDM side of the MG

[Required] The MG shall convert between North American 56 kbps G.711 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.

[Required] The MG shall convert between North American analog voice transmission and ITU-T 64 kbps G.711 µ-law PCM in cases where North American analog voice trunks are used on the TDM side of the MG.

[Conditional] When the MG supplier supports analog foreign CAS trunks, the MG shall support TDM voice streams using international (foreign) analog voice transmission over analog trunks on TDM trunk groups on the TDM side of the MG.

[Conditional] When the MG supplier supports analog foreign CAS trunks, the MG shall convert between international (foreign) analog voice transmission and ITU-T 64 kbps G.711 A-law PCM in cases where international (foreign) analog voice trunks are used on the TDM side of the MG.

5.3.2.12.12.6.5.1 Support for Uncompressed, Packetized VoIP per ITU-T Recommendation G.711

[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.

[Required] The MG shall packetize/depacketize G.711 media streams received or sent between its TDM side and its VoIP side.

[Required] The MG shall transport each packetized G.711 VoIP stream to and from the destination local PEI, local AEI, local MG, remote PEI (via an EBC), remote AEI (via an EBC), or remote MG (via an EBC) using SRTP, UDP, and IP protocol layers on the VoIP side of the MG.

[Required] The MG shall support the use of uncompressed, packetized G.711 µ-law and A-law VoIP media streams for both Fixed and Deployable applications.

5.3.2.12.12.6.5.2 Support for Compressed, Packetized VoIP per ITU-T Recommendation G.72x

[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:

- ITU-T Recommendation G.723.1
- ITU-T Recommendation G.729, plus Erratum 1, and Annexes A through J, and Appendices I, II, and III

The MG 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.

[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 EBC), remote AEI (via an EBC), or remote MG (via an EBC) using SRTP, UDP, and IP protocol layers on the VoIP side of the MG.

[Required] The MG shall support the use of packetized G.72x VoIP media streams for both Deployable and Fixed applications.

5.3.2.12.12.6.6 MG Support for Group 3 Fax Calls

[Required] The MG shall support Group 3 Facsimile (G3 Fax) calls between TDM trunk-side interfaces on the MG, PEIs, AEIs, TAs, IADs, TDM line-side interfaces on the MG, and EBCs.

The MG shall support G3 Fax calls on TDM trunks for the following TDM trunk types:

- **[Conditional: LSC, MFSS]** DoD CCS7
- U.S. ISDN PRI
- U.S. CAS trunk (Conditional: when the MG supplier supports U.S. CAS trunks)
- Foreign ISDN PRI (Required: When the MG supplier supports ETSI PRI – Conditional: when the MG supplier supports other foreign ISDN PRIs)

[Required] The MG support for G3 Fax calls on the TDM trunk types listed 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 today, as specified in the UCR 2008, Section 5.2.2, Multilevel Precedence and Preemption.

[Required] The MG support for G3 Fax calls on the TDM trunk types listed in this section shall allow G3 Fax calls to:

1. 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.

2. 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.

3. 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.

[Required] The MG shall support a mechanism to detect FoIP calls, to distinguish them from VoIP calls, and to treat them differently from VoIP calls. The MG shall support this FoIP detection mechanism on both TDM-to-FoIP calls (i.e., inbound from a TDM network to the IP appliance) and FoIP-to-TDM calls (i.e., outbound from the IP appliance to a TDM network).

[Required] The MG shall <u>not</u> rely on called number screening or calling number screening for detecting inbound TDM-to-FoIP calls or outbound FoIP-to-TDM calls.

In other words, the IP appliance administrator should not be required to maintain a list of calling and called fax numbers that are local to the IP appliance (representing FoIP end points within the appliance), and a list of calling and called fax numbers that are outside the IP appliance (representing G3 Fax and FoIP end points outside of the appliance) to determine whether the call is an FoIP call.

[Required] The MG, in conjunction with the MGC, shall support two separate options for "Handling of FoIP calls within the IP appliance:"

- Handle FoIP calls as G.711 VoIP calls (Fax Passthrough Calls)
- Handle FoIP calls as ITU-T Recommendation T.38 FoIP calls (Fax Relay Calls)

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.

[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.

5.3.2.12.12.6.6.1 MG Option to "Handle FoIP Calls as G.711 VoIP Calls" (Fax Passthrough Calls)

[Required] When the MG is configured to "Handle FoIP calls as G.711 VoIP Calls," the MG shall support the use of uncompressed, packetized G.711 μ-law and A-law FoIP media streams for both Fixed and Deployable applications.

[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:

1. 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 5.3.2.12.13, Echo Cancellation).

2. The MG may disable silence suppression on the FoIP side of the call.

[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.

[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/TA/IAD, local MG, remote EI/TA/IAD (via an EBC), or remote MG (via an EBC) 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 in RTS 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.

5.3.2.12.12.6.6.2 MG Option to "Handle FoIP Calls as T.38 FoIP Calls" (Fax Relay Calls)

[Required] When the MG is configured to "Handle FoIP Calls as T.38 FoIP Calls," the MG shall not handle FoIP calls within the appliance in the same way it handles G.711 VoIP calls within the appliance. Instead, upon detection that a VoIP call request is actually a FoIP call request, the MG shall direct the FoIP call request to a "T.38 Fax Server" that is internal to the appliance.

NOTE: This "T.38 Fax Server" may be part of the MG, part of the separate UFS Server in the appliance, or part of the separate media server in the appliance.

[Required] The T.38 Fax Server shall support the full set of procedures and protocols for Fax Relay in ITU-T Recommendation T.38.

[Required] The T.38 Fax Server shall support the full set of procedures and protocols for Group 3 Fax reception and transmission in ITU-T Recommendation T.4.

[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 LSC or MFSS, and analog fax devices behind TAs, IADs, and MG line cards on an LSC or MFSS.

5.3.2.12.12.6.7 MG Support for Voiceband Data Modem Calls

The UCR 2008 requirements in this section have been deleted in UCR 2008, Change 1. Please see Section 5.3.2.21, V.150.1 Modem Relay Secure Phone Support Requirements, for the most recent V.150.1 Modem Relay requirements for UC Media Gateways.

5.3.2.12.12.6.8 MG Support for SCIP over IP Calls

The UCR 2008 requirements in this section have been deleted in UCR 2008, Change 1. Please see Section 5.3.2.21, V.150.1 Modem Relay Secure Phone Support Requirements, for the most recent SCIP-216 Modem Relay requirements for UC MGs.

5.3.2.12.12.6.9 MG Support for ISDN over IP Calls and 64-kbps Clear Channel Data Streams

The MG is expected to support ISDN over IP calls and 64 kbps unrestricted digital information (i.e., 64-kbps Clear Channel Data) streams from ISDN interfaces, in addition to the other types of voice streams (i.e., FoIP, MoIP, SCIP over IP) described in the previous sections. For 64-kbps Clear Channel Data, the MG is not expected to perform any media processing for TDM ⇔ IP conversion other than packetization and depacketization. In this case, the MG's main role is to provide a transparent relay of a 64-kbps Clear Channel Data stream across the IP network using RTP packets. RFC 4040 specifies the SDP coding that should be used to support this scenario.

[Required] The MG shall support 64-kbps Clear Channel Data on TDM trunks for the following TDM trunk types:

- U.S. ISDN PRI
- **[Required: When the MG supplier supports ETSI PRIs – Conditional: When the MG supplier supports other foreign ISDN PRIs]** Foreign ISDN PRI

[Required] Media Gateway support for 64-kbps Clear Channel Data calls on the TDM trunk types listed 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 today, as specified in UCR 2008, Section 5.2.2, Multilevel Precedence and Preemption.

[Required] Media Gateway support for 64-kbps Clear Channel Data calls on the trunk types listed 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.

[Required] The MG shall support a mechanism to detect 64-kbps Clear Channel Data calls; to distinguish them from VoIP, FoIP, MoIP, and SCIP over IP calls; and to treat them differently from VoIP, FoIP, MoIP, and SCIP over IP calls. The MG shall support this 64-kbps Clear Channel Data detection mechanism on both TDM-to-IP calls (i.e., inbound from a TDM network to the IP appliance) and IP-to-TDM calls (i.e., outbound from the IP appliance to a TDM network).

[Required] When a 64-kbps Clear Channel Data call enters the IP appliance MG over one TDM trunk, and then leaves the same IP appliance MG over another TDM trunk, the MG shall support the ability to interconnect the two-way TDM media streams from the first trunk directly with the two-way TDM media streams from the second trunk, without performing any TDM-to-IP and IP-to-TDM conversions.

[Required] The MG shall support the procedures and protocols for carrying 64-kbps Clear Channel Data streams over IP, UDP, and RTP as described in RFC 4040. This shall include the coding of SDP Multipurpose Internet Mail Extension (MIME) parameters in the following manner (as excerpted from RFC 4040):

1. MIME media type name: audio.

2. MIME subtype name: clearmode.

3. Optional parameters: ptime, maxptime.

    a. "ptime" gives the length of time in milliseconds represented by the media in a packet, as described in RFC 4566.

    b. "maxptime" represents the maximum amount of media that can be encapsulated in each packet, expressed as time in milliseconds, as described in RFC 4566.

4. Encoding considerations: This type is only defined for transfer via RTP.

5. Parameter mapping considerations:

    a. The MIME type (audio) goes in the SDP "m=" attribute as the media name.

    b. The MIME subtype (clearmode) goes in the SDP "a=rtpmap" attribute as the encoding name.

    c. The optional parameters "ptime" and "maxptime" go in the SDP "a=ptime" and "a=maxptime" attributes, respectively.

5.3.2.12.12.6.10 MG Support for "Hair-Pinned" MG Calls

[Required] The MG shall support VoIP sessions between trunks on the same MG, including all combinations of TDM call legs and VoIP media end points.

[Required] In the TDM-to-TDM sessions, the MG shall not establish any IP, UDP/TCP/SCTP, RTP, or VoIP codec communication between the "call-originating" and "call-terminating" side of the MG. In addition, the MG shall not establish any TDM-to-VoIP media conversion, or VoIP-to-TDM media conversion, on either side of the MG, for either direction of media transmission.

5.3.2.12.13 Echo Cancellation

5.3.2.12.13.1 MG Requirements for Echo Cancellation

The following basic requirements for MG Echo Cancellation are based on the commercial VoIP network Echo Cancellation requirements in Telcordia Technologies GR-3054-CORE (for the TG serving CCS7 trunk groups) and GR-3055-CORE (for the AG serving ISDN PRI and CAS trunk groups). These Echo Cancellation requirements have been updated to reference the DSN Echo Cancellation requirements in UCR 2008, Section 5.2.12.1, Echo Cancellation Requirements.

5.3.2.12.13.2 Trunk Gateway Echo Cancellation

In any 2-wire or combination 2- and 4-wire telephone circuit, echo is caused by impedance mismatch. Echo Cancellers are voice-operated devices placed in the 4-wire portion of a circuit, which may be an individual circuit path or a path carrying a multiplexed signal, and are used for reducing the echo by subtracting an estimated echo from the circuit echo.

The ECs are assumed to be "half" ECs, i.e., those in which cancellation takes place only in the send path due to signals present in the receive path. In particular, echo cancellation should be enabled for all voice calls. The ITU-T requirements for echo cancellation are specified in ITU-T Recommendation G.168.

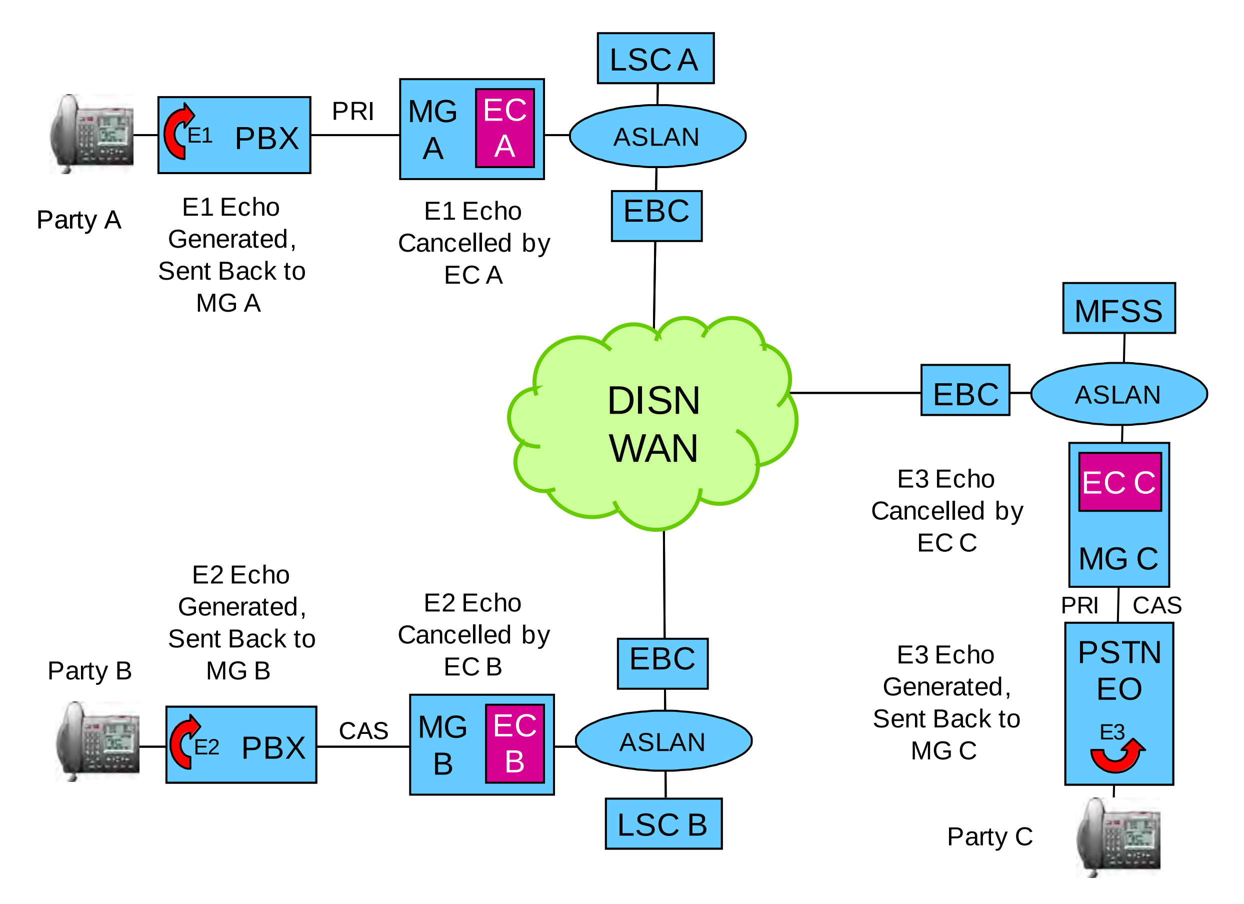
5.3.2.12.13.2.1 Echo Control Design

An example MG echo control design is illustrated in Figure 5.3.2.12-6, Example IP Network Echo Control Design.

The EC function in MG A (controlled by LSC A) is pointing toward the PRI interface to the PBX, canceling voice-frequency (VF) echo returning from the local PBX and the telephone end users behind that PBX. The EC function in MG B (controlled by LSC B) is pointing toward the

CAS interface to the other PBX, canceling VF echo returning from the local PBX and the telephone end users behind that PBX.

On a call between Party A and Party B, the EC function in MG A protects the “far-end party” (Party B) from excessive acoustical echo from the “near-end party” (Party A). Similarly, the EC function in MG B protects the “far-end party” (Party A) from excessive acoustical echo from the “near-end party” (Party B).


LSC A
ASLAN
EBC
PRI
MG A
EC A
E1
PBX
Party A
E1 Echo Generated, Sent Back to MG A
E1 Echo Cancelled by EC A
MFSS
ASLAN
EBC
DISN WAN
E3 Echo Cancelled by EC C
EC C
MG C
PRI
CAS
PSTN EO
E3
E3 Echo Generated, Sent Back to MG C
Party C
E2 Echo Generated, Sent Back to MG B
E2 Echo Cancelled by EC B
Party B
E2
PBX
CAS
MG B
EC B
EBC
ASLAN
LSC B

LEGEND

ASLAN	Assured Services Local Area Network	EO	End Office	PBX	Private Branch Exchange
CAS	Channel Associated Signaling	LSC	Local Session Controller	PRI	Primary Rate Interface
DISN	Defense Information Systems Network	MFSS	Multifunction Softswitch	PSTN	Public Switch Telephone Network
EBC	Edge Boundary Controller	MG	Media Gateway	WAN	Wide Area Network
EC	Echo Canceller				

Figure 5.3.2.12-6. Example IP Network Echo Control Design

In addition, the EC function in MG C (controlled by the MFSS) is pointing toward the PRI or CAS interface to the PSTN EO, canceling VF echo returning from that EO and the telephone end users behind that EO. On a connection between Party A and Party C (a PSTN-served customer), the EC function in MG C is protecting the IP-network-served party (Party A) from excessive acoustical echo. Similarly, the EC function in MG A is controlling the VF echo returned toward the PSTN-served party (Party C).

5.3.2.12.13.2.2 Echo Cancellation Criteria

The echo path capacity of an EC is the maximum echo path delay for which the device is designed to operate.

[Required] The MG shall provide an EC capability with an echo path capacity (echo tail length) of at least 64 ms.

[Objective] It is an objective that the MG shall provide an 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.

[Required] The MG shall provide echo cancellation for voice, G3 Fax, and VBD modem fax calls. (In the G3 Fax and VBD modem call cases, the MG shall provide echo cancellation if an “echo canceller disabling signal” is not sent by any end user’s equipment on the G3 Fax or modem call.) This echo cancellation shall conform to the echo cancellation requirements specified in ITU-T Recommendation G.168.

[Required] Each MG 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.

[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.

Media Gateways serving DoD CCS7 trunk groups need to perform CCS7 Continuity Checks on individual trunks within those trunk groups. As part of these continuity checks, the MGs send and receive in-band tones on the individual CCS7 trunks. The presence of active ECs on these trunk circuits interferes with the exchange of these in-band tones, and therefore, interferes with the CCS7 Continuity Checks.

As a result, it is necessary for the MG to disable the ECs on trunk circuits during CCS7 Continuity Checks, and to re-enable the ECs on these circuits after the CCS7 Continuity Checks have been completed.

[Conditional] The MG shall disable its MG EC on an individual trunk circuit while a CCS7 Continuity Check is being run on that circuit (without requiring that the EC disabling signal be detected on either the send path or receive path on that circuit).

[Required] The MG shall support all DSN Echo Cancellation requirements in UCR 2008, Section 5.2.12.1, Echo Cancellation Requirements. In the case of a discrepancy between the DSN Echo Cancellation requirements in Section 5.2.12.1 and the VVoIP Echo Cancellation requirements here, the VVoIP Echo Cancellation requirements here shall take precedence.

5.3.2.12.14 MG Requirements for Clock Timing

[Required] The MG shall derive its clock timing from a designated T1 or PRI interface. See UCR 2008, Section 5.2, Circuit-Switched Capabilities and Features, for detailed requirements on how clock synchronization is supported in DSN TDM switches today.

5.3.2.12.15 MGC-MG CCA Functions

Per Section 5.3.2.9.2.2, CCA MGC Component, the role of the MGC within the CCA is to

1. Control all MGs within the LSC or MFSS.

2. Control all trunks (DoD CCS7, PRI, CAS) within each MG:

   a. **[Required: LSC, MFSS]** Support for DoD ISDN trunks.
   b. **[Conditional: LSC, MFSS]** Support for CAS trunks.

3. Control all signaling and media streams on each trunk within each MG.

4. Accept IP-encapsulated signaling streams from an SG or MG, and return IP-encapsulated signaling streams to the SG or MG accordingly.

   a. This approach is used for CCS7 signaling to/from an SG **[Conditional: in both the MFSS and LSC cases]**, and for PRI signaling to/from an MG.

5. Within the LSC, use either ITU-T Recommendation H.248 or a supplier-proprietary protocol to accomplish these controls.

The MGC and the MG that it controls are Conditional – Deployable for the LSC (Conditional for Deployable LSC locations), but are Required for the MFSS. The MGC and the MG that it controls are Required for Fixed LSC locations.

[Required] The MGC within the CCA shall be responsible for controlling all the MGs within the LSC or MFSS.

[Required] The MGC within the CCA shall be responsible for controlling all the trunks (i.e., DoD CCS7, PRI, or CAS) within each MG within the LSC or MFSS.

[Required] The MGC within the CCA shall be responsible for controlling all media streams on each trunk within each MG.

[Required] The MGC within the CCA shall accept IP signaling streams from an MG, conveying received PRI or CAS trunk signaling. The MGC shall return IP signaling streams to the MG accordingly, for conversion to transmitted PRI or CAS trunk signaling.

[Conditional] When the appliance supplier supports foreign PRI or CAS trunks on its product, the CCA shall know which national variant of PRI or CAS signaling (e.g., ETSI/TTC/TTA; Germany/Japan/South Korea) the Foreign PRI or CAS Trunk supports.

[Required] Within the appliance (i.e., LSC or MFSS), the MGC shall use either ITU-T Recommendation H.248 (Gateway Control Protocol Version 3) or a supplier-proprietary protocol to accomplish the MG, trunk, and media stream controls described previously.

5.3.2.12.15.1 MG Support for MGC-MG Signaling Interface

An open MGC-MG interface that involves ITU-T Recommendation H.248 is optional (i.e., a closed MGC-MG interface can be used instead).

[Objective] The MGC shall use ITU-T Recommendation H.248 for MG control.

[Required] The MGC protocol for MG control (MG Control Protocol) shall support the following:

1. Control message exchanges that are functionally equivalent to the control message exchanges used in ITU-T Recommendation H.248.

2. Transport Layer functionality, including message sequencing, detection of message loss, and recovery from message loss, which are functionally equivalent to the sequencing, loss detection, and loss recovery mechanisms in TCP and SCTP.

3. Strong security for the exchange of gateway control messages and their underlying Transport Layer packets and Network Layer packets, so security controls (i.e., MG and MGC authentication, encryption and decryption of exchanged messages down to the Network Layer) are at least as strong as the IPSec security protection used when ITU-T

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 5.4, Information Assurance Requirements.

[Required] The CCA and MGC shall be able to select the VoIP codec used by the MG to match the type of end point (i.e., PEI, AEI, EBC) and service requested (i.e., uncompressed VoIP; compressed VoIP, FoIP, MoIP, SCIP over IP; or video over IP).

[Required] The CCA and MGC shall ensure that both endpoints of each VVoIP session use the same VVoIP codec for both directions of media stream transmission between the MG and the peer EBC, 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.)

[Required] If the VoIP codec requested by a calling or called PEI, AEI, or EBC 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 EBC, 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.

"EBC 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 EBC.

"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.

[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:

- ITU-T Recommendation G.711, both North American μ-law and international A-law variants

- ITU-T Recommendation G.723.1

- ITU-T Recommendation G.729

5.3.2.12.15.2 MG Support for Encapsulated National ISDN PRI Signaling

[Required] The MG shall transport ISDN PRI signaling messages between the MG and the MGC. In this case, the MG shall support the following:

- Transparent passing of ISDN PRI messages between the MG and MGC
- Preservation of correct message sequences, in both directions of transmission
- Detection of message loss and recovery from message loss (e.g., by retransmission of lost messages), in both directions of transmission
- Detection of message errors and correction of message errors (e.g., by retransmission of errored messages), in both directions of transmission
- Securing of ISDN PRI messages using MG and MGC encryption, in both directions of transmission

The MG shall support all these capabilities over the supplier-specific protocol so the resulting exchange of ISDN PRI messages (and security of exchanged ISDN PRI messages) is identical to what would occur if IUA, UDP/TCP/SCTP, and IPSec were used.

When an open protocol is used to support the transport of ISDN PRI signaling messages between the MG and MGC, the following objective applies:

1. **[Objective]** The MG shall use the following protocol stack to support encapsulation of ISDN PRI signaling messages sent from the MG to the MGC, and de-encapsulation of ISDN PRI signaling messages sent from the MGC to the MG when an open interface is used:

   a. National ISDN PRI signaling messages, as described in Telcordia Technologies SR-4994.

   b. IUA frames, where IUA shall be supported as defined in RFC 4233.

   c. One of the following IETF-standard Transport Layer Protocols:

      (1) TCP
      (2) UDP
      (3) SCTP

d. IPSec packets, secured using mutual MGC and MG encryption, at the IP Network Layer. This encryption shall be performed consistent with the MGC and MG encryption of encapsulated ISDN PRI messages described in Section 5.4, Information Assurance Requirements.

5.3.2.12.15.3 MG Support for Mapped CAS Trunk Signaling using H.248 Packages for MF and DTMF Trunks

[Conditional] The MG shall transport the CAS trunk signaling between the MG and the MGC. In this case, the MG shall still support the following:

- Transparent passing of CAS trunk signaling (or indications of CAS trunk signaling) using supplier-specific messages between the MG and MGC
- Preservation of correct message sequences, in both directions of transmission
- Detection of message loss and recovery from message loss (e.g., by retransmission of lost messages), in both directions of transmission
- Detection of message errors and correction of message errors (e.g., by retransmission of errored messages), in both directions of transmission
- Securing of supplier-specific messages using MGC and MG encryption, in both directions of transmission

The MG shall support all these capabilities over the supplier-specific protocol so the resulting exchange of CAS trunk signaling (and security of the messages carrying the CAS trunk signaling) is identical to what would occur if H.248, UDP/TCP/SCTP, and IPSec were used.

When an open protocol is used to support the transport of CAS signaling messages between the MG and MGC, the following requirements apply:

1. **[Conditional]** The MGC shall use the following protocol stack to support encapsulation of CAS trunk signaling sent from the MG to the MGC, and de-encapsulation of CAS trunk signaling sent from the MGC to the MG:

   a. ITU-T Recommendation H.248 signaling messages carrying indications of MGC-to-MG and MG-to-MGC signaling for DTMF trunks and MF trunks. This H.248 signaling message shall include DTMF, MF, and CAS information from the following H.248 packages:

      (1) Basic DTMF Generator Package (from ITU-T 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 UCR 2008, Section 5.4, Information Assurance Requirements.

[Conditional] The MGC shall support the following set of CAS trunk signals, consistent with their use in Telcordia Technologies GR-3055-CORE (for the MG) and GR-3051-CORE (for the MGC):

1. Seizure Signal. A signal, sent from the originating switching system (or MGC/MG) to the terminating switching system (or MGC/MG), that defines the transition from the trunk idle state to the trunk seizure state.

2. Addressing Control Signal. A signal that marks the transition from the seizure state to the addressing state. Two addressing control methods of operation exist:

   a. Wink Start. After receiving a seizure signal, the terminating switching system (or MGC/MG) sends an off-hook signal with a defined duration (wink) to indicate that it is prepared to receive address information.

   b. Immediate-Dial. No addressing control signal is used. The originating switching system (or MGC/MG) waits for a specified time after sending a seizure signal before sending the first address digit.

3. Answer Signal. A signal that defines the transition from the call-processing state to the communications state, and persists for the duration of the communications state.

4. Transfer of address digits using DTMF signaling for DTMF trunk groups.

5. Transfer of address digits using MF signaling for MF trunk groups.

6. Disconnect Signal. A signal that defines the transition from the call-processing state or the communications state to the idle state.

5.3.2.12.15.4 MG Support for Glare Conditions on Trunks

As defined in UCR 2008, Section 5.2, Circuit-Switched Features and Capabilities, "Glare occurs when both interfaces of switching systems connected to the same inter-switching-system facility (trunk) apply a seizure signal at approximately the same time." In this section, at least one of the "switching systems connected to the same inter-switching-system facility (trunk)" is an LSC or MFSS MG, as represented by a CAS trunk group. Note that MG support for CAS trunks is conditional.

[Conditional: LSC, MFSS] The MG shall provide functions required to handle a glare situation on CAS trunks as specified in Telcordia Technologies GR-506-CORE, Section 11.5, Glare Resolution.

5.3.2.12.15.5 MGC and IWF Treatments for PRI-to-AS-SIP Mapping for TDM MLPP

[Required] In conjunction with the IWF, the MGC shall support the following mapping of PRI-signaled MLPP information to AS-SIP-signaled RPH information on calls or sessions that involve TDM MLPP and PRI/AS-SIP interworking:

1. The four NI digits received in octets 5 and 6 of the ISDN PRI precedence level IE shall be mapped to the network-domain subfield of the Namespace field in the AS-SIP RPH.

2. The "MLPP Service domain" information received in octets 7, 8, and 9 of the ISDN PRI precedence level IE shall be mapped to the precedence-domain subfield of the Namespace field in the AS-SIP RPH.

3. The "Precedence level" information received in bits 4 through 1 of octet 4 of the ISDN PRI precedence level IE shall be mapped to the "Resource-Priority (r-priority)" field in the AS-SIP RPH.

In the absence of a received ISDN PRI precedence level IE:

1. **[Required]** The MGC/IWF shall use a default network-domain value of "uc" in the Namespace field in the AS-SIP RPH.

2. **[Required]** The MGC/IWF shall use a default precedence-domain value of “000000” in the Namespace field in the AS-SIP RPH.

3. **[Required]** The MGC/IWF shall use a default Resource Priority value of “0 (Routine)” in the “r-priority” field in the AS-SIP RPH.

[Required] The MGC/IWF shall support mapping of the four NI digits to the network-domain subfield of the Namespace field in the RPH as follows:

1. Until the 2012 timeframe, the MGC/IWF shall always use the value “uc” in the network-domain subfield, independent of the NI digits received.

2. 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 5.3.2.12-3, 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 5.3.2.12-3. NI Digit Translation Table

LEVEL IE NI DIGITS	OUTPUT SIP RPH NETWORK DOMAIN
0000	uc
0001	cuc
0002	dod
0003	nato
LEGEND IE Information Element NI Network Identifier	 RPH Resource Priority Header SIP Session Initiation Protocol

3. 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.

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.

[Required] The MGC/IWF shall support mapping of the PRI “MLPP Service domain” field to the precedence-domain subfield of the Namespace field in the RPH as follows:

1. The MGC/IWF shall convert the three-octet hexadecimal values from the three-octet PRI MLPP service domain field into a text string consisting of six text characters. The MGC/IWF shall use this six-character string as the precedence-domain subfield of the Namespace field in the RPH. For example:

- For the 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.

2. If the received network-domain value is not included in the translation table for this PRI, the MGC/IWF shall use a default NI digits value of “0000” for this call.

[Required] The MGC/IWF shall support mapping of the precedence-domain subfield of the Namespace field in the RPH to the PRI MLPP service domain field as follows:

- The MGC/IWF shall replace the six-character text string from the RPH precedence-domain with the hexadecimal-encoded number “000000” in the three-octet PRI MLPP service domain field. The MGC/IWF shall use this three-octet hexadecimal-encoded number, “000000,” in the MLPP service domain field in the ISDN PRI precedence level IE.

[Required] The MGC/IWF shall support mapping of the Resource-Priority field of the RPH to the PRI Precedence Level field (a semi-octet) as follows:

1. If the network-domain field in the RPH is “uc,” then the MGC/IWF shall set the Precedence Level field in the ISDN PRI precedence level IE according to Table 5.3.2.12-4, Mapping of RPH r-priority Field to PRI Precedence Level Value.

2. If the network-domain field in the RPH is any value other than “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).

5.3.2.12.15.6 MGC Support for MG-to-MG Calls

[Required] The MGC shall be able to support multiple MGs.

[Required] The MGC shall support VoIP sessions between 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 EBC to the DISN WAN.

Table 5.3.2.12-4. 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

[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.

5.3.2.12.16 MGs Using the V.150.1 Protocol

[Required: MG] Whenever the MG uses ITU-T Recommendation V.150.1, the following applies:

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.

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 EBC.

5.3.2.12.17 MG Preservation of Call Ringing State during Failure Conditions

[Required: LSC MG, MFSS MG, WAN SS MG] The LSC MG, MFSS MG, and WAN SS MG shall not allow AS-SIP sessions that have reached the ringing state (i.e., an AS-SIP 180 (Ringing) message or 183 (Session Progress) has been sent from the called party to the calling party, and the calling party is receiving an audible ringing tone) to fail when an internal failure occurs within that MG. ("Internal failure" as used here includes cases where one component of the MG fails, and a failover occurs within the MG so a second redundant component is brought into service to replace the first failed component.) Instead, the MG shall ensure that the "call ringing state" is preserved (rather than dropped) at both the calling party interface (where audible ringing tone is being returned to the caller) and the called party interface (where incoming call alerting is being provided to the called party).

5.3.2.13 Signaling Gateway Requirements

5.3.2.13.1 Introduction

This section provides GSRs for the SG. The SG is a conditional functional component in the MFSS and LSC.

The scope of these SG requirements covers CCS7 signaling connectivity for DSN (DoD) CCS7.

5.3.2.13.1.1 SG Requirements Assumptions

The SG functional requirements are based on the following key assumptions:

1. The SG, together with the CCA, is modeled as a Signaling End Point (SEP) in the CCS7 network.

2. The SG is assigned a unique Signaling Point Code (SPC) in the CCS7 network.

3. The SG connects to a pair of mated STPs in the CCS7 network using two Access Link Sets (A-link sets).

4. The SG supports Message Transfer Part 2 (MTP2) links (56 kbps or 64 kbps based on the interconnected CCS7 network).

5. Depending on vendor-specific implementation, the SG can be physically combined with the CCA, or physically separated and located in a different location from the CCA.

6. The requirements in this section assume that the SG and CCA are part of the same solution platform.

7. The SG-CCA interface is assumed to be an internal, unexposed interface. This interface could be based on proprietary protocols or standard protocols defined for such an interface (e.g., IETF SIGTRAN Adaptation protocols over the SCTP/IP).

8. An MFSS may support multiple SGs for reliability and scalability.

5.3.2.13.1.2 SG Primary Function and Interfaces

The primary function of the SG is to provide CCS7 signaling interface functions on the CCS7 network side, provide connectivity to IP transport, and relay CCS7 signaling messages to and from the CCA. These functions can be grouped based on the following two main interfaces of the SG:

- SG-CCS7 interface (circuit-switched side)
- SG-CCA interface (IP side)

The SG-CCS7 network interface provides CCS7 link and network connectivity functions facilitating E2E exchanges of CCS7 call control (i.e., ISUP – **[Required]**) and services control (e.g., TCAP – **[Conditional]**) signaling messages between the CCA and SEPs in interconnected TDM networks. The SG will provide signaling connectivity with DoD CCS7 networks.

The SG-CCA interface provides transport functions to convey CCS7 information between the SG and CCA functional components.

5.3.2.13.2 Role of the SG in Appliances

The SG described in the following requirements is part of the SCS functions of the MFSS and LSC products. The primary function of the SG is to provide the necessary functions for CCS7 signaling connectivity to circuit-switched networks. The SG, together with the CCA and the MG, will provide the products and functions necessary for interconnection between the IP packet network and circuit-switched network. Specifically, the SG will provide the necessary functions to facilitate call and service control signaling for CCS7 control trunks (bearer connections) to the MG.

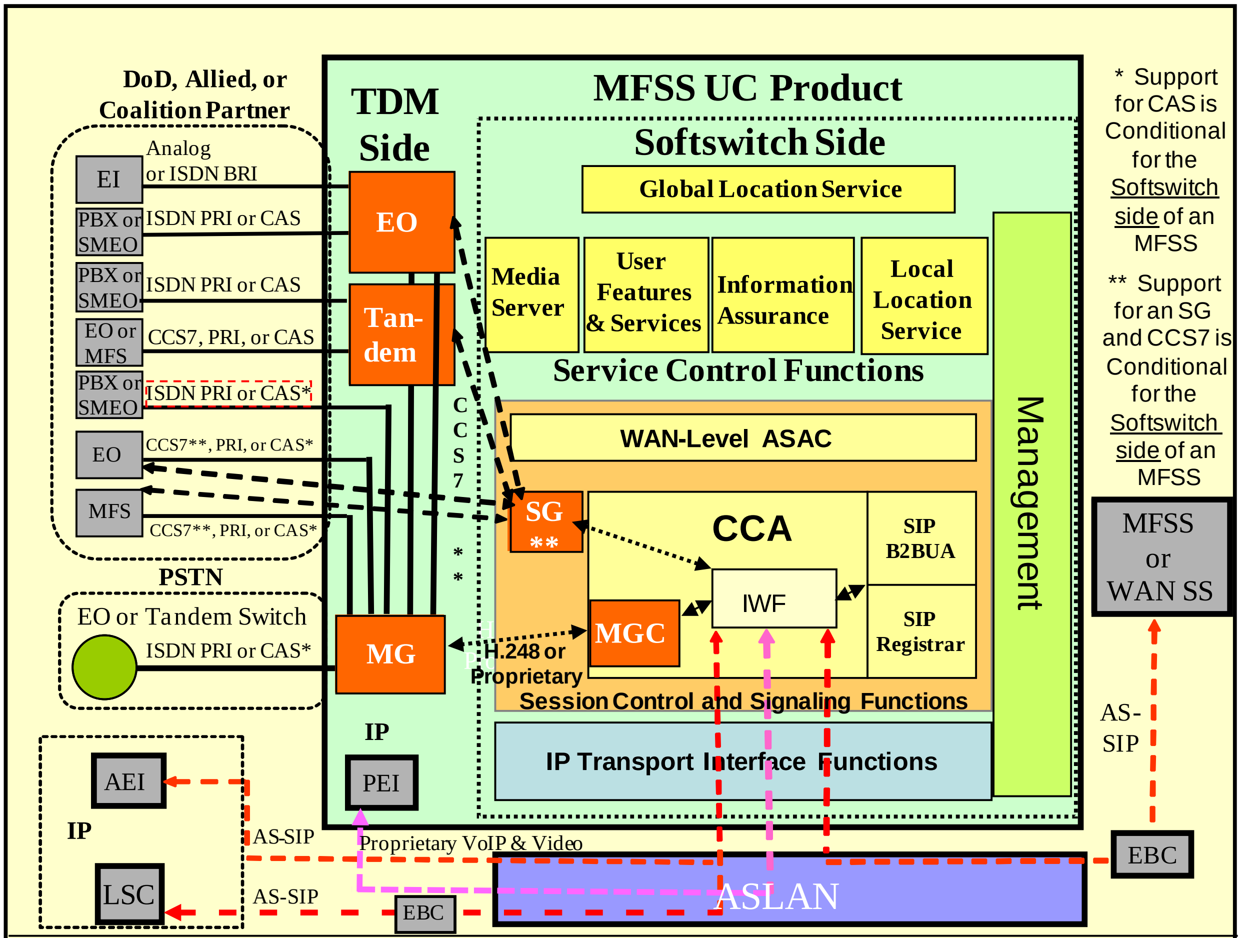
5.3.2.13.2.1 MFSS Functional Reference Model

Figure 5.3.2.13-1, Functional Reference Model – MFSS, shows the functional reference model for the MFSS. It shows the functional components of the MFSS (e.g., SG, CCA, MGC, and MG) and the relationships between the various components. For a description of the different functional components of the MFSS, please refer to Section 5.3.2.8, Multifunction Softswitch.

5.3.2.13.3 SG's Role – Interacting with MFSS Functions and Elements

5.3.2.13.3.1 End Office and Tandem Side of the MFSS

The TDM side of the MFSS supports EO and Tandem Switch functionality. The EO and Tandem functions in the MFSS provide circuit-switched network functions that terminate CCS7/TDM trunks, ISDN lines, and analog lines.



LEGEND:

AEI	AS-SIP End Instrument
ASAC	Assured Service Admission Control
ASLAN	Assured Services Local Area Network
AS-SIP	Assured Services Session Initiation Protocol
B2BUA	Back-to-Back User Agent
BRI	Basic Rate Interface
CAS	Channel Associated Signaling
CCA	Call Connection Agent
CCS7	Common Channel Signaling No. 7
DoD	Department of Defense
EBC	Edge Border Controller
EI	End Instrument
EO	End Office
IA	Information Assurance
IP	Internet Protocol
ISDN	Integrated Services Digital Network
IWF	Interworking Function
LSC	Local Session Controller
MFS	Multifunction Switch
MFSS	Multifunction Softswitch
MG	Media Gateway
MGC	Media Gateway Controller
PBX	Private Branch Exchange
PEI	Proprietary End Instrument
PRI	Primary Rate Interface
PSTN	Public Switched Telephone Network
SCS	Session Control and Signaling
SG	Signaling Gateway
SIP	Session Initiation Protocol
SMEO	Small End Office
SS	Softswitch
SUT	System Under Test
TDM	Time Division Multiplexer
UC	Unified Capabilities
VoIP	Voice over Internet Protocol
WAN	Wide Area Network

Note: The PEI (using Proprietary VoIP and Video) is part of the MFSS UC Product ; the AEI (using AS-SIP VoIP and Video) is not.

Figure 5.3.2.13-1. Functional Reference Model – MFSS

The SG interacts with the EO and Tandem functions through industry-standard external interfaces (e.g., CCS7 signaling links and TDM media trunks, as shown in the MFSS functional model), or through internal interfaces that use protocols that are specific to an appliance supplier’s solution.

5.3.2.13.3.2 SG, CCA, and IWF Relationships

The role and functions of the CCA including the IWF are described in Section 5.3.2.9, Call Connection Agent. The SG does not provide call processing or call control and service control functions. The primary role of the SG is to transfer the call control and service control signaling messages to the CCA of the MFSS where these functions are provided. The SG interacts with the CCA component of the MFSS as follows:

1. Transfers CCS7 call and service control-signaling messages to and from the CCA in support of DoD CCS7 trunk connections supported by the MG of the MFSS. The SG is responsible for conveying the CCS7 call control signaling and service control signaling to the CCA IWF for processing. The CCA IWF in the MFSS supports the necessary interworking of the DoD CCS7 protocols with AS-SIP, and with ISDN PRI and CAS protocols for TDM trunk signaling.

2. Needs to support consistent procedures for encapsulation and de-encapsulation of DoD CCS7 messages in IP packets for transport to and from the CCA in the MFSS.

5.3.2.13.3.3 CCA Interactions with SG

[Conditional: LSC, MFSS] The role of the CCA with respect to the SG in the appliance is as follows:

- Controls all SGs within the appliance.
- Controls all signaling links (DoD CCS7) within each SG.

[Conditional: LSC, MFSS] The CCA shall be responsible for controlling all of the SGs within the MFSS and LSC. (NOTE: This covers cases where there is a single SG within the appliance, and cases that are more complex where there are multiple SGs within the appliance.)

[Conditional: LSC, MFSS] The CCA shall be responsible for controlling each signaling link within each SG within the MFSS or LSC.

[Conditional: LSC, MFSS] The CCA shall be responsible for controlling the DoD CCS7 signaling stream(s) within each signaling link within each SG.

[Conditional: LSC, MFSS] Within the appliance (the MFSS and LSC), the CCA shall use either an IETF-standard set of CCS7-over-IP protocols or a supplier-proprietary protocol to accomplish the previously discussed SG, signaling link, and signaling stream controls.

5.3.2.13.3.3.1 CCA Support for CCA SG Signaling Interface

[Objective] The CCA shall use IETF-standard CCS7-over-IP protocols for SG control. In this case, the CCA shall transport the CCS7 messages that it exchanges with the SG using one of the following IETF-standard Transport Layer Protocols:

- TCP
- UDP
- SCTP

[Conditional] When the CCA uses IETF-standard CCS7-over-IP protocols for SG control, the CCA shall secure the CCS7-over-IP information that it exchanges with the SG using IPSec at the IP Network Layer, consistent with the Information Assurance requirements in Section 5.4, Information Assurance Requirements, in this document.

[Conditional: LSC, MFSS] For SG control, the CCA shall

1. Support Transport Layer functionality, including message sequencing, detection of message loss, and recovery from message loss, which are functionally equivalent to the sequencing, loss detection, and loss recovery mechanisms in TCP and SCTP.

2. Support strong security for the exchange of CCS7 messages and any underlying Transport Layer packets and Network Layer packets, so the security controls (SG and CCA authentication, encryption, and decryption of exchanged messages down to the Network Layer) are at least as strong as the security controls used when UDP/TCP/SCTP and IPSec are used to transport CCS7 messages over IP. This strong security shall be supported consistent with the IPSec requirements in Section 5.4, Information Assurance Requirements, in this document.

[Conditional: MFSS, LSC] When CCS7 ISUP messages are transported between the CCA and SG, the CCA shall support

- Transparent passing of CCS7 ISUP messages between the SG and CCA

- Preservation of correct message sequences, in both directions of transmission

- Detection of message loss and recovery from message loss (e.g., by retransmission of lost messages), in both directions of transmission

- Detection of message errors and correction of message errors (e.g., by retransmission of errored messages), in both directions of transmission

- Securing of CCS7 ISUP messages using CCA and SG encryption, in both directions of transmission

The CCA shall support all these capabilities so the resulting exchange of CCS7 ISUP messages and the security of exchanged CCS7 ISUP messages are identical to what would occur if IETF-standard CCS7-over-IP protocols were used.

5.3.2.13.3.3.2 CCA Support for SG-to-CCA-to-SG Signaling Paths

[Conditional: LSC, MFSS] The CCA shall be able to support multiple SGs.

[Conditional: LSC, MFSS] Since the CCA supports per-call ISUP signaling that enters the appliance on one SG signaling link, and then leaves the appliance on another SG signaling link, the CCA shall support SG-to-CCA-to-SG ISUP signaling paths within the appliance, which link per-call ISUP signaling on a signaling link on one SG with per-call ISUP signaling on a signaling link on the same or another SG.

5.3.2.13.3.4 SG Interactions with Appliance Management Functions

The Management function in the MFSS supports functions for MFSS FCAPS management and audit logs. Details on FCAPS management and audit logs for the SG function in the MFSS are covered in Section 5.3.2.18.2, Management Requirements of the SG Function, in this document.

The SG interacts with the MFSS Management function by

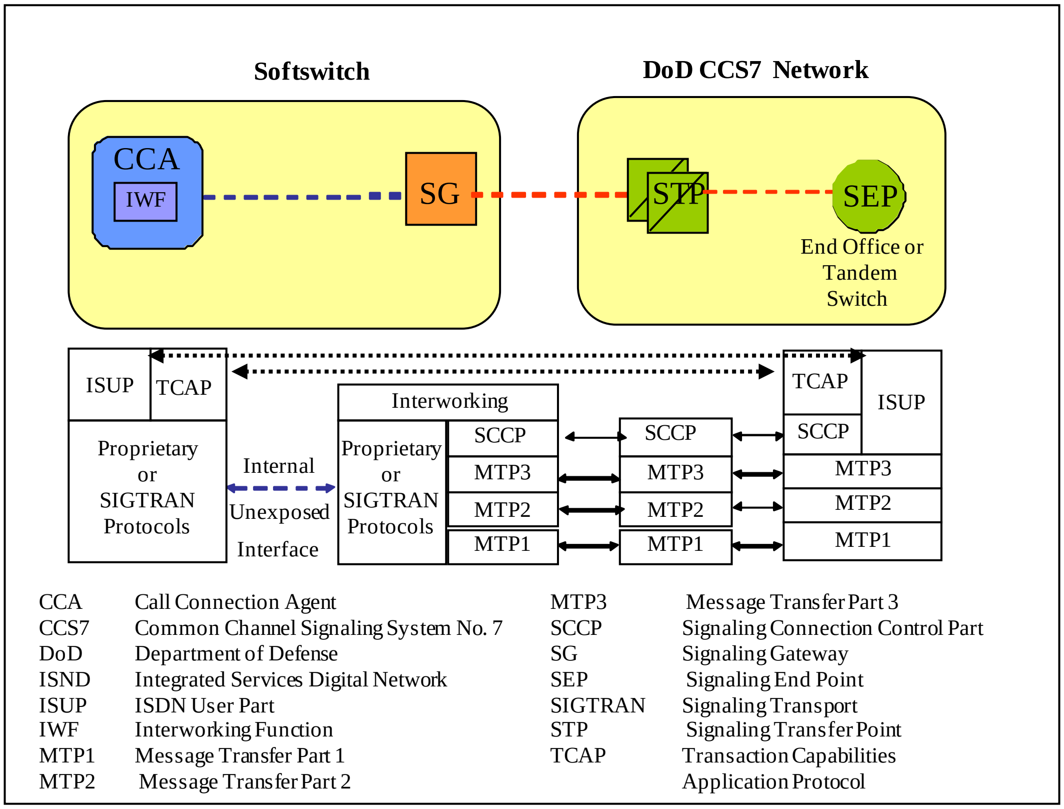
1. Making changes to its configuration in response to the Management function commands that request these changes.

2. Returning information to the Management function on its FCAPS, in response to the Management function commands that request this information.

3. Sending information to the Management function on a periodic basis (e.g., on a set schedule), keeping the Management function up-to-date on SG activity. An example of this update would be a periodic transfer of audit reports from the SG to the Management function, so that the Management function could either store the report locally, or transfer it to a remote NMS for remote storage and processing.

5.3.2.13.4 SG Protocol Design

Figure 5.3.2.13-2, SG Protocol Design, shows the protocol design for the SG, and the relationship with the CCA and signaling points in the interconnected CCS7 network.



CCA	Call Connection Agent	MTP3	Message Transfer Part 3
CCS7	Common Channel Signaling System No. 7	SCCP	Signaling Connection Control Part
DoD	Department of Defense	SG	Signaling Gateway
ISND	Integrated Services Digital Network	SEP	Signaling End Point
ISUP	ISDN User Part	SIGTRAN	Signaling Transport
IWF	Interworking Function	STP	Signaling Transfer Point
MTP1	Message Transfer Part 1	TCAP	Transaction Capabilities Application Protocol
MTP2	Message Transfer Part 2		

Figure 5.3.2.13-2. SG Protocol Design

The SG can be viewed as a functional component with two primary interfaces providing application-level connectivity between CCS7 SEPs and the CCA. The protocol stack interfacing with the CCS7 signaling network is a standard CCS7 protocol stack. The protocol stack interfacing with the CCA is an internal, unexposed interface that can be based on proprietary protocols or IETF SIGTRAN protocols. For example, the interface between the SG and the CCA can use SIGTRAN Adaptation protocols (i.e., Signaling Connection Control Protocol (SCCP) User Adaptation (SUA) specified in RFC 3868; Message Transfer Part 3 (MTP3) User Adaptation (M3UA) specified in RFC 4666; MTP2 Peer-to-Peer Adaptation (M2PA) specified in RFC 4165; or MTP2 User Adaptation (M2UA) specified in RFC 3331) over SCTP/IP. An Interworking Layer is required at the SG to act as a mediation function between the two interfaces as shown in the diagram.

5.3.2.13.4.1 SG and CCS7 Network Interactions

5.3.2.13.4.1.1 SG-CCS7 Interface Functions

The SG provides the following primary functions on the CCS7 network side:

1. CCS7 Network Connectivity. Standard CCS7 link connectivity to the DSN CCS7 network. This includes the necessary link and data link functions and procedures.

2. CCS7 Message Transfer Network Functions. These functions include the following:

    a. Receiving CCS7 messages over a set of links from a CCS7 node (e.g., an STP).

    b. Encapsulating or translating the user information contained in the message (i.e., ISUP information for call setup and service-related signaling, or SCCP/TCAP information for other service-related signaling) for delivery to the CCA.

    c. Processing the received encapsulated ISUP, SCCP/TCAP, and MTP information from the CCA.

    d. Transferring the message to the interconnecting CCS7 node after stripping off the IP packet information.

    e. Populating the lower layer CCS7 information in the message.

3. CCS7 MTP3 NM Functions. These functions include receiving MTP3 NM messages from interconnected CCS7 networks and performing the necessary network management functions and procedures. This includes flow control-related functions between the CCS7 interface and the CCA interface.

4. Transport Protocol Interworking Functions. These functions include providing necessary transport protocol interworking between the CCS7 transport protocols (i.e., Message Transfer Part (MTP) protocols) on the CCS7-SG interface and IP transport protocols (i.e., SIGTRAN or proprietary protocols) on the SG-CCA interface.

5. CCS7 Network Gateway Screening and Security Functions. These functions include providing gateway screening functions to inspect fields and parameters of received CCS7 messages, and providing signaling network monitoring capabilities and functions for security.

5.3.2.13.4.1.2 SG-CCS7 Interface Protocols

MTP Level 1, MTP Level 2, and MTP Level 3 of the CCS7 protocol stack shall be used by the SG for connectivity between the SG and the DISN CCS7 network. The CCS7 MTP protocols are specified in ANSI T1.111.

MTP Level 1 (Signaling Data Link Functions) defines the physical, electrical, and functional characteristics of a signaling data link and the means to access it. The Level 1 element provides a bearer for a signaling link. Signaling Data Link is specified in ANSI T1.111, Chapter T1.111.2, Signaling Data Link.

MTP Level 2 (Signaling Link Functions) defines the functions and procedures for, and relating to, the transfer of signaling messages over one individual Signaling Data Link. The Level 2 functions, together with a Level 1 Signaling Data Link as a bearer, provide a signaling link for reliable transfer of signaling messages between two points.

A signaling message delivered by the higher levels is transferred over the signaling link in variable length signal units. For proper operation of the signaling link, the signal unit comprises transfer control information in addition to the information content of the signaling message.

Signaling Link functions include the following:

- Delimitation of signal unit by flags.
- Flag imitation prevention by bit stuffing.
- Error detection by check bits included in each signal unit.
- Error correction by retransmission and signal unit sequence control by explicit sequence numbers in each signal unit and explicit continuous acknowledgments.
- Signaling link failure detection by signal unit error rate monitoring and signaling link recovery by special procedures

The protocol specification for signaling link functions is given in ANSI T1.111, Chapter T1.111.3, Signaling Link.

MTP Level 3 (Signaling Network Functions) defines the transport functions and procedures that are common to, and independent of, the operation of individual signaling links. These functions fall into two major categories:

1. Signaling Message Handling Functions. These functions, at the actual transfer of a message, direct the message to the proper signaling link or higher level function.

2. Signaling Network Management Functions. These functions, based on predetermined data and information about the status of the signaling network, control the current message routing and configuration of signaling network facilities. In the event of changes in the status, they control reconfigurations and other actions to preserve or restore the normal message transfer capability.

The protocol specification for MTP3 (Signaling Network Functions) is given in ANSI T1.111, Chapter T1.111.4, Signalling Network Functions and Messages. Some means for testing and maintenance of the signaling network are given in ANSI T1.111, Chapter T1.111.7, Testing and Maintenance.

The SCCP provides additional functions to the MTP to provide both connectionless, as well as connection-oriented, network services to transfer circuit-related and non-circuit-related signaling information and other types of information.

The SCCP protocol is specified in ANSI T1.112.

5.3.2.13.4.2 SG and CCA Interactions

5.3.2.13.4.2.1 SG-CCA Interface Functions

The SG provides the following primary functions on the CCA side:

1. Connectivity to the CCA. Provides connectivity to the CCA via an internal, unexposed interface within a vendor solution platform.

2. Message Transfer Functions.

    a. Delivery of encapsulated user information contained in CCS7 messages received from the CCS7 side (i.e., ISUP information for call setup and service-related signaling, or SCCP/TCAP information for other service-related signaling) to the CCA.

    b. Receipt of encapsulated ISUP, SCCP/TCAP, and MTP information from the CCA, stripping off the IP packet information, populating the lower layer CCS7 information in the message, and transferring the message to the interconnecting CCS7 node.

3. SG-CCA Transport Network Management Functions. Provide necessary transport network management functions on the SG-CCA interface based on events on the CCS7 network side (e.g., network congestion and signaling node failure).

5.3.2.13.4.2.2 SG-CCA Interface Protocols

The protocol stack interfacing with the CCA is an internal, unexposed interface that can be based on proprietary protocols or IETF SIGTRAN protocols. For example, this interface can use applicable IETF SIGTRAN Adaptation protocols over the SCTP/IP.

5.3.2.13.4.3 SG Interworking Functions

To enable seamless operation of the peer-to-peer CCS7 call control and service control protocols (i.e., ISUP and TCAP) in the CCS7 SEPs and the CCA, the SG will provide the necessary interworking functions between the transport protocols on the CCS7 side and the CCA side. The interworking function's purpose is to deliver the CCS7 information received from the CCS7 interface in an appropriate form to be conveyed to the CCA. This internal SG function delivers CCS7 messages received from the CCA to the CCS7 interface, after the appropriate NAT, mapping, and appropriate formatting for routing. This function is viewed as an implementation-specific function, depending on vendor-specific solutions.

5.3.2.13.5 Detailed SG Requirements

The requirements identified in this section are **[Conditional: LSC, MFSS]**.

5.3.2.13.5.1 SG and CCS7 Network Interactions

5.3.2.13.5.1.1 General Functional Requirements

[Conditional] The SG shall support signaling connectivity to the DoD CCS7 network based on UCR 2008, Section 5.2, Circuit-Switched Capabilities and Features, specifications for CCS7.

NOTE: The detailed requirements for the SG described in the following sections are based on ANSI CCS7 standards and on UCR 2008, Section 5.2, Circuit-Switched Capabilities and Features, specifications for DoD CCS7.

5.3.2.13.5.1.2 CCS7 Network Protocol Interface

This section describes the MTP requirements for the SG to interface with the DoD CCS7 network using MTP2 signaling links.

5.3.2.13.5.1.2.1 Signaling Data Link Functions (MTP Level 1)

A "signaling data link" is a bidirectional transmission path for signaling, comprising two "data transmission paths" operating together in opposite directions at the same data rate. It is the lowest functional level (Level 1) in the CCS7 functional hierarchy.

[Conditional] The SG shall support the physical, electrical, and functional characteristics of a Signaling Data Link as specified in ANSI T1.111, Chapter T1.111.2, Signalling Data Link, for a 56-kbps data rate.

5.3.2.13.5.1.2.2 Signaling Link Functions (MTP Level 2)

The Signaling Link functions, together with the data link as bearer, provide a signaling link for the reliable transfer of signaling messages between two directly connected signaling points (e.g., the SG and an STP). Signaling messages received from the MTP3 are transferred over the signaling link in variable-length "signal units." The Signaling Link function comprises the following:

- Signal unit delimitation
- Signal unit alignment
- Signal unit error detection
- Signal unit error correction
- Signaling link initial alignment
- Signaling link error monitoring
- Flow control

5.3.2.13.5.1.2.2.1 Signaling Unit Format, Delimitation, and Alignment

[Conditional] The SG shall support the signaling unit formats and coding as specified in ANSI T1.111, Chapter T1.111.3, Signalling Link.

[Conditional] The SG shall perform the protocol procedures as specified in ANSI T1.111, Chapter T1.111.3, Signalling Link, for signaling unit delimitation and alignment.

5.3.2.13.5.1.2.2.2 Signaling Unit Acceptance and Error Detection

[Conditional] The SG shall perform the procedures for signaling unit acceptance and signaling unit error detection as specified in ANSI T1.111, Chapter T1.111.3, Signalling Link.

5.3.2.13.5.1.2.2.3 Error Correction

[Conditional] The SG shall support MTP Signaling Link functions for both terrestrial and satellite signaling links. This involves supporting both of the MTP2 error correction methods specified in ANSI T1.111.3, Signalling Link: the basic error correction method and the preventive cyclic retransmission error correction methods.

5.3.2.13.5.1.2.2.4 Signaling Link Initial Alignment

The procedure for signaling link initial alignment is used for activation and restoration of the signaling link.

[Conditional] The SG shall perform the procedure for signaling link initial alignment as specified in ANSI T1.111, Chapter T1.111.3, Signalling Link.

5.3.2.13.5.1.2.2.5 Signaling Link Error Monitoring

ANSI T1.111 specifies two types of error rate monitor, as follows:

1. The alignment error rate monitor is used while a signaling link is in the proving state of the initial alignment procedure.

2. The signal unit error rate monitor is used while a signaling link is in service and provides one of the criteria for taking the link out of service.

[Conditional] The SG shall support the procedures for alignment error rate monitor as specified in ANSI T1.111, Chapter T1.111.3, Signalling Link. The alignment error rate monitor procedures shall be performed while a link is in the proving state of the initial alignment procedure.

[Conditional] The SG shall support the procedures for signal unit error rate monitor as specified in ANSI T1.111, Chapter T1.111.3, Signalling Link. The signal unit error rate monitor shall be employed for each active signaling link.

5.3.2.13.5.1.2.2.6 Level 2 Flow Control

The procedure for Level 2 flow control is used to control congestion situations at MTP2.

[Conditional] The SG shall support the procedures for Level 2 flow control as specified in ANSI T1.111, Chapter T1.111.3, Signalling Link.

5.3.2.13.5.1.2.2.7 Processor Outage

A processor outage condition occurs when the use of a link is precluded due to factors at a functional level higher than MTP2. An example of this would be if Level 2 could not transfer signaling messages to Level 3. Though one possible cause for this condition is central processor failure, it is possible that the condition would not affect all links in the SG. Furthermore, it is still possible that MTP3 would be able to control the operation of the signaling link, even if it cannot communicate to the other levels.

The goal of the processor outage procedures in different signaling points is to remove the affected link from service when a processor outage condition occurs, and return the link to service when the processor outage condition ceases, all in a coordinated manner between signaling points. These procedures use the changeover and changeback procedures to divert traffic to and from other links.

[Conditional] The SG shall support the processor outage procedures as specified in ANSI T1.111, Chapter T1.111.3, Signalling Link.

[Conditional] The SG shall support the requirements for processor outage that are applicable to a CCS7 SEP, as specified in Telcordia Technologies GR-606-CORE, Section 2.7, Processor Outage.

5.3.2.13.5.1.2.2.8 Provisional Values for Level 2 Timers

[Conditional] The SG shall support the provisional values for MTP2 Timers as specified in Telcordia Technologies GR-606-CORE, Table 1-1, Provisional Values for Level 2 Timers.

5.3.2.13.5.1.2.2.9 Link Performance

1. Signaling Link Availability. Signaling link availability depends on the absence of failures, not only for the link itself, but also for its associated signaling link terminals. The SG should have sufficient connections to STPs to meet an availability objective (99.9996 percent) of not more than 2 minutes per year downtime for network access. Unavailability of network access would occur if the SG became isolated because all signaling links between the SG and the STPs (or EO or Tandem) on which it is connected became unavailable.

2. Link Output Delay. Link output delay is defined as the interval beginning when the message has been placed in the output signaling link terminal buffer and ending when the last bit of the message has been transmitted on the outgoing signaling data link.

Link output delay is the sum of queuing delay and message emission time. Message emission time is a function of the signaling data link speed, message length distribution, and modem delay. Queuing delay is a function of message emission time and link occupancy.

The SG signaling link terminals should meet the message transmission delay objectives stated in Table 5.3.2.13-1, Link Output Delay Objective (15 Octet Long Messages), and Table 5.3.2.13-2, Link Output Delay Objective (279 Octet Long Messages), which are based on the following assumptions:

Table 5.3.2.13-1. Link Output Delay Objective (15 Octet Long Messages)

LINK LOAD	MEAN	95 PERCENTILE
0.4 Erlangs	4 ms	6 ms
0.8 Erlangs	7 ms	18 ms

Table 5.3.2.13-2. Link Output Delay Objective (279 Octet Long Messages)

LINK LOAD	MEAN	95 PERCENTILE
0.4 Erlangs	56 ms	105 ms
0.8 Erlangs	122 ms	323 ms

1. Message retransmissions are not considered when calculating transmission delay.

2. The signaling link is normally loaded to 40 percent of its signaling information transmission capacity (.4 Erlangs traffic loading). The signaling link load under failure conditions is considered to be 8 Erlangs (twice normal loading).

3. Signaling data link speed is 56 kbps.

4. There is no modem delay for the 56-kbps signaling links.

5. Message Signaling Units (MSUs) are a minimum of 15 octets and a maximum of 279 octets in length (see Table 5.3.2.13-1, Link Output Delay Objective (15 Octet Long Messages), and Table 5.3.2.13-2, Link Output Delay Objective (279 Octet Long Messages)). These message length limits are derived from the message formatting principles described in ANSI T1.111. Link output delay objectives are stated only for messages of minimum and maximum length; the actual message transmission delays present at the SG will depend on message length distributions, but should be less than that indicated for messages of maximum length (i.e., 279 octets).

5.3.2.13.5.1.2.2.10 False Link Congestion

See Section 5.3.2.13.5.1.2.4.6, False Link Congestion.

5.3.2.13.5.1.2.3 Signaling Network Functions and Messages (MTP3)

The MTP3 protocol specifies the functions and procedures that are common to, or independent of, the operation of individual signaling links. Level 3 functions fall into two main categories: signaling message handling and signaling network management functions. The MTP3 protocol is specified in ANSI T1.111, Chapter T1.111.4, Signalling Network Functions and Messages.

5.3.2.13.5.1.2.3.1 CCS7 Message Formatting

Specific guidelines for CCS7 message formatting are specified in ANSI T1.111, Chapter T1.111.4, Signalling Network Functions and Messages.

[Conditional] The SG shall adhere to the rules and specifications for formatting of CCS7 messages and coding of the fields and subfields as specified in ANSI T1.111, Chapter T1.111.4, Signalling Network Functions and Messages.

[Conditional] The SG shall be capable of verifying that messages received from interconnected CCS7 networks are of the proper formats and adhere to the rules for coding of the fields and subfields as specified in ANSI T1.111, Chapter T1.111.4, Signalling Network Functions and Messages.

5.3.2.13.5.1.2.3.2 Message Handling

[Conditional] The SG shall support the procedures for message handling as specified in ANSI T1.111, Chapter T1.111.4, Signalling Network Functions and Messages.

5.3.2.13.5.1.2.3.3 Handling of Messages under Signaling Link Congestion

[Conditional] The SG shall support the procedures for the handling of messages under signaling link congestion for U.S. networks, as specified in Section 2.3.5.2, ANSI T1.111, Chapter T1.111.4, Signalling Network Functions and Messages.

5.3.2.13.5.1.2.3.4 Message Discrimination and Distribution

Message discrimination is the determination of whether the SG receiving a message is the correct destination signaling node. All messages received at the SG should be addressed to the SG.

[Conditional] The SG shall examine each message received to verify that the Destination Point Code (DPC) is valid.

[Conditional] If the DPC of a received message does not correspond to the point code assigned to the SG (and CCA), the SG shall report the event to the Management function and should discard the message without further processing.

After the discrimination validates the DPC, the message distribution function is used to deliver the received message to the appropriate MTP user for further processing. The information required for message distribution is contained in the Service Information Octet (SIO).

The CCS7 User Part protocols (e.g., ISUP and TCAP) are not deployed at the SG. Therefore, in theory, after the discrimination function verifies that the DPC of the message is the SG, the MTP distribution function shall deliver the message to the vendor-specific IWF for further processing and transfer to the CCA.

5.3.2.13.5.1.2.3.5 Message Routing

The MTP message routing involves selecting an outgoing signaling link that will deliver a message to its proper destination node.

[Conditional] Before transmitting an MSU, the SG shall identify the normal (combined) link sets on which the message should be transported.

A link set is the set of links from the SG that terminate at a particular signaling point. Link sets of equal ranking or equal preference for carrying a particular signaling message are referred to as a "combined link set."

The preferred link set or preferred combined link set with the highest priority for signaling messages to a particular destination is referred to as the "normal link set." A (combined) link set of lower priority could be identified at the SG in the event that all links in the normal (combined) link set are unavailable. A link set or a combined link set with a lower priority than the normal link set that is used as a backup route to the same destination is referred to as an "alternate link set." The (combined) link set being used at any given time for traffic to a given destination is referred to as the "current (combined) link set." This could be either the normal link set or an alternate link set, but not both.

5.3.2.13.5.1.2.3.6 Backup Routing Procedures

For messages having a DPC uniquely associated with a signaling point that is at the remote end of a signaling link set connected to the SG, the normal link set should consist of the single link set that directly connects the two signaling points. For such messages, the SG should be able to identify a link set or combined link set of lower priority to be used in case all links in the normal link set are unavailable. For other messages, the normal combined link set should consist of at least two link sets between the SG and STPs.

[Conditional] The SG shall support backup routing procedures as specified in ANSI T1.111, Chapter T1.111.4, Signalling Network Functions and Messages.

[Objective] The SG shall support the requirements for backup routing procedures as specified in Telcordia Technologies GR-606-CORE, Section 3.3, Message Routing.

5.3.2.13.5.1.2.3.7 Loadsharing

The purpose of loadsharing is to distribute traffic evenly over the links of a link set (combined link set). The loadsharing method to be used on the CCS7 links is specified in ANSI T1.111, Chapter T1.111.5, Section 7.3, Signalling Network Structure. As specified in ANSI T1.111, loadsharing of messages over available links in a link set is done by using the 8-bit Signaling Link Selection (SLS) field and is referred to as “modified SLS rotation.”

[Conditional] The SG shall support procedures for loadsharing as specified in ANSI T1.111, Chapter T1.111.5, Signalling Network Structure.

[Conditional] The SG shall provide loadsharing of messages over all available links in the current (combined) link set by the method of modified SLS rotation. The 256 possible values of the 8-bit SLS field shall be mapped to the available links so that the total number of values assigned to each link shall differ by no more than one.

Previously, the ANSI CCS7 standard used a 5-bit SLS for loadsharing. Therefore, the SG may have to interconnect to signaling points using a 5-bit SLS field.

[Conditional] The SG shall be capable of interconnecting and operating with signaling points using a 5-bit SLS field.

[Conditional] The SG shall be capable of supporting link set sizes of up to 16 links per link set.

5.3.2.13.5.1.2.3.8 Message Sequencing

The CCS7 signaling link protocol is designed to ensure that all messages sent over the same signaling link will be received at the destination point in the order transmitted, since messages are retransmitted in their original order. Signaling network management procedures are designed with the intent that messages having a common SLS assignment, as well as identical destinations, will be delivered to the destination point in the original order of transmission. Message sequencing for such messages is normally retained even with changes in signaling link availability.

It is assumed that the SLS value is generated by the upper layer CCS7 protocols at the CCA (e.g., ISUP) and provided along with the other information (e.g., DPC and Originating Point Code (OPC)) for the SG to format the outgoing CCS7 message.

5.3.2.13.5.1.2.4 MTP3 Signaling Network Management Functions

5.3.2.13.5.1.2.4.1 Signaling Traffic Management

Signaling traffic management functions are used to divert signaling traffic from a link or route to one or more different links or routes, or to temporarily slow down signaling traffic in the case of congestion at a signaling point.

[Conditional] The SG shall support the following signaling traffic management procedures as specified in ANSI T1.111, Chapter T1.111.4, Signalling Network Functions and Messages:

- Changeover
- Changeback
- Forced rerouting
- Controlled rerouting
- Management inhibiting
- Signaling traffic flow control

[Conditional] The SG shall support the requirements for the following traffic management procedures as specified in Telcordia Technologies GR-606-CORE, Section 4, Signaling Network Management:

- Changeover
- Changeback
- Forced rerouting
- Controlled rerouting
- Management inhibiting
- Signaling traffic flow control

5.3.2.13.5.1.2.4.2 MTP Restart

The MTP restart is described in ANSI T1.111, Chapter T1.111.4, Section 9, MTP Restart. The MTP restart procedure can be separated into actions for being adjacent to a restarting node and actions for a restarting node. The SG is required to perform the actions for being adjacent to a restarting node and to perform procedures for a restarting node is an SG objective.

[Objective for a Restarting SG]

At an SG, the full MTP restart procedures provide value because the SG cannot perform effectively until it has re-established signaling links to at least a significant fraction of its adjacent signaling points. Without the MTP restart procedures, each adjacent signaling point in the CCS7 network will send signaling messages to the SG as soon as a signaling link to the SG becomes available, but a call cannot be completed unless the connection to the CCA is established. The MTP restart procedure shields the SG from user traffic (ISUP) until signaling links have been established to sufficient adjacent nodes. Thus, the SG shall perform MTP restart procedures for a restarting node.

[Objective] The SG shall support MTP restart procedures for a restarting node as specified in ANSI T1.111, Chapter T1.111.4, Section 9, MTP Restart.

[Objective] An unavailable SG that is ready to resume operation by making links available and resuming the exchange of signaling traffic shall initiate the MTP restart procedures corresponding to a restarting node when the first link(s) becomes available at Level 3.

Requirements for an SG adjacent to a restarting signaling point:

- Since the SG will be connected to STPs and EOs that may be supporting the MTP restart procedures, it is necessary that the SG satisfy the requirements for being adjacent to a restarting node.

[Conditional] The SG shall support MTP restart procedures for being adjacent to a restarting node as specified in ANSI T1.111, Chapter T1.111.4, Section 9, MTP Restart.

5.3.2.13.5.1.2.4.3 Signaling Link Management

Signaling link management is used to control the locally connected signaling links. The function provides controls to restore failed links, to activate idle links, and to deactivate aligned links.

[Conditional] The SG shall support the signaling link management procedures for signaling link activation, restoration, and deactivation, and signaling link set activation as specified in ANSI T1.111, Chapter T1.111.4, Signalling Network Functions and Messages, for automatic allocation of signaling data links and signaling terminals.

5.3.2.13.5.1.2.4.4 Signaling Route Management

Signaling route management is used to distribute information about signaling network status and to control signaling routes.

[Conditional] The SG shall support the following signaling route management procedures as specified in ANSI T1.111, Section T1.111.4, Signalling Network Functions and Messages:

- Transfer-prohibited
- Transfer-allowed
- Transfer-restricted
- Signaling-route-set-test
- Transfer-controlled
- Signaling-route-set-congestion

[Objective] The SG shall support the requirements for the following signaling route management procedures as specified in Telcordia Technologies GR-606-CORE, Section 4, Signaling Network Management:

- Transfer-prohibited
- Transfer-allowed
- Transfer-restricted
- Signaling-route-set-test
- Transfer-controlled
- Signaling-route-set-congestion

5.3.2.13.5.1.2.4.5 Message Priority and Congestion Control

Message priorities are indicated in the subservice field of the SIO for CCS7 messages, allowing up to four priority levels. The CCS7 message priorities are not intended to indicate which messages should be processed first, but instead are used to determine which messages should be discarded in the event of signaling network congestion. Messages assigned priority level "0" are of the lowest priority, while priority level "3" is used for messages of the highest priority. Network management messages, with the exception of signaling-route-set-congestion-test messages, are assigned the highest priority.

[Conditional] The SG shall adhere to the message priority scheme as specified in ANSI T1.111, Section T1.111.5, Signalling Network Structure, Annex A.

[Conditional] The SG shall provide nine congestion thresholds for each signaling link: three congestion thresholds set at each of the three levels. There shall be no congestion thresholds assigned that affect transmission of priority 3 messages. The types of congestion thresholds that shall be used are congestion onset, congestion discard, and congestion abatement.

Congestion onset thresholds are used to detect overload conditions, whereas congestion abatement thresholds detect recovery from congestion.

[Conditional] As the transmit buffer occupancy is increasing and a congestion onset threshold is exceeded, or the buffer occupancy drops below a congestion abatement threshold, the SG shall update the congestion status of the signaling link.

[Conditional] If the condition above causes the congestion status of the signaling route set for a destination to be updated, the SG shall notify the MTP user (via the IWF) of the change in congestion status for affected destinations.

[Conditional] The congestion status of the signaling route set for a destination, which indicates the degree of congestion in a signaling route set, shall be maintained by the SG for destinations to which the SG routes messages.

[Conditional] The congestion status of the signaling route set shall be determined as defined in ANSI T1.111, Chapter T1.111.4, Section 3.8.4.

[Conditional] Messages received from local Level 4 (the IWF) with congestion priorities lower than the current signaling route set congestion status shall be discarded by the SG MTP (see ANSI T1.111, Chapter T1.111.4, Section 11.2.4).

The congestion discard threshold is used in combination with the buffer occupancy to determine the signaling link discard status. The signaling link discard status determines whether, during overload conditions, a message from Level 3 should be transmitted or discarded.

[Conditional] The current signaling link discard status shall be determined by the highest discard threshold exceeded by the current buffer occupancy.

[Conditional] If the current buffer occupancy does not exceed discard threshold 1, then the current signaling link discard status shall be zero.

[Conditional] The SG shall discard all messages from Level 3 with a priority lower than the signaling link discard status, but shall continue to transmit messages from Level 3 that are assigned a priority higher than or equal to the signaling link discard status.

5.3.2.13.5.1.2.4.6 False Link Congestion

False link congestion is a condition where a CCS7 link stays in service, but is effectively transmitting or receiving few or no messages. For example, an SG may erroneously believe a link is congested when it is not, or is available when it has failed. There could be more than one root cause of the symptomatic state of an in-service link not effectively transmitting or receiving traffic and not being taken out of service automatically. The effect is harmful, regardless of the root cause: the transmitting end of the link will experience transmit congestion and invoke congestion control Level 3 procedures to stop CCS7 traffic at its source, affecting customer calls and resulting in customer reattempts that increase the call processing and signaling traffic load. One common characteristic of a link experiencing false link congestion is that it stays in one signaling link congestion status for a relatively long period. Therefore, if a link is in the same signaling link congestion status for a given period, it should be removed from service, as described in the following requirement. The link should be removed from service even if the removal causes a destination to be isolated.

[Conditional] The SG shall support the requirements for false link congestion as specified in Telcordia Technologies GR-606-CORE, Section 2.10.

5.3.2.13.5.1.2.4.7 Signaling Link Tests

The CCS7 protocol provides procedures for testing of operational signaling links. The SG should transmit the signaling link test message upon receiving the request from maintenance personnel.

[Conditional] The SG shall support the signaling link test procedure as specified in ANSI T1.111, Chapter T1.111.7, Testing and Maintenance.

1. The SG shall perform the signaling link test when a signaling link is activated or restored.

2. The SG shall perform the signaling link test every T1.111.7/T2 seconds on links while they are in the available state.

3. The SG shall support an option to turn on or turn off the periodic signaling link tests on a per-SG basis.

4. The SG shall route signaling link test and signaling link test acknowledgment messages only on the link being tested (there shall be no loadsharing of messages based on their SLS values).

5.3.2.13.5.1.2.4.8 MTP User Flow Control

The procedure for MTP user flow control is used to control MTP User Part traffic flow when unavailability of an MTP user (e.g., ISUP) is detected. It is assumed that the procedure for MTP user flow control is not widely supported by SEPs (e.g., EOs and Tandems). Therefore, the SG itself will not be required to perform User Part Unavailability (UPU) procedures in the CCS7 network. For example, the SG is not required to send UPU messages. However, the SG should be capable of receiving and accepting a valid UPU message.

[Conditional] The SG shall be capable of receiving and accepting valid UPU messages.

In the SG-CCA CCS7 protocol design, the MTP and SCCP protocols are located at the SG, while the ISUP and TCAP protocols are located at the CCA. In this document, failure or unavailability of any of the protocols above MTP3 (i.e., SCCP, TCAP, and ISUP) is considered to be equivalent to loss of connectivity to the CCA, and the procedures in Section 5.3.2.13.5.1.2.4.10, Actions for Loss of Connectivity to the CCA, apply.

5.3.2.13.5.1.2.4.9 MTP3 Timers

[Conditional] The SG shall support the provisional values and ranges for MTP3 timers as specified in Telcordia Technologies GR-606-CORE, Table 1-2.

5.3.2.13.5.1.2.4.10 Actions for Loss of Connectivity to the CCA

Depending on the implementation design and deployment conditions of the connectivity between the SG and CCA, loss of connectivity to the CCA may occur in certain failure scenarios. When all SG connectivity to the CCA is lost, the MTP in the SG should be notified, based on an implementation-dependent method via the SG IWF. When this occurs, corresponding action must be taken on the CCS7 interface to restrict the traffic being received from the CCS7 network. The corresponding action to be taken on the CCS7 side should be to apply the Processor Outage procedures on all the CCS7 links. This should cause the adjacent STPs (and EOs and Tandems) to stop sending traffic to the SG without having to fail the links on the CCS7 side of the SG.

NOTE: Unavailability of the SCCP, TCAP, and ISUP protocols between the SG and the CCA is considered equivalent to loss of SG connectivity to the CCA.

[Conditional] The SG shall be capable of detecting loss of connectivity to the CCA and detecting when connectivity to the CCA is restored.

[Conditional] The SG shall send the Status Indication Processor Outage (SIPO) message on all CCS7 links when loss of connectivity to the CCA is detected. The method for detecting this loss and performing this action is implementation dependent.

[Conditional] Upon notification that connectivity to the CCA is restored, the SG shall perform the procedures related to cessation of a local processor outage condition as specified in ANSI T1.111, Chapter T1.111.4, Signalling Network Functions and Messages. The method for obtaining the notification and performing this action is implementation dependent.

5.3.2.13.5.1.2.5 SCCP

Support for TCAP is not a requirement; therefore, support for the underlying SCCP is not a requirement. No services or features requiring the utility of TCAP have been identified as required.

5.3.2.13.5.1.2.5.1 Overview

The SCCP protocol provides special message transport capabilities for non-circuit-related information exchange. The SCCP transport capabilities provide additional functions to the MTP protocol. All SCCP information is contained in the signaling information field of the message. The SCCP information consists of an MTP Routing Label, mandatory and optional SCCP message parameters, and a data field. The information contained in the data field is provided by an SCCP user, such as TCAP.

The SCCP protocol supports both connectionless and connection-oriented services. However, the SG is only required to support connectionless services. Specifically, the SG is required to support the following protocol classes for connectionless services:

1. Class 0 – Basic Connectionless Class. This protocol class provides datagram transport. It is appropriate for MSUs that may be transported independent of all other messages. No attempt is made to guarantee a relationship between two or more messages from the same node.

2. Class 1 – Sequenced (MTP) Connectionless Class. This class is similar to protocol class 0 except that related messages are encoded with identical SLS values to determine the signaling path used. Protocol class 1 represents an improved quality of service over protocol class 0 in that message sequencing will be maintained under normal conditions.

5.3.2.13.5.1.2.5.2 SCCP Messages and Parameters

[Conditional] The SG shall support the SCCP messages and parameters for connectionless service as specified in ANSI T1.112, Section T1.112.3:

- Unitdata (UDT)
- Extended Unitdata (XUDT)
- Unitdata Service (UDTS)
- Extended Unitdata Service (XUDTS)

[Conditional] The SG shall support the SCCP management messages and parameters for connectionless service as specified in ANSI T1.112, Section T1.112.3:

- Subsystem-Allowed (SSA)
- Subsystem-Prohibited (SSP)
- Subsystem Status Test (SST)

[Conditional] The SG shall adhere to the coding and addressing rules for SCCP parameters and fields as specified in ANSI T1.112, Section T1.112.3.

5.3.2.13.5.1.2.5.3 SCCP Connectionless Procedures

Since the SG together with the CCA of the MFSS or LSC is viewed as a SEP from the CCS7 network perspective, the SG is only required to support SCCP connectionless procedures that are necessary for a SEP.

[Conditional] The SG shall support connectionless procedures necessary for a SEP originating and receiving SCCP messages in the CCS7 network as specified in ANSI T1.112, Section T1.112.4, for

- Data transfer
- Message return

- Syntax error

5.3.2.13.5.1.2.5.4 SCCP Management Procedures

[Conditional] The SG shall support SCCP management procedures necessary for a SEP originating and receiving SCCP messages in the CCS7 network as specified in ANSI T1.112, Section T1.112.4, for

- Signaling Point Status Management
- Subsystem Status Management

[Conditional] The SG shall support the requirements specified in Telcordia Technologies GR-606-CORE, Section 5.4, for the following SCCP management procedures:

- Signaling Point Status Management
- Subsystem Status Management

5.3.2.13.5.1.2.6 CCS7 Gateway Screening and Security Functions

5.3.2.13.5.1.2.6.1 CCS7 Message Screening

ANSI T1.111, Chapter T1.111.5, Signalling Network Structure, specifies procedures to prevent unauthorized messages on the CCS7 network. These procedures are commonly referred to as “gateway screening.” Gateway screening is performed by the STP in CCS7 networks to check the contents of the incoming message and to determine whether the message should be accepted or rejected (i.e., whether it is authorized) based on criteria specified by the CCS7 network administrator. Typically in CCS7 networks (and as specified in ANSI T1.111), screening at the STP is focused on lower layer protocol information (e.g., MTP and SCCP information). However, screening of ISUP and TCAP information is performed at the CCS7 application level in SEPs.

Since the SG is acting as a gateway network element between the interconnected CCS7 network and VoIP packet network, the SG should support screening functions to minimize the risks (e.g., address spoofing or masquerading) from interconnected CCS7 networks. The screening requirements specified in this document do not impose any solution constraint that the requirements have to be supported by the SG network element itself. However, the SG together with the CCA shall be capable of supporting these requirements.

[Conditional] The SG and CCA shall support procedures to identify unauthorized CCS7 messages (i.e., screening procedures) as specified in ANSI T1.111, Chapter T1.111.5, Section 8, Procedures to Prevent Unauthorized Use of an STP.

[Conditional] In addition, the SG and CCA shall support signaling and control procedures as defined in Alliance for Telecommunications Industry Solution (ATIS) ATIS-PP-1000012.2006.

[Conditional] It shall be possible to establish and implement SG and CCA CCS7 message screening rules for CCS7 at each network interconnection at the SG.

5.3.2.13.5.1.2.6.2 CCS7 Message Monitoring

CCS7 message screening cannot detect certain types of intrusion (e.g., message deletion, insertion, and replay). Therefore, the SG, together with the CCA, should support implementation-specific CCS7 message monitoring systems or tools with functions to detect intrusions and attacks that cannot be detected by CCS7 message screening.

[Conditional] The SG and the CCA shall support an implementation-specific solution for CCS7 message monitoring, or tools capable of detecting CCS7 attacks or intrusions that cannot be detected by CCS7 message screening.

Implementation-specific solutions should be designed to detect attacks and problems (e.g., Denial of Service (DoS) events, misuse of management messages) through observation and analysis of message patterns (e.g., frequency, contents, message types). For example, baseline traffic characteristics (norms) can be established, and algorithms can be defined to monitor network traffic. The monitored CCS7 message pattern can be compared with the established norms to identify abnormal events. The pattern algorithms could be keyed to the generic CCS7 information, such as message types (e.g., MTP, SCCP, ISUP, and TCAP message types), information in the message header (e.g., OPC, DPC, and Service Indicator (SI)), or to detailed application-level information (e.g., TCAP and ISUP parameters).

Implementation-specific solutions may involve, but are not limited to, the following considerations:

- Monitoring at the network level, individual network element level, component or system level, individual protocol level, and the application/service level.

- Monitoring of generic CCS7 information, such as message types (e.g., MTP, SCCP, ISUP, or TCAP), address information (e.g., OPC, DPC, and SI), and application-level information (ISUP and TCAP parameters) against established norms.

- Monitoring of CCS7 traffic volume against established norms.

These solutions may be applied globally to all types of CCS7 message traffic, or may be applied selectively to specific types of CCS7 traffic, based on the identified source of the CCS7 traffic.

5.3.2.13.5.1.2.7 Requirements for MLPP

The MTP message priority values used in the PSTN CCS7 network are different from those used in the DoD CCS7 MLPP network. The SG and CCA are required to adhere to the message priority codes and values specified for DoD CCS7 MLPP.

[Conditional] The SG, together with the CCA, shall adhere to the guidelines and rules for coding of the MTP message priority values for the CCS7 network as shown in Table 5.3.2.13-3, MTP3 Message Priority Value for DoD CCS7 Network.

Table 5.3.2.13-3. MTP3 Message Priority Value for DoD CCS7 Network

IAM MLPP PRECEDENCE LEVEL	MTP PRIORITY VALUE
FLASH OVERRIDE	3
FLASH	3
IMMEDIATE	2
PRIORITY	1
ROUTINE	0

LEGEND

IAM	Initial Address Message	MTP	Message Transfer Part
MLPP	Multilevel Precedence and Preemption		

5.3.2.13.5.2 SG Interactions with CCA

The SG and CCA are considered part of the same solution platform, and the SG-CCA interface is viewed as an internal unexposed interface. Since this interface can be based on proprietary protocols or on variants of SIGTRAN protocols, the requirements in this section are not based on industry protocol specifications as the SG-CCS7 interface requirements are. Instead, this section provides general functional requirements on the SG-CCA interface without placing any constraint on the protocol solution for the interface.

5.3.2.13.5.2.1 General Requirements

The primary functions of the SG-CCA interface are as follows:

1. Transporting and delivering user information contained in CCS7 messages received from the CCS7 side (i.e., ISUP information for call setup and service-related signaling, or TCAP information for other service-related signaling) to the CCA.

2. Transporting and delivering ISUP, SCCP/TCAP, and MTP information from the CCA to the SG for routing to the interconnecting CCS7 node.

Reliability, integrity, and in-sequence delivery is required for the CCS7 information flow over the SG-CCA connection.

[Conditional] The SG shall support a supplier-specific interface to the CCA for interactions between the SG and CCA. The protocol solution for this interface is implementation specific and can be based on IETF's SIGTRAN protocol solution (e.g., use of adaptation protocols over SCTP/IP).

[Conditional] The signaling message flows and interactions on the supplier-specific SG-CCA interface shall be supported over a reliable transport connection providing message sequencing, integrity, detection of message loss, and recovery from message loss, which are functionally equivalent to the sequencing, loss detection, and loss recovery mechanisms in TCP and SCTP.

[Conditional] The signaling message flows and interactions on the supplier-specific SG-CCA interface shall be supported over a secure transport connection. The SG-CCA connection shall support strong security functions for authentication, confidentiality, and integrity in accordance with UCR 2008, Section 5.4, Information Assurance Requirements.

5.3.2.13.5.2.2 Congestion Control

[Conditional] The transport connection between the SG and CCA shall support congestion control procedures. The congestion control mechanism shall be equivalent to the mechanisms used in TCP or SCTP and SIGTRAN Adaptation protocols.

5.3.2.13.5.2.3 Performance

The vendor solution for the SG-CCA interface and connection is required to take into consideration CCS7 performance requirements for the E2E CCS7 message flow. This means that any delays, errors, or message loss introduced by the SG-CCA connection should not result in the E2E CCS7 performance requirements being missed between the CCA and the interconnection CCS7 SEP. For example, MTP3 peer-to-peer procedures require MTP message response times within 500 to 1200 ms. This response time value includes round-trip time and processing time at the remote end. Failure to meet this limitation will result in the initiation of error procedures for expiration of specific timers, e.g., ANSI T1.111.4, timer T4. Similarly, the requirement for E2E call setup delay in ISUP is that an E2E response message (ACM, Answer message(ANS)) be received within 20 to 30 seconds of the sending of the IAM. (NOTE: While this is the ISUP protocol guard timer value, end users will expect faster response time.)

[Conditional] The SG and CCA shall support the message delay requirements (described as protocol guard timers) for MTP, SCCP, ISUP, and TCAP, as specified in ANSI T1.111, T1.112, T1.113, and T1.114, respectively, for the E2E CCS7 message path including the SG-CCA connection.

[Conditional] The SG and CCA shall support the performance requirements for message loss, sequence error, message errors, and availability specified for MTP in ANSI T1.111, Chapter T1.111.6, Message Transfer Part Signalling Performance, for the E2E CCS7 message path including the SG-CCA connection.

5.3.2.13.5.3 SG Interworking Functions

5.3.2.13.5.3.1 General

The SG will terminate CCS7 links on its CCS7 side and transport the CCS7 call control and service control protocols (i.e., ISUP and TCAP) to the CCA. Similarly, the SG will receive CCS7 call control and service control messages from the CCA. The SG is responsible for the appropriate formatting of the messages for transmission on the CCS7 links. To enable seamless operation E2E, the SG will provide the necessary IWFs between the transport protocols on its CCS7 side and its CCA side. This includes necessary functions to interwork the MTP network management procedures on its CCS7 side with the management procedures of the transport connection between the SG and the CCA. This function is viewed as an implementation-specific function, depending on vendor-specific solutions.

[Conditional] The SG shall support vendor-implementation-specific functions to enable seamless interworking between the CCS7 transport protocols (i.e., MTP and SCCP) on its CCS7 side and the transport connection between the SG and CCA. Specifically, the SG shall take specific actions based on management events in the CCS7 network, provide the necessary interworking actions on the transport connections to the CCA, and inform the CCA to take certain actions depending on these interworking actions.

5.3.2.13.5.3.2 Detection and Notification of Loss of Connectivity to CCS7 Network

If conditions in the CCS7 network change, loss of connectivity to the CCS7 network may occur. In addition, local failure of the SG's MTP may occur, which results in loss of connectivity to the CCS7 network. If loss of connectivity to the CCS7 network occurs, appropriate actions must be taken on the SG-CCA interface and the CCA to stop the traffic. NOTE: The notification from MTP3 that CCS7 connectivity has been lost and the detection of local MTP failure are implementation dependent. The following requirements describe the procedures necessary for detection and notification of loss of connectivity to the CCS7 network:

1. **[Conditional]** The SG (i.e., the SG IWF) shall monitor the status of the local MTP3 availability. Upon detection of MTP3 failure (and thus loss of connectivity to the CCS7 network), the SG shall notify the CCA that connectivity to the CCS7 network has been lost. The methods for monitoring the local MTP3 and providing notifications to the CCA are implementation dependent.

2. **[Conditional]** Upon detection of restoral of the local MTP3, which had previously failed, the SG (i.e., the SG IWF) shall notify the CCA that connectivity to the CCS7 network has been restored. The methods for monitoring the local MTP3 and providing notifications to the CCA are implementation dependent.

5.3.2.13.5.3.3 Detection and Notification of Loss of Connectivity to CCA

Depending on certain events, the SG may lose connectivity to the CCA. The following requirements describe the procedures necessary for notification of loss of connectivity to the CCA:

1. **[Conditional]** The SG (i.e., the SG IWF) shall be capable of detecting loss of connectivity to the CCA and notifying the MTP3 of the loss of connectivity. The methods for detection of connectivity loss and providing notifications to MTP3 are implementation dependent.

2. **[Conditional]** The SG (i.e., the SG IWF) shall be capable of detecting that connectivity has been restored to the CCA (which was previously inaccessible) and notifying the MTP3 of the restored connectivity. The methods for detecting of connectivity restoral and providing notification to the MTP3 are implementation dependent.

NOTE: See Section 5.3.2.13.5.1.2.4.10, Actions for Loss of Connectivity to the CCA, for actions to be taken on the CCS7 side because of loss of CCA connectivity.

5.3.2.13.5.3.4 Internal Flow Control Functions

Situations can arise in which the signaling message handling functions at an SG cannot handle messages at the rate at which they are received at the SG. Such situations may result, for example, from a surge of signaling traffic (either to or from the CCA) or from failures that reduce message handling capacity (e.g., MTP2 link set failures). An SG should be able to control the traffic that is destined for the overloaded resources by performing message handling functions in these situations. The CCS7 protocol provides some procedures that may be used to deal with such overload situations. Likewise, the transport connection between the SG and CCA is required to support congestion control procedures. Precise criteria for using each of these procedures in overload situations are dependent on the particular implementation, but some guidelines, objectives, and requirements can be given.

An SG's first defense against an overload of the message handling functions is to reduce the rate at which incoming messages are accepted, to the rate that the message handling functions can process without overload. For interconnection to the CCS7 network, this may result in the invocation of the MTP2 flow control procedures (described in ANSI T1.111, Chapter T1.111.3, Section 9, Level 2 Flow Control), and possibly a triggering of the transfer-controlled procedures or the signaling flow control procedures at adjacent nodes. Use of the Level 2 flow control procedures may be most suitable if there is an overload of the message handling resources associated with a particular incoming link, or if there is a fairly uniform overload of message handling resources at the SG (i.e., the SG-CCA connection has become congested). If the Level 2 flow control procedure is used, it should be designed so that the potential for timer T1.111.3/T6 expiration is not increased.

[Conditional] The SG shall be able to detect when the resources associated with signaling message handling are in danger of becoming overloaded. The method used to detect overload, while supplier dependent, shall be so congestion controls can be performed by the SG. The following two congestion cases apply:

1. If the congestion occurs for traffic directed toward the CCA (from the CCS7 network), the SG shall execute the MTP2 flow control procedures on the signaling links to the CCS7 network nodes causing the congestion.

2. If congestion occurs for traffic directed toward the CCS7 network (from the CCA), the SG shall execute congestion control procedures on the transport connection to the CCA.

5.3.2.14 Customer Edge Router Requirements

5.3.2.14.1 Traffic Conditioning

[Required: CE Router] The 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.

[Required: CE Router] The product shall be capable of traffic conditioning the bandwidth associated with a service class.

5.3.2.14.2 Differentiated Services Support

[Required: CE Router] The product shall be capable of supporting DiffServ in accordance with RFCs 2475 and 2474.

NOTE: The DSCP requirements are specified in Section 5.3.3, Wide Area Network Requirements, of this document.

5.3.2.14.3 Per Hop Behavior Support

[Required: CE Router] The product shall be capable of supporting the Per Hop Behaviors (PHBs).

NOTE: The PHB requirements are specified in Section 5.3.3, Wide Area Network Requirements, of this document.

[Required: CE Router] The product shall be capable of supporting EF PHBs in accordance with RFC 3246.

[Required: CE Router] The product shall be capable of supporting the AF PHB in accordance with RFC 2597.

5.3.2.14.4   Interface to the LSC/MFSS for Traffic Conditioning

[Conditional: CE Router] The CE Router shall be capable of interfacing to the LSC/MFSS in real time to adjust traffic conditioning parameters based on the updated LSC/MFSS budgets.

NOTE: For example, if the LSC budget decreases from ten Voice sessions to five Voice sessions, then the traffic conditioning parameters should change from 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.

5.3.2.14.5   Interface to the LSC/MFSS for Bandwidth Allocation

[Conditional: CE Router] The product shall be capable of interfacing to the LSC/MFSS in real time to adjust the PHB bandwidth allocations based on the updated LSC/MFSS budgets.

NOTE: For example, if the LSC budget decreases from ten Voice sessions to five Voice sessions, then the EF queue bandwidth allocation should change from 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.

5.3.2.14.6   Network Management

[Required: CE Router] The product shall support FCAPS Network Management functions as defined in the Section 5.3.2.17, Management of Network Appliances, in this document.

5.3.2.14.7   Availability

The four types of CE Routers are High Availability, Medium Availability without System Quality Factors (SQF), Medium Availability with SQF, and Low Availability. Defining four types of CE Routers is driven by cost factors, and the availability that can be provided by COTS products.

Locations serving FO/F users and I/P users and R users with PRIORITY and above precedence service should install High Availability CE Routers. The Medium Availability (two types) and Low Availability CE Router provide a cost-effective solution for locations that serve R users.

[Required: High Availability CE Router] 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 5.3.2.5.2, Product Quality Factors, in this document.

[Required: Medium Availability CE Router 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 5.3.2.5.2, Product Quality Factors.

[Conditional: Medium Availability CE Router 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 5.3.2.5.2, Product Quality Factors.

[Conditional: Low Availability CE Router] 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 UCR 2008, Section 5.3.2.5.2, Product Quality Factors.

NOTE: The vendor will provide a reliability model for the product showing all calculations for how the availability was met.

5.3.2.14.8 Packet Transit Time

[Required: CE Router] The CE Router shall be capable of receiving, processing, and transmitting a voice packet within 2 ms or less in addition to the serialization delay for voice packets as measured from the input interface to output interface under congested conditions (as described in UCR 2008, Section 5.3.1.4.1.1, ASLAN Voice Services Latency) to include all internal functions. For example, the serialization delay of a 100BT Interface is 0.017 ms, which would allow for a voice packet latency from input to Ethernet output under congested conditions of 2.017 ms.

NOTE: Internal functions do not include Domain Name System (DNS) lookups and other external actions or processes.

5.3.2.14.9 Customer Edge Router Interfaces and Throughput Support

The CE Router supports an ASLAN-side connection to the EBC and a WAN-side connection to the DISN WAN.

[**Required: CE Router**] The ASLAN-side interface shall be an Ethernet interface (10 BT or 100 BT) full duplex, and at least one of the WAN-side interfaces shall be an Ethernet interface (10 BT or 100BT) full duplex.

[**Conditional: CE Router**] The WAN-side access connection interface can also be 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).

The CE Router needs to support information "throughput" in two directions: from the ASLAN side to the WAN side, and from the WAN side to the ASLAN side. The CE Router also needs to support this throughput in full-duplex mode, which means that the CE Router needs to support the maximum possible throughput on the WAN-side interface for packets sent in the ASLAN-to-WAN direction. At the same time, the CE Router needs to support the maximum possible throughput on the WAN-side interface for packets sent in the WAN-to-ASLAN direction. The maximum possible throughput for an interface is the maximum line rate for that interface, as provisioned on the CE Router.

A CE Router may support multiple interfaces on the ASLAN side, such as two 100 BTs to an EBC and a data firewall, and on the WAN side, such as two DS1s to two different DISN SDNs. These requirements assume that the CE Router only has one WAN-side interface active. They also assume that the line rate for the WAN-side interface is less than or equal to the sum of the line rates for the ASLAN-side interfaces.

[Required: CE Router] The CE Router shall support the maximum possible throughput on the WAN-side interface for a full traffic load of all traffic types sent in the ASLAN-to-WAN direction.

[Required: CE Router] The CE Router shall support the maximum possible throughput on the WAN-side interface for a full traffic load of all traffic types sent in the WAN-to-ASLAN direction.

[Required: CE Router] The CE Router shall support the maximum possible throughput on the WAN side interface in a full-duplex mode, for a full traffic load of UC packets sent simultaneously in both the ASLAN-to-WAN and WAN-to-ASLAN directions.

[Required: CE Router] The maximum possible throughput on the WAN-side interface shall be the maximum line rate that the WAN-side interface is provisioned for on the CE Router. The following maximum possible throughputs shall apply for the different WAN-side interfaces:

- 10 BT: 10 Mbps
- 100 BT: 100 Mbps
- DS1: 1.5 Mbps **[Conditional]**
- DS3: 45 Mbps **[Conditional]**
- E1: 2.0 Mbps **[Conditional]**

5.3.2.15 EBC Requirements

5.3.2.15.1 AS-SIP Back-to-Back User Agent

[Required: EBC] 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 UCR 2008, Section 5.4, Information Assurance Requirements, and the proper processing of an AS-SIP message is found in this section and UCR 2008, Section 5.3.4, AS-SIP Requirements.

1. **[Required: EBC]** 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.

    a. **[Required: EBC]** The product shall assign a locally unique combination of “c” and “m” lines when anchoring the media stream.

    b. **[Required: EBC]** If an INVITE request is forwarded to a product fronting an MFSS for which the INVITE request is not destined (i.e., the MFSS will forward the INVITE request downstream to another MFSS or LSC), the 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 MFSS.

    NOTE: The MFSS will not modify the “c” and “m” lines. The reason why the anchoring occurs upon receipt of the message is that the product does not know at that point whether the session will terminate within the enclave.

    c. **[Required: EBC]** If a session is forwarded or transferred so the session is external to the enclave (i.e., the session no longer terminates or originates within the enclave), then the 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.

2. **[Required: EBC]** The EBC shall be capable of processing Route headers in accordance with RFC 3261, Sections 20.34, 8.1.2, 16.4, and 16.12.

   [Required: MFSS] The MFSS will generate Route headers for the product to tell the product the next hop for the AS-SIP message.

   [Required 2012: LSC, MFSS] Both the LSC and the MFSS will be required to generate Route headers for the product.

3. **[Required: EBC]** The product shall preserve/pass the CCA-ID field in the Contact header.

4. **[Required: EBC]** The product shall always decrement the Max-Forward header.

5. **[Required: EBC]** The product shall modify the Contact header to reflect its IP address to ensure it is in the return routing path.

6. **[Required: EBC]** The product fronting an LSC shall be capable of maintaining a persistent TLS session between the EBC fronting the primary MFSS and the EBC fronting the secondary MFSS. Persistent means the TLS session is established when the product joins the signaling network, and it is not established on a session-by-session basis.

   a. **[Required: EBC]** The EBC shall be capable of distinguishing between the primary (associated with the primary MFSS) and a secondary (associated with the secondary MFSS) TLS path for the purposes of forwarding AS-SIP messages.

   b. **[Required: EBC]** With the exception of OPTIONS requests, the EBC shall forward all AS-SIP messages received from the LSC across the secondary TLS path if the primary TLS path fails, or a notification arrives at the product indicating that the primary MFSS has failed. If the primary TLS path is available, then the EBC MUST continue to send OPTIONS requests received from the LSC to the EBC serving the primary MFSS. Once the primary TLS path is restored or the primary MFSS recovers, the product shall forward all AS-SIP messages corresponding to new call requests across the primary TLS paths. The AS-SIP messages associated with existing calls that were established in conjunction with the secondary MFSS MUST continue to be sent to the EBC for the secondary MFSS to facilitate a non-disruptive failback to the primary MFSS.

(1) **[Required: EBC]** The EBC shall fail over to the secondary TLS path when the product receives an AS-SIP message indicating a (408) Request Timeout, (503) Service Unavailable, or (504) Server Timeout response.

(2) **[Required: EBC]** The EBC shall fail over to the secondary TLS path when it detects a configurable number of AS-SIP OPTIONS request failures. The default number of failures shall be two. NOTE: A failure is indicated by a lack of a response or a failure notice.

(3) **[Required: EBC]** The EBC shall return to forwarding all new calls on the primary TLS path (to the primary MFSS) upon receipt of a 200 (OK) response from the primary MFSS to an OPTIONS request issued by its LSC.

(4) **[Required: EBC]** The EBC fronting a secondary MFSS shall respond with a (481) Call/Transaction Does Not Exist when it receives a RE-INVITE, UPDATE, or BYE AS-SIP message for which it has no match (because the session was established via the primary MFSS).

c. **[Required: EBC]** The EBC initiates a session toward its subtended LSC/MFSS (arriving from the WAN) when receiving an incoming INVITE AS-SIP message from the WAN.

5.3.2.15.2 Call Processing Load

[Required: EBC] The product shall be capable of handling the aggregated WAN call processing load associated with its subtended LSCs and MFSSs.

NOTE: For instance, if the B/P/C/S has three LSCs within the B/P/C/S and each LSC is expected to handle 50 WAN calls per minute, then the CE Router subsystem shall handle 150 calls per minute.

5.3.2.15.3 Network Management

[Required: EBC] The product shall support FCAPS Network Management functions as defined in Section 5.3.2.17, Management of Network Appliances, of this document.

5.3.2.15.4 DSCP Policing

[Required: EBC] The EBC shall be capable of ensuring that media streams associated with a particular session use the appropriate DSCP based on the information in the AS-SIP RPH.

NOTE: This requires that the product maintain a table of the appropriate DSCP for an RPH marking. The mapping between precedence and DSCP is found in Section 5.3.3, Wide Area Network Requirements, of this document.

5.3.2.15.5 Codec Bandwidth Policing

[Required: EBC] The EBC 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.

NOTE: For example, if an AS-SIP message signals that the media session will use a G.729a codec, the product shall traffic shape that session to 44 kbps (39.2 kbps (codec) plus 4.8 kbps (safety margin and signaling)). The 39.2 kbps assumes 20 ms samples or 50 pulses per second (pps). Payload is 8000 bits/50 pps equals 160 bits per packet (20 bytes). The IP overhead (40 bytes) plus Ethernet overhead (38 bytes) plus 160 bits per packet/8 bits per byte equals 98 bytes per packet. The 98 bytes per packet * 50 pps * 8 bits/byte equals 39.2 kbps for IPv4. The IPv6 calculations would occur in the same manner.

5.3.2.15.6 Availability

There are four types of EBCs: High Availability with No Loss of Active Sessions (NLAS), High Availability without NLAS, Medium Availability, and Low Availability. Defining four types of EBCs is driven by cost factors and the availability that can be provided by COTS products. Locations serving FO/F users, I/P users. and R users with PRIORITY and above precedence service should install High Availability EBCs. The Medium and Low Availability EBCs provide a cost-effective solution for locations that serve R users.

[Required: High Availability EBC with NLAS] 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 5.3.2.5.2, Product Quality Factors, of this document.

[Conditional: High Availability EBC without NLAS] 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 UCR 2008, Section 5.3.2.5.2.1, Product Availability, except for Item 9, No Loss of Active Sessions.

[Required: Medium Availability EBC without NLAS] The product shall have an availability of 99.99 percent. The product shall meet the requirements specified in Section 5.3.2.5.2.1, Product Availability, except for Item 9, No Loss of Active Sessions.

[Conditional: Low Availability EBC] The product shall have an availability of 99.9 percent. The product does not need to meet the requirements specified in Section 5.3.2.5.2, Product Quality Factors, of this document.

NOTE: The vendor will provide a reliability model for the product showing all calculations for how the availability was met.

5.3.2.15.7 IEEE 802.1Q Support

[Required: EBC] The product shall be capable of supporting the IEEE 802.1Q 2-byte TCI Field 12-bit Virtual VID.

NOTE: The VID field has 12 bits and allows the identification of 4096 (2^{12}) VLANs. Of the 4096 possible VIDs, a VID value of 0 and 4095 (Hexadecimal FFF) are reserved, so the maximum possible VIDs are 4094. The component must be capable of distinctly tagging each media (i.e., voice, video, data, signaling, and NM) with any of the 4094 VIDs.

5.3.2.15.8 Packet Transit Time

[Required: EBC] The product shall be capable of receiving, processing, and transmitting an UC packet within 2 ms to include executing all internal functions.

NOTE: Internal functions do not include DNS lookups and other external actions or processes.

5.3.2.15.9 H.323 Support

[Conditional: EBC] If the EBC supports H.323 video, then the product shall be capable of processing and forwarding H.323 messages in accordance with Section 5.4, Information Assurance Requirements, of this document.

5.3.2.16 Worldwide Numbering and Dialing Plan

[Required: LSC, MFSS, PEI, AEI] The precedence level and dialed number input to the PEI or AEI shall be as specified in UCR 2008, Section 5.2.3.5.1.2, Interswitch and Intraswitch Dialing.

5.3.2.16.1 DSN Worldwide Numbering and Dialing Plan

[Required: LSC, MFSS] The DSN Worldwide Numbering and Dialing Plan will be used as the addressing schema within the current DSN and its migration into the SIP environment. The highlights of the DSN Worldwide Numbering and Dialing Plan are summarized in the following paragraphs; the detailed specifications of this plan are provided in UCR 2008, Section 5.2, Circuit-Switched Capabilities and Features. The LSC shall operate with the dialing format illustrated in Table 5.3.2.16-1, DSN User Dialing Format. The digits shown in parentheses may not be dialed by the DSN user on all calls.

Table 5.3.2.16-1. 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.					

The highlights of the DSN Worldwide Numbering and Dialing Plan are described as follows:

1. The current DSN numbering plan will be used in the near future by DISN Assured Services users as the means of specifying a called party address within the converged DISN. (Simply stated, an originating user will dial a DSN telephone number.) That means the subscriber’s telephone number will be used as a basis for routing call requests within the AS-SIP-based converged network. The following attributes are associated with the DSN numbering plan:

    a. The internal DSN numbering plan is a private network plan (internally, a DSN number is not an E.164 number), which is modeled after the North American Numbering Plan (NPA-NNX-XXXX). Internally within the DSN, the DSN numbers are not part of the E.164-based global numbering plan; therefore, internally within the DSN, addressing will be based on a “SIP URI” using the “tel URI” with “phone context equals ‘uc’” and not the Electronic Numbering (ENUM) schema. The tel URI method will provide the flexibility required when the DSN numbering plan is expanded to allow variable numbering schemes that will be used in support of coalition partner networks. The rationale is outlined as follows:

        (1) Most all DSN telephones can be direct dialed from the PSTN/PTT telephone, in addition to being direct dialed from internal DSN telephones. This is made possible because the PSTN/PTTs have assigned public telephone numbers to most DSN locations. The PSTN/PTT numbers are part of the global PSTN/PTT E.164 numbering plan. This is significant because, in the future,

the PTTs can use the ENUM scheme within their own IP-based networks to address DSN numbers.

(2) The DSN telephone number is the fundamental and globally unique address element of both the TDM- based real-time DSN and the VoIP- (e.g., SIP) based real-time UC network.

Examples of internal DSN telephone numbers and their corresponding numbers, which are used when dialing through the PSTN, are illustrated in Table 5.3.2.16-2, Examples of Internal DSN Numbers and Their Corresponding Global E.164 PSTN Telephone Numbers.

Table 5.3.2.16-2. Examples of Internal DSN Numbers and Their Corresponding Global E.164 PSTN Telephone Numbers

COUNTRY/ DSN LOCATION	CIVILIAN E.164 NUMBERS	DSN INTERNAL PRIVATE NUMBER
U.S./Scott AFB	+(1) 618-229-xxxx	(312) 779-xxxx
U.S./Wheeler AAF	+(1) 808-656-xxxx	(315) 456-xxxx
Germany/Patch Barracks	+(49) 711-68639-xxxx	(314) 430-xxxx
Bahrain/TCCC	+(973) 1785-xxxx	(318) 439-xxxx
Korea/Yongsan Main	+(822) 7913-xxxx	(315) 723-xxxx

2. Next, it is important to understand the relationship between basic SIP addressing, subscriber identification, and the existing DSN addressing plan and how it will be used as part of the SIP signaling messages. NOTE: The following examples use the SIP connotation.

a. The simplest form of a SIP signaling message is:

sip:sgtbill@patch.eur.uc.mil

This is sgtbill's sip identity. (Note the absence of a telephone number.)

b. The sip identity is a type of URI called a SIP URI (RFC 3261, Section 19.1, SIP and SIPS (Session Initiation Protocol Secure) Uniform Resource Indicators (URI)).

c. The SIP URI has a form similar to an e-mail address, typically containing a username and a host name. In the above example, patch.eur.uc.mil is the domain of sgtbill's SIP service provider (e.g., the LSC at Patch Barracks in the European Theater UC network within the .mil top-level domain).

3. The addressing system needs to correlate sgtbill's telephone number as part of the SIP URI (sip:sgtbill@patch.eur.uc.mil). This can be accomplished by analyzing the SIP URI format outlined as follows (RFC 3261, Section 19.1, SIP and SIPS Uniform Resource Indicators):

   a. The SIP URI general form is as follows:

      sip:user;password@host:port;uri-parameters?headers

      (1) User: This is the identifier of a particular resource at the host being addressed.

          The userinfo part of a URI consists of the following:

          User field, Password field, and the @ sign following them.

          NOTE: The RFC does not recommend using the Password field.

      (2) The "Host" field represents the host (LSC) providing the SIP resources. The Host field contains an FQDN, an IPv4 address, or an IPv6 address. The RFC recommends using an FQDN for the Host field.

          NOTE: Support for IETF FQDNs implies that UC also supports IETF DNS, which uses domain name servers and allows FQDNs to be resolved to IP addresses (and vice versa). The UC support for DNS is not a 2010 requirement in UCR 2008, Change 1. Instead, UC support for DNS is a 2012 objective in UCR 2008, Change 1.

      (3) Because we are addressing hosts that can process telephone numbers (e.g., an LSC), we will use a "telephone-subscriber" field to populate the "user" field. [RFC 3966] This is accomplished by using the tel URI.

          (a) The tel URI specifies the telephone number as an identifier.

          (b) The termination point of the tel URI telephone number is not restricted. It can be in the public telephone network, a private telephone network, or the internet.

          (c) It can be fixed or wireless and address a fixed-wired, mobile, or nomadic terminal.

          (d) The terminal addressed can support any electronic communication service, including voice, data, and fax.

(e) The tel URI specifies the telephone number as an identifier, which can be either globally unique, or only valid within a local context.

In summary, the tel URI allows us to bring a DSN telephone number into the internal DSN SIP addressing schema.

4. RFC 3966 defines the extent to which a telephone number is valid within a private network (e.g., a "local" number), or as a number part of the global public telephone system (e.g., a "global" number).

   a. The DSN, being a private line network (although geographically it is a global network), with an internal standard numbering plan recognized by all DSN voice service locations, allows the definition of the entire DSN numbering plan as "local" telephone numbers at all LSCs in accordance with RFC 3966.

   b. Local telephone numbers must have a "phone context" parameter that identifies the scope of their validity. Standard 10-digit DSN numbers are valid throughout the DSN and the UC network, and thus, the phone context parameter in the UC network becomes phone-context=uc.mil.

   Therefore, an example of a SIP URI containing a 10-digit DSN number becomes:

   sip:3144301123;phone-context=uc.mil

   Finally, there are two ways for SIP signaling to search for the called subscriber.

   sip:sgtbill@patch.eur.uc.mil becomes:

   sip:3144301123;phone-context=uc.mil@patch.eur.uc.mil;user=phone

5. There are two ways of using the SIP URI to direct the network-wide search for the SIP end point address, i.e., by NPA NNX or by a combination of a "username" (sgtbill) in conjunction with the FQDN assigned to an LSC (patch.eur.uc.mil). In the near future, call requests will be forwarded (routed) based on the telephone number contained within the SIP request.

Table 5.3.2.16-3, Mapping of DSN tel Numbers to SIP URIs, provides examples of DSN numbers using SIP URIs that use the syntax defined in RFC 3966 and referenced in RFC 3261, Section 19.1.6.

Table 5.3.2.16-3. Mapping of DSN tel Numbers to SIP URIs

ALIAS TYPE	SIP URI
7-digit intradomain (LSC enclave) call	sip:4305335;phone-context=uc.mil@patch.eur.uc.mil;user=phone
7-digit interdomain (LSC enclave) call within same area code	sip:4801235;phone-context=uc.mil@rsx.eur.uc.mil;user=phone
10-digit interdomain (LSC enclave) call to another area code	sip:3157261135;phone-context=uc.mil@ysm.pac.uc.mil;user=phone

[Required: LSC, MFSS] The CCA shall allow session requests from LSC, MFSS EIs, other appliances, and MFSS MGs to contain

- Called addresses including DSN numbers from the DSN numbering plan
- Called addresses including E.164 numbers from the E.164 numbering plan

NOTE: The LSC and MFSS may require the use of a DSN escape code, such as “98” or “8,” as a prefix to a DSN number from the DSN numbering plan.

NOTE: The LSC and MFSS may require the use of a PSTN escape code, such as “99” or “9,” as a prefix to an E.164 number from the E.164 numbering plan.

[Required: LSC, MFSS] When a session request’s called address includes a DSN number from the DSN numbering plan, the CCA shall determine whether the called DSN number is local to the LSC or MFSS, or external to the LSC or MFSS.

If the called DSN number is local to the LSC or MFSS, the CCA shall complete the session request within the LSC or MFSS.

If the called DSN number is external to the LSC or MFSS, the CCA shall route the session request outside of the LSC or MFSS, using one of the following:

- The external IP address of the next appliance (i.e., LSC or MFSS) that should handle the session request, or

- The local IP address of the LSC or MFSS MG and MG trunk group that should handle the session request.

[Required: LSC, MFSS] When a session request’s called address includes an E.164 number from the E.164 numbering plan, the CCA shall determine whether the called E.164 number is local to the LSC or MFSS, or external to the LSC or MFSS.

If the called E.164 number is local to the LSC or MFSS, the CCA shall complete the session request within the LSC or MFSS.

If the called E.164 number is external to the LSC or MFSS, the CCA shall route the session request outside of the LSC or MFSS, using one of the following:

- The external IP address of the next signaling appliance that should handle the session request, or
- The local IP address of the LSC or MFSS MG and MG trunk group that should handle the session request.

5.3.2.16.1.1 CCA and GLS Support for Dual Assignment of DSN and E.164 Numbers to MFSS EIs

[Required: LSC, MFSS] The CCA shall allow each VoIP and Video PEI and AEI served by an LSC or MFSS to have both a DSN number assigned and an E.164 number assigned.

[Required: LSC, MFSS] For VoIP and Video 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.

5.3.2.16.1.2 CCA Differentiation between DSN Numbers and E.164 Numbers

[Required: LSC, MFSS] The CCA shall be able to distinguish DSN called numbers from E.164 called numbers when processing VoIP and Video session requests from PEIs, AEIs, EBCs, MG line cards, and MG trunk groups.

[Required: LSC, MFSS] The CCA shall be able to distinguish local DSN called numbers from external DSN called numbers when processing VoIP and Video session requests from PEIs, AEIs, EBCs, MG line cards, and MG trunk groups.

[Required: LSC, MFSS] The CCA shall be able to distinguish local E.164 called numbers from external E.164 called numbers when processing VoIP and Video session requests from PEIs, AEIs, EBCs, MG line cards, and MG trunk groups.

[Objective: LSC, MFSS] On SIP and AS-SIP calls from PEIs or AEIs and the EBC, the CCA (and its LLS and GLS Servers) shall use the contents of the phone-context parameter in the called SIP URI to determine

- Whether the session request is intended for a DSN number or an E.164 number, and

- In the E.164 case, whether the E.164 number is locally significant, nationally significant, or internationally significant.

[Conditional: LSC, MFSS] On DoD CCS7 calls from an MG, the CCA shall use the contents of the Nature of Address Indicator and Numbering Plan fields in the ISUP Called Party Number parameter in the IAM to determine

- Whether the call request is intended for a DSN number or an E.164 number, and

- In the E.164 case, whether the E.164 number is locally significant, nationally significant, or internationally significant.

[Required: LSC, MFSS] 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

- Whether the call request is intended for a DSN number or an E.164 number, and

- In the E.164 case, whether the E.164 number is locally significant, nationally significant, or internationally significant.

[Conditional: LSC, MFSS] On CAS trunk calls from an MG, the CCA shall use the identity of the trunk group that the call was received on (and the presence or absence of prefix digits in the received Called Party Number) to determine

- Whether the call request is intended for a DSN number or an E.164 number, and

- In the E.164 case, whether the E.164 number is locally significant, nationally significant, or internationally significant.

5.3.2.16.1.3 CCA Use of SIP "phone-context" to Differentiate between DSN and E.164 Numbers

[Objective: LSC, MFSS] 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:

1. 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.

2. If the "phone-context" parameter in the "User" portion of the called SIP URI indicates a sequence of digits, possibly prefixed with a "+" character, then the CCA shall treat the variable length number that precedes the "phone-context" parameter as an E.164 number.

[Objective: LSC, MFSS] On SIP and AS-SIP calls from MFSS 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:

1. If there is no "phone-context" parameter in the "User" portion of the called SIP URI, then the CCA shall treat the variable length number in the "User" portion of this URI as an international E.164 number.

2. If the "phone-context" parameter in the "User" portion of the called SIP URI contains a "+" character followed by an E.164 country code, but no area code or city code, then the CCA shall treat the variable length number that precedes the "phone-context" parameter as a national E.164 number (for the country identified by the country code).

3. If the "phone-context" parameter in the "User" portion of the called SIP URI contains a "+" character followed by an E.164 country code and an area code or city code, then the CCA shall treat the variable length number that precedes the "phone-context" parameter as a local E.164 number (for the country identified by the country code, and the area or city identified by the area code or city code).

5.3.2.16.1.4 Use of SIP URI Domain Name with DSN Numbers and E.164 Numbers

The SIP URIs used for VVoIP calls contain both a username (with a numeric Called Party Number and an optional "phone-context" parameter) and a domain name, such as "patch.eur.uc.mil" or "ysm.pac.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 not a 2010 requirement in UCR 2008, Change 1. Instead, UC support for DNS is an 2012 objective in UCR 2008, Change 1.

[Objective - 2010: LSC, MFSS – Required - 2012: LSC, MFSS] Each signaling appliance shall support a configurable per-appliance parameter that indicates how the appliance handles domain names received in VoIP and Video session requests.

This parameter, named "Domain Name Treatment for Session Requests," shall support the following values:

- Overwrite with Network Domain Name
- Overwrite with Appliance FQDN
- Passthrough

The default value shall be Overwrite with Network Domain Name.

To meet this requirement, the appliance must support all three of these options, and must support the default parameter value of "Overwrite with Network Domain Name." The appliance must allow the option selected to be software-configurable.

[Objective - 2010: LSC, MFSS – Required - 2012: LSC, MFSS] 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.

[Objective - 2010: LSC, MFSS – Required - 2012: LSC, MFSS] 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, CUC) shall be supported: "uc.mil" and "cuc.mil."

[Objective - 2010: LSC, MFSS – Required - 2012: LSC, MFSS] When the value of the Domain Name Treatment for Session Requests parameter for the appliance is Overwrite with Appliance FQDN, the appliance CCA shall discard all domain names received in called SIP URIs in session requests, and overwrite them with the FQDN of the appliance.

[Objective - 2010: LSC, MFSS – Required - 2012: LSC, MFSS] The appliance shall support a per-appliance parameter called the "Appliance FQDN," to be used in overwriting the received domain names in this case.

The value of this parameter shall be a text string that identifies the FQDN of the appliance, for domain name overwriting purposes. Examples of possible FQDNs for appliances (i.e., LSCs, MFSSs) are as follows:

- "lsc10.mfss20.patch.germany.eur.uc.mil" (i.e., LSC 10, subordinate to MFSS 20, located at the Patch Barracks in Germany in the European Theater on the UC network)

- "lsc20.lsc30.mfss40.ysm.korea.pac.uc.mil" (i.e., LSC 20, subordinate to LSC 30, subordinate to MFSS 40, located at Yongsan Main in South Korea in the Pacific Theater on the UC network)

- "mfss50.scott.cent.conus.uc.mil" (i.e., MFSS 50, located at Scott Air Force Base in Central CONUS on the UC network)

[Objective - 2010: LSC, MFSS – Required -2012: LSC, MFSS] When the value of the Domain Name Treatment for Session Requests parameter for the appliance is "Pass-through," the appliance CCA shall transparently pass-through all domain names received in called SIP URIs in session requests, without altering them.

5.3.2.16.1.4.1 SIP URI Domain Names in UC Spiral 1

[Required: LSC, MFSS] The MFSS or LSC is only required to support one network FQDN for use with SIP URI domain names: "uc.mil" if that appliance is used for SBU traffic, and "cuc.mil" if that appliance is used for classified traffic.

[Required: LSC, MFSS] The MFSS or LSC is required to ensure that all AS-SIP session requests entering or leaving that appliance use the network FQDN of that appliance (i.e., "uc.mil" for SBU traffic, or "cuc.mil" for Classified traffic) as the domain name in called SIP URIs.

In cases where a received called SIP URI in a received AS-SIP message has a domain name other than "uc.mil" (for SBU traffic) or "cuc.mil" (for Classified traffic), the MFSS or LSC shall either

1. Reject the AS-SIP session request that contained the unexpected domain name, or

2. Accept the AS-SIP session request that contained the unexpected domain name, but overwrite the received domain name with "uc.mil" (for SBU traffic) or "cuc.mil" (for Classified traffic).

Future versions of the UCR document will give additional detail on requirements for the support of SIP URI domain names that are different from "uc.mil" and "cuc.mil."

5.3.2.16.1.5 Domain Directory

Before discussing directories and directory services, it is important to understand that within the IP telephony environment, directories and directory services are not required or used for processing and routing of telephone call requests. Rather, the term directory services refers to the capability of using an IP telephone or other voice and/or video end points for looking up user information directly to obtain a user's telephone numbers (often referred to as "white pages" service). This eliminates the need for dialing an operator or using a hard-copy telephone book to obtain this information.

[Required: LSC, MFSS] All voice systems, TDM or IP technology-based, must contain subscriber assignment information.

Traditionally, the subscriber assignment information contained within telephone switching systems consisted of just the subscriber telephone number, line equipment assignment, and subscriber calling classmarks. Typically, data elements, such as the subscriber name, physical address, e-mail address, or department code, were not part of the subscriber line assignment information. An internal table structure, rather than embedded databases, was used by the switching system to store this information.

Most new IP-based VoIP systems have the capability to store subscriber name, physical address, e-mail address, and/or department code in addition to the basic traditional assignment information as part of the subscriber information. Rather than using a table structure, the new systems store this information as embedded databases, often referred to as "directories" as part of the LSC complex. An example of the embedded subscriber line database would be a Lightweight Directory Access Protocol (LDAP)-compliant format. This arrangement of a subscriber line database represents a more "open standard" than a current TDM system's unique arrangement of using a table-based internal call processing structure.

The discussion of LDAP-based subscriber line databases here applies to Fixed appliances only, and not to Deployable appliances. Requirements for subscriber line databases for Deployable appliances are candidates for a future version of this document.

When the LSC uses an LDAP (or other open standard)-based structure to store subscriber line data, this data can be imported easily from, or exported to, other external LDAP-based structures. The LDAP-based directories are extensible and multiple entries of "telephony" data can be added in batch mode, or additional attributes can be added to an existing LDAP directory using LDAP Interchange Format (LDIF) files. Consequently, when installing a new VoIP system, a subset of the subscriber line information can be extracted from an existing corporate directory (if it contains subscriber telephone number information) and automatically loaded into a new VoIP system. This represents a labor saving over having to build a portion of the subscriber information database manually.

Pure IP-based systems often have a built-in feature allowing importing and exporting of relevant telephone subscriber information between the VoIP system and an existing external "enterprise directory." Telephony-related data is usually stored in a single branch of the enterprise directory (referred to as the IP Telephony Network Branch). This enterprise directory is often a corporate e-mail directory. To facilitate data transfer, both the VoIP system subscriber database and the external corporate directory conform to a common standard.

Most VoIP systems provide instruments that can provide access to a "directory" function. These telephones have a display where alphanumeric information, such as telephone numbers and subscriber names, can be shown. A user can access the directory function via a dedicated button or via soft keys. Then the VoIP system connects the telephone to the directory portion of the subscriber line database. Then the user can initiate a directory search from the telephone. This search is performed against subscriber data contained within the LSC where the telephone is registered.

Additionally, VoIP systems have a feature allowing their instruments to access a web browsing capability. Since a VoIP telephone is connected to a LAN to obtain voice services through the LSC, a VoIP telephone also may be allowed to access an external directory server. This opens up possibilities: If the external directory server is accessible from the LAN, the IP telephone user may be allowed to browse to the corporate directory and perform a search of that directory, as well as the LSC-contained directory.

A domain directory should allow the following functions:

1. Allow a user assigned to an LSC to look up the telephone numbers of other users assigned to (served by) that common LSC. This function is referred to as "white pages" services, and it should not be confused with call routing tables used for forwarding SIP call requests.

2. For security reasons, the Directory Look-Up function will only be available from a user's IP telephone instrument, not via the Internet. The IP telephone instrument will contain a small display and function keys that facilitate the Directory Look-Up function.

3. Access to the Directory Look-Up function shall be controlled by subscriber classmarks. There may be specific reasons for denying this privilege to certain users.

4. The LSC shall allow the system administrator to update the directory database in response to service order activity (i.e., subscriber adds, moves, changes, or removals). The LSC shall update the white pages data automatically as well as subscriber line information contained as part of the Directory Look-Up function.

5. When automatic instrument registration is allowed using DHCP, a service order “flag” must be sent to the system administrator terminal so the administrator can update the subscriber’s location information as necessary.

6. The data elements shown in Table 5.3.2.16-4, White Pages Directory Data Elements, shall be incorporated as part of the white pages directory portion of the LSC subscriber database.

Table 5.3.2.16-4. 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

7. In the near-term planning horizon, the local directory contained within an LSC will not be required to send updates automatically to a “global directory” database, but planning should allow for this in the future. Then the automatic update shall be performed at a defined interval (e.g., weekly) using an automated electronic transfer of data. The transfer will be under the control of a system administrator responsible for the global directory.

8. It is anticipated that long-range functionality should be provided so that the “telephone part” of the LSC directory can be imported to an external “corporate” (e-mail) directory. (NOTE: It is anticipated that the external DSN directory will be a branch of the UC directory under development by the Net-Centric Enterprise Services (NCES) effort.) This function will require that the external directory is based on common standards, for example LDAP, and that the administrator in charge of the external directory extends the directory schema to add new object classes for storing the user telephony information. Likewise, the LSC must have stored the subscriber directory information previously in an LDAP-based system as outlined previously under item 6. Under these conditions, an LDIF file can be used to facilitate the upload of multiple entries in batch mode, or add the telephony attributes to the existing external LDAP directory.

   The material here on exporting an LSC directory to an external “corporate” directory (and storing subscriber directory information in an LDAP-based format) applies to Fixed appliances only, and not to Deployable appliances. Requirements for LSC directory exports for Deployable appliances are candidates for a future version of this document.

9. The user should be offered the following ways of searching for local (domain) directory information:

a. User access to the local domain directory is provided by a "directory" feature available on the VoIP instrument. Directory search will be limited to information contained within the LSC subscriber information.

b. The basic search may be made based on Last Name, First Name.

c. The advanced search utility should have a built-in Boolean logic to perform searches using OR with multiple entries in a single field AND across fields.

5.3.2.16.1.6 Global Directory Services

A global directory service should not be confused with the directory itself, which is the database that holds the information about objects that are to be managed by the directory service. The global directory service is the interface to the directory and provides access to the data that is contained in that directory. It acts as a central authority that can securely authenticate resources and manage identities and relationships between them.

A directory service is highly optimized for reads and provides advanced search on the many different attributes that can be associated with objects in a directory. The data that is stored in the directory is defined by an extendable and modifiable schema. Directory services use a distributed model for storing their information, and that information is usually replicated between directory servers.

[Objective: MFSS] A global directory services system shall allow the following functions and interfaces:

1. Allow a DSN user to perform a DSN-wide telephone number look-up for a user assigned anywhere on the DSN. This function is referred to as white pages services, and it should not be confused with call routing tables used for forwarding of SIP call requests.

2. For security reasons, the telephone directory look-up function will only be available from a user's telephone instrument, not via the Internet.

3. Access to the Directory Look-Up function shall be controlled by subscriber classmarks. There may be specific reasons for denying this privilege to certain users.

4. A global search capability will require multivendor Interoperability among LSCs. This will be made feasible by using standardized formats (e.g., LDAP based) for storing directory data within an LSC.

5. A global search capability should allow a user to search using the basic or advanced search methods outlined in Section 5.3.2.16.1.5, Domain Directory, item 9, as well as by

specifying the "name" of an LSC (e.g., patch.eur.uc.mil). This capability will require that an LSC extend a directory search request through the signaling network.

6. In the near-term planning horizon, the local directory contained within an LSC will not be required to send updates automatically to a "global directory" database, but planning should allow for this in the future. Then the automatic update shall be performed at a defined interval (e.g., weekly) using an automated electronic transfer of data. The transfer will be under the control of a system administrator responsible for the global directory.

7. It is anticipated that long-range functionality should be provided so the "telephone part" of the local directory can be imported to an external local "corporate" e-mail directory. (NOTE: It is anticipated that the external DSN directory will be a branch of the UC directory under development by the NCES effort.) This function will require that the external directory is based on a common standard (e.g., LDAP), and that the administrator in charge of the external directory extends the directory schema to add new object classes for storing the user telephony information. Likewise, the LSC must store the subscriber directory information outlined previously under item 6 using a common standard (e.g., LDAP based). Under these conditions, an LDIF file can be used to facilitate the upload of multiple entries in batch mode, or add the telephony attributes to the existing external directory.

8. In the near-term planning horizon, the domain directories will not be required to send updates automatically to a global directory database, but planning should allow for this in the future. The automatic update shall be provided at a defined interval (e.g., weekly) using an automated electronic transfer of data.

9. The location and administration responsibilities and standard to be used for the global directory database and server have yet to be determined.

5.3.2.17 Management of Network Appliances

Figure 5.3.2.17-1, Network Appliance Management Model, is a logical view of a network appliance with an emphasis on its management functions. The internal implementations of the management functions are determined by the appliance supplier and may or may not align with Figure 5.3.2.17-1.

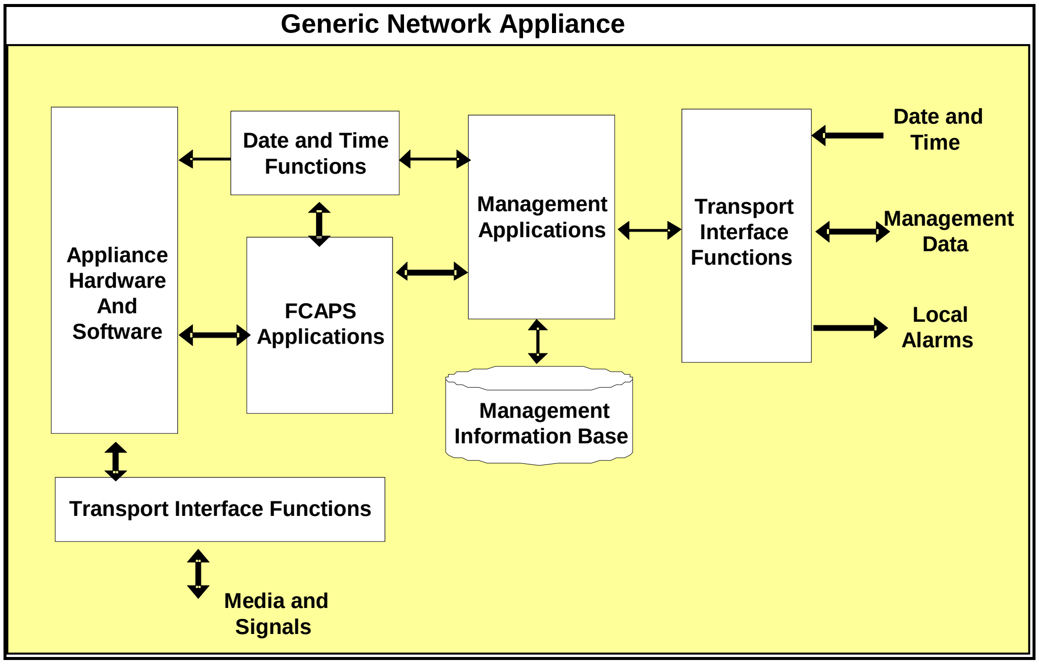

Generic Network Appliance
Appliance Hardware And Software
Date and Time Functions
FCAPS Applications
Management Applications
Management Information Base
Transport Interface Functions
Transport Interface Functions
Date and Time
Management Data
Local Alarms
Media and Signals

Figure 5.3.2.17-1. Network Appliance Management Model

This document makes no assumptions about the number of physical components that constitute a network appliance or of the spatial distribution of these components.

All internal interactions are determined by the supplier and are out of the scope of this document.

Figure 5.3.2.17-1 is a functional model and does not require that the Network Appliance Management functions be internal to the appliance. However, the figure does imply that interfaces between the management functions and the appliance's hardware and software elements are closed.

In this section, the management requirements are frequently specified in terms of network appliances, or NEs. It is understood that these requirements refer to the management functions associated with the network appliance, or NE.

5.3.2.17.1 Voice and Video Network Management Domain

Management of DoD's UC Voice and Video services requires each UC product have a minimum of two separate management domains. Typically, one domain will provide local, on-site craft person type support, typically referred to an OA&M, while the other domain will provide a remote, centralized management capability, typically referred to as NM. There is no attempt to delineate the responsibilities between these two functions in this section. The essential point of this OA&M/NM construct is that two separate domains must have simultaneous access to the UC products to effectively perform the DoD's E2E UC Management function. Where necessary, for clarification, the remote NM system will be referred to as the VVoIP EMS and the local OA&M system will be referred to as the Local EMS. See Figure 5.3.2.17-2, Relationship of UC Managements.

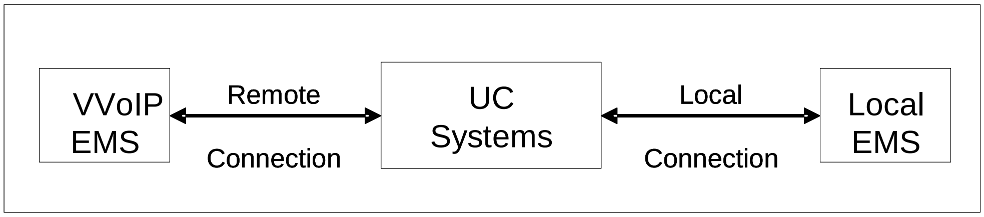


Figure 5.3.2.17-2. Relationship of UC Managements

5.3.2.17.2 General Management Requirements

This document assumes that all Voice and Video network switching appliances meet the requirement in UCR 2008, Section 5.2.8.1, DISA/DSN Network Management.

Except where otherwise specified, Telcordia Technologies GR-740-CORE shall guide the interface between the network appliances (or components) and the external VVoIP EMS.

The following Network and Systems Management are common across all DISN components in the VVoIP solution, including, but not limited to, the MFSS and its elements, the WAN SS and its elements, the LSC and its elements, the CE Router, and the EBC. The MFSS, WAN SS, and LSC components shall each have an individual pair of Ethernet interfaces for management purposes, even in cases where the MFSS or LSC component contains multiple physical devices. It is understood that the EBC and the CE Router components shall each have their own individual pair of Ethernet management interfaces, as specified in Section 5.3.2.4.4, VoIP NMS Interface Requirements.

[Objective] The preferred approach to managing the DoD VVoIP is using SNMP and MIBs. The two applicable IETF Standards are Standard 58 and 62. These two standards are composed of the following RFCs:

- Standard 58, Structure of Management Information Version 2 (SMIv2)
  - RFC 2578
  - RFC 2579
  - RFC 2580
- Standard 62, Simple Network Management Protocol Version 3 (SNMPv3)
  - RFC 3411

- RFC 3412
- RFC 3413
- RFC 3414
- RFC 3415
- RFC 3416
- RFC 3417
- RFC 3418

Although the title of Standard 62 indicates SNMPv3, SNMPv2 is still the predominant protocol in use. SNMPv2 is defined in RFCs 3416, 3417, and 3418.

In addition to the two standards listed earlier, RFC 1213, still contains much of the MIB-II definition.

[Required 2010: NM] SNMPv3 format

[Required] As specified in Section 5.3.2.4.4, VoIP NMS Interface Requirements, the MFSS, WAN SS, and LSC components shall support at least one pair of physical Ethernet management interfaces at the component level (not at the device level). One of these Ethernet management interfaces shall be used for component-level communication with a Local EMS. The other Ethernet management interface shall be used for component-level communication with the remote VVoIP EMS. The MFSS and LSC components shall also support at two redundant physical Ethernet interfaces at the component level (not the device level) to carry the signaling and media streams for VVoIP traffic.

Per Section 5.3.2.4.4, the signaling and bearer traffic may use the same physical Ethernet interface as the local or VVoIP EMS management traffic, or it may use a separate physical Ethernet interface. If the signaling and bearer traffic shares a physical Ethernet interface with the local or VVoIP EMS management traffic, then the signaling and bearer traffic must use a separate VLAN.

Example 1: Four physical Ethernet interfaces per LSC or MFSS:

- Local EMS management traffic
- VVoIP EMS management traffic
- Signaling and bearer traffic (redundant with interface D)
- Signaling and bearer traffic (redundant with interface C)

Example 2: Two physical Ethernet interfaces per LSC or MFSS:

- Local EMS management traffic on one VLAN, plus
  signaling and bearer traffic on a separate VLAN

(redundant with signaling and bearer traffic on the separate VLAN on
interface B)

- VVoIP EMS management traffic on one VLAN, plus
  signaling and bearer traffic on a separate VLAN
  (redundant with signaling and bearer traffic on the separate VLAN on
  interface A)

[Required] As specified in Section 5.3.2.4.4, VoIP NMS Interface Requirements, the EBC and CE Router components shall support one pair of physical Ethernet management interfaces at the component level. One of these Ethernet management interfaces shall be used for component-level communication with a Local EMS. The other Ethernet management interface shall be used for component-level communication with the remote VVoIP EMS. The EBC and CE Router components shall also support at two redundant physical Ethernet interfaces at the component level to carry the signaling and media streams for VVoIP traffic.

Per Section 5.3.2.4.4, the signaling and bearer traffic may use the same physical Ethernet interface as the local or VVoIP EMS management traffic, or they may use a separate physical Ethernet interface. If the signaling and bearer traffic shares a physical Ethernet interface with the local or VVoIP EMS management traffic, then the signaling and bearer traffic must use a separate VLAN.

Example 1: Four physical Ethernet interfaces per EBC or CE Router:

- Local EMS management traffic
- VVoIP EMS management traffic
- Signaling and bearer traffic (redundant with interface C)
- Signaling and bearer traffic (redundant with interface D)

Example 2: Two physical Ethernet interfaces per EBC or CE Router:

- Local EMS management traffic one VLAN, plus
  signaling and bearer traffic on separate VLAN
  (redundant with signaling and bearer traffic on the separate VLAN on
  interface B)

- VVoIP EMS Management traffic , plus
  signaling and bearer traffic on separate VLAN
  (redundant with Signaling and bearer traffic on the separate VLAN on
  interface A)

[Required] A network appliance shall have Operations interfaces that provide a standard means by which management systems can directly or indirectly communicate with and, thus, manage the various network appliances in the DISN.

[Required] The physical interface between the Local EMS and the VVoIP network components (i.e., LSC, MFSS, EBC, CE Router) shall be an Ethernet connection as specified in Section 5.3.2.4.4, VoIP NMS Interface Requirements. The physical interface between the VVoIP EMS and the VVoIP network components shall also be an Ethernet connection as specified in, Section 5.3.2.4.4.

[Required] There shall be a local craftsperson interface (Craft Input Device (CID)) for OA&M for all VVoIP network components. The CID is a supplier-provided input/output device that is locally connected to a network component. The CID may be connected to the Local EMS, which is in turn connected to the VVoIP component using the Local EMS Ethernet management interface. The CID may be connected directly to the VVoIP network component also, using the Ethernet management interface on the component that would otherwise be used by the Local EMS (there is no Local EMS in this case). The CID may be connected directly to the VVoIP network component using a separate serial interface.

[Required] The network appliances shall provide NM data to the external VVoIP EMS.

[Required] A network appliance shall communicate with an external Voice and Video management system by a well-defined, standards-based management interface using an industry-accepted management protocol.

While the majority of management applications will use an interactive mode of communication, some management applications (e.g., transfer of bulk performance information, downloading software generics) will use file-oriented communications.

[Required] Communications between VVoIP EMS and the VVoIP network appliances shall be via IP.

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

- **[Required 2010: NM]** Extensible Markup Language (XML)
- **[Objective 2012: NM]** Multi-Technology Operations System(s) Interface (MTOSI)

[Objective] To support file-oriented communications, it is desirable that a network appliance support a Federal Information Processing Standard (FIPS) 140-2 encryption algorithm.

[Required] A network appliance shall issue state change notifications for changes in the states of replaceable components, including changes in operational state or service status, and detection of new components.

[Required] A network appliance shall be provisioned by the VVoIP EMS with the address, software, and OSI Layer 4 port information associated with its Core Network interfaces.

[Required] 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.

[Required] Network appliances that provide voice and video call service shall have the capability to invoke traffic flow (NM) controls as detailed in Section 5.3.2.18, Network Management Requirements of Appliance Functions.

[Required] A network appliance shall be capable of setting the Administrative state and maintaining the Operational state of each Core Network interface, and maintaining the time of the last state change.

[Required] A network appliance shall generate an alarm condition upon the occurrence of any of the following failure conditions, as defined in ITU-T Recommendation M.3100:

- Power loss
- Environmental condition not conductive to normal operation
- Loss of data integrity

[Required] A network appliance shall be capable of maintaining and responding to requests for physical resource capacity information for installed components. This information includes the following:

- Component type and model
- Shelf location
- Rack location
- Bay location

5.3.2.17.3 Requirements for FCAPS Management

The requirements for the five general functional areas of FCAPS management involve the CCA, SG, and MG functions. Detailed descriptions of how these functions support the FCAPS management requirements are provided in separate sections of the UCR 2008, as follows:

1. Section 5.3.2.18.3, Management Requirements of the CCA Function, contains management requirements for the CCA function.

2. Section 5.3.2.18.4, Management Requirements of the SG Function, contains management requirements for the SG function.

3. Section 5.3.2.18.5, Management Requirements of the MG Function, contains the management requirements for the MG function.

General requirements for the five management functional areas are defined in the following sections.

5.3.2.17.3.1 Fault Management

Fault Management supports the detection, isolation, and correction of abnormal operating conditions in a telecommunications network and its environment. Fault Management provides the functions to manage service problems, to support customer interactions associated with service troubles, and to support business policies related to service problems. Faults will be reported IAW IETF RFC 1215.

5.3.2.17.3.1.1 Alarm Messages

[Required: NM] Alarm messages must be distinguishable from administrative log messages.

5.3.2.17.3.1.2 Self-Detection of Fault Conditions

[Required: NM] The NEs shall detect their own fault (alarm) conditions.

5.3.2.17.3.1.3 Alarm Notifications

[Required: NM] The NEs shall generate alarm notifications.

5.3.2.17.3.1.4 Near-Real-Time Alarm Messages

[Required: NM] The network elements shall send the alarm messages in NRT. More than 99.95 percent of alarms shall be detected and reported in NRT. Near Real Time is defined as event detection and alarm reporting within 5 seconds of the event, excluding transport time.

5.3.2.17.3.1.5 SNMP Version 3 Format Alarm Messages

The network components shall send alarm messages in:

- **[Required: NM]** SNMPv3 format

This requirement does not apply to any legacy components of an MFSS or LSC. For the purpose of this requirement, “legacy” is defined as any TDM-based component that has been previously tested and listed on the APL. Alarm reporting requirements for these components are specified in UCR 2008, Section 5.2.

5.3.2.17.3.2 Configuration Management

Configuration Management (CM) exercises control over, identifies, collects data from, and provides data to NEs and the connections between NEs. Configuration Management is responsible for the planning and installation of NEs and their interconnection into a network. Configuration Management includes the establishment of customer services that use the network, all services and product planning, and business policy level functions related to service establishment.

[Objective: VVoIP NEs] All CM information shall be presented IAW RFCs 1213 and 3418.

Detailed CM support requirements of the CCA, SG, and MG functions are provided in separate sections, as follows:

- Section 5.3.2.18.3, Management Requirements of the CCA Function.
- Section 5.3.2.18.4, Management Requirements of the SG Function.
- Section 5.3.2.18.5 Management Requirements of the MG Function.

5.3.2.17.3.2.1 Read-Write Access to CM Data by the VVoIP EMS

[Required: NM] Capability to access and modify configuration data by the VVoIP EMS shall be controllable by using an access privileges function within the network appliance.

5.3.2.17.3.3 Accounting Management

Accounting Management enables the network service usage to be measured and the costs for such use to be determined. It provides facilities to collect accounting records and to set billing parameters for the usage of services and for access to the network. It also includes functionality to exercise control over the proper flow of funds within the enterprise and between the enterprise and its owners and creditors. Detailed requirements for Accounting Management, including requirements related to call quality, are found in UCR 2008, Section 5.3.2.19, Accounting Management.

5.3.2.17.3.4 Performance Management

Performance Management (PM) evaluates and reports the effectiveness with which the network and its NEs support assigned services. Performance Management provides mechanisms to measure service quality and provides the business policy functions for quality control.

[Objective: VVoIP NEs] All PM information shall be presented IAW RFCs 1213 and 3418.

Detailed requirements for PM interactions by the CCA, SG, and MG functions are provided in separate sections, as follows:

- Section 5.3.2.18.3, Management Requirements of the CCA Function
- Section 5.3.2.18.4, Management Requirements of the SG Function
- Section 5.3.2.18.5, Management Requirements of the MG Function

5.3.2.17.3.4.1 Near-Real-Time Network Performance Monitoring

Near-real-time network performance monitoring is a subset of PM. The VVoIP EMS collects alarm messages in real time and selected performance data from the NEs 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 NEs must be capable of receiving and responding to NM controls from the VVoIP EMS. The next section defines requirements for traffic flow (NM) controls.

5.3.2.17.3.4.2 Remote Network Management Commands

[Required: VVoIP NEs] The VVoIP NEs shall be able to receive and respond to remote NM commands. The commands are described in the following sections.

5.3.2.17.3.4.2.1 Comparison of Controls for Circuit-Switched and IP-Based Environments

The IP-based voice solution shall be able to exercise protective and expansive NM controls. (NOTE: Some controls used in the circuit-switched environment are not applicable in the IP-based voice environment because of the fundamental differences in how the two network environments operate.) The set of applicable IP-based traffic control capabilities and actions are outlined in the following paragraphs. The following descriptions and Table 5.3.2.17-1, Control Function Crosswalk: TDM to VVoIP, indicate which IP control actions (singularly and in combination), across the IP-based Voice solution, are necessary to mitigate or resolve the underlying situation for which each TDM equivalent control exists.

5.3.2.17.3.4.2.2 Automatic Congestion Controls

Within an IP network, the LSC handles only call signaling, while the IP network connecting the two communicating end instruments handles the bearer stream. The LSC congestion resulting from an overload of SIP requests must be detected and controlled. Bearer stream congestion will affect non-real-time as well as real-time bearer traffic, making it an IP NM concern. While good traffic engineering and the presence of an MPLS router core mitigates much of the traffic congestion within LAN and WAN environments, congestion at the boundaries between these domains is of concern and needs specific detection and control actions to mitigate the congestion.

The LSC congestion occurs when the volume of AS-SIP messages exceeds the LSC's capacity to process them. While a particular vendor's LSC solution may threshold and alarm on congestion, a simpler approach may be monitoring the Central Processing Unit (CPU) utilization on the LSC host. Alarms generated from CPU utilization threshold violations could be the trigger events necessary for the VVoIP EMS to take the appropriate pre-emptive policy-based management action to execute PEI/AEI destination controls, limiting other LSCs and their PEIs/AEIs from sending SIP (or proprietary protocol) messages to the overloaded LSC. From the viewpoint of these other LSCs, in effect, a code control would be executed on them.

Detection of network congestion at the edge of the LANs and WAN (DISN Core) resides with the performance management tools in place over those networks. These performance management tools must detect and report (via SNMP or syslog events) bandwidth utilization threshold violations in each of the CE Router, NIPRNet AR traffic queues. For the AR Routers, this must be by a southbound (CE connected) interface. From these events, each domain's policy-based management system must take the appropriate (precoordinated) control actions to mitigate the congestion.

Given no change in the physical resources (i.e., a larger bandwidth connection between the LAN and WAN), three basic actions can be taken to reduce congestion at the network edge:

1. Reallocate the queue bandwidth on the CE and PE Routers.

2. Change the call budget on the LSC, with a corresponding change in the VVoIP queue bandwidths on the CE and PE Routers.

3. Place a code control on other LSCs to reduce the load of SIP messages sent through the overloaded edge (although this would have minimal effect on reducing the bearer traffic, unless done in conjunction with a call budget and bandwidth change).

4. **[Required: LSC, MFSS, WAN 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 allowed to terminate naturally. This assumes that the CE Router queue bandwidths would not be reduced until the LSC session count fell below or equal to the newly commanded reduced budget, to prevent the corruption of existing sessions.

In summary, three control actions can help reduce congestion in the IP-based voice network: implementing EI destination controls, call budget changes, and router queue bandwidth allocations. Each control action is described in detail in the following paragraphs.

5.3.2.17.3.4.2.3 Selective Incoming Load Controls

Like Automatic Congestion Controls (ACCs), Selective Incoming Load Controls (SILCs) are designed to protect the switches and their connecting circuits from overload (congestion) conditions when CCS7 is not available to signal the overload condition to the connected switches.

Within the IP environment, the same two forms of congestion that apply to ACC are of concern: LSC processor congestion, and congestion across the LAN/WAN edge. The control solution that applies is similar to that of ACC.

While under SILC, LSC signaling of its congestion state to other LSCs cannot occur. Since LSC congestion can be detected and reported without SIP being involved, the alarms generated from CPU utilization threshold violations could be the trigger events necessary for the VVoIP EMS to take the appropriate policy-based management action to execute call destination controls (i.e., limiting other LSCs and their PEIs/AEIs from sending SIP (or proprietary protocol) messages to the overloaded LSC). From the viewpoint of these other LSCs, in effect, a code control would be executed on them. This does not mitigate a mass dialing event on base, where the PEI- or AEI-generated SIP (or proprietary protocol) messages would fill the base LSC’s messaging queue, awaiting processing. This makes its handling effectively the same as under ACC.

Congestion across the LAN/WAN edge is detected and handled the same way as under ACC.

5.3.2.17.3.4.2.4 Trunk Reservation

The primary intent of trunk reservation is to reserve resources for handling specific mission requirements, such as bonding of DS0-level channels to create bandwidth and reserving trunks for a video teleconference.

Reservation of resources in the IP environment is done by controlling the call budget for the class of traffic requiring the reserved resources at the LSC and its associated bandwidth on the LAN CE Router and DISN PE Router queues.

5.3.2.17.3.4.2.5 Precedence Access Threshold

Precedence Access Threshold (which is no longer a requirement in the TDM switch network) does not apply to IP traffic. The number of simultaneous precedence calls onto/off of the base will only be limited by the total call budget for that base.

5.3.2.17.3.4.2.6 Essential Service Protection

Essential Service Protection (ESP), which, in TDM, "guarantees" an EI will get dial tone, even in case of emergency or switch congestion, applies differently to VVoIP.

The PEI/AEI gets dial tone from itself, not the switch. The PEI/AEIs are not connected to the LSC, but to the ASLAN, that the LSC is also connected to. The first time the LSC knows a PEI/AEI is "off hook" is when a number is dialed and the SIP INVITE request (or other equivalent message) is sent to the LSC. In the VVoIP design, the LSC has no way of providing a priority queuing of SIP/proprietary messages from one PEI/AEI over another. The first time the LSC knows that a PEI/AEI needs service is when the SIP INVITE request (or other equivalent message) is taken from the LSC's signaling queue and processed. If that particular PEI/AEI has some service guarantee (over other EIs), then that EI really has an increased precedence over the others. (NOTE: UCR 2008, Section 5.2.2, Multilevel Precedence and Preemption, already covers EI precedence and preemption.) The LSC signals for the call IAW the Practices and Procedures (P&P) rules. Even if the PEI/AEI could somehow be tagged with an ESP tag, there would be no way of advertising it to the LSC in advance of the SIP INVITE request (or other equivalent message), thereby providing that guarantee, other than what is already provided through precedence and preemption. Because of this, ESP applies only to service restoral for selected IP users. If a PEI/AEI needs some level of call guaranteed service, then that PEI/AEI's precedence level needs to be elevated so the LSC can take the appropriate preemption activity when that EI requests service.

5.3.2.17.3.4.2.7 Destination Code Controls

The TDM code controls are manual protective controls that restrict calls having code prefixes for destinations that have been temporarily designated as difficult or impossible to reach.

[Required: LSC, MFSS, WAN SS] Within the IP environment, <u>Destination Code Control</u> functionality is applied at the LSC or MFSS to prevent or limit the number of calls (session requests) to reach a specific destination. Destination code controls are applied to reduce calls to a specific area or location that has been temporarily designated as "difficult to reach" due to several circumstances.

Within the DISN, call completion "difficulties" may include fixed or deployable situations for which a commander may want to minimize traffic to a given destination or set of destinations, such as a theater of operations. Given this, Minimize (currently a behavioral control to reduce traffic to a particular destination or region) initiated by a commander's order could be enforced using code controls, and set up to allow only precedence traffic to be passed to the minimized destination.

[Required] Destination Code Controls shall be implemented based on specifying:

- An entire Numbering Plan Area (NPA).
- A group of specific NNX codes within an NPA. (An example of when this control becomes necessary is when a large military base having multiple NNX codes becomes isolated.)
- A single NNX.
- An NNX-D (hundred group within an NNX. Reason: There are locations within CONUS that share an NNX.)

[Required] The LSC, MFSS, and WAN SS shall have the capability of setting the percentage of calls to be blocked to the designated destination(s).

[Required] FLASH and FLASH-OVERRIDE calls shall not be affected by NM controls.

5.3.2.17.3.4.2.8 SKIP, Cancel To, Cancel From

Within TDM, the protective controls Cancel From (CANF), Cancel To (CANT), and SKIP are those that block traffic from using a trunk group.

[Required] Within the IP environment, the analogous functionality is performed within the ASLAN to control traffic (VVoIP and non-VVoIP) flows onto and off the base. It presumes there are multiple paths off the base (redundancy) and an ASLAN-controlled load balancing or other traffic management capability to maintain appropriate control of all traffic flows. If, for tactical or technical reasons, one or more paths off the base cannot or should not be used, this is controlled within the base's NM and affects all traffic. Since it is applicable to all traffic traversing the ASLAN edge, not just VVoIP flows, it is not a voice-specific control.

5.3.2.17.3.4.2.9 Total Office Manual Control Removal

The ability to remove all controls that were put in place is equally applicable to TDM- and IP-based voice systems.

5.3.2.17.3.4.2.10 Directionalization

Directionalization is intended to control the relative volume of call initiation from on base to off base, or vice versa (i.e., control the sourcing direction). This requirement stems from the Chairman of the Joint Chiefs of Staff Instruction (CJCSI) 6215.01C, Appendix A.

[Required] Within IP, directionalization is controlled by designating all or part of the call budget as inbound (i.e., local destination) and/or outbound (i.e., local origination). The default is no designation (i.e., calls up to the total budget can be inbound or outbound in any combination). It does not change the total budget, only the sourcing direction of the budget; therefore, there is no impact to the router queue bandwidths.

5.3.2.17.3.4.2.11 Reroute (with All Subcontrols)

Within TDM, Reroute restricts offered calls from those routes known to be congested or failed, and provides substitute routes that have a higher probability of call completion.

[Required: MPLS] Within IP, the routing of all traffic (i.e., VVoIP and non-VVoIP) is handled via MPLS in the DISN core. The MPLS automatically finds the most effective route for the traffic.

5.3.2.17.3.4.2.12 IP Queue Control Capabilities

An important control unique to the IP-based environment is queue bandwidth allocations. The following requirements are for queue management:

1. Setting the queue bandwidth allocations on the CE Router and its connected port on the Aggregation Router involves setting the amount (or percentage) of bandwidth allocated to each of the (currently) four queues on the CE Router and connected PE Router. Two bandwidth allocation actions/functions can be performed as follows:

    a. **[Required: CE Router, AR]** Setting the bandwidth allocations by router queue, and

    b. **[Required: CE Router, AR]** Setting the drop probabilities within each queue if the router supports this functionality.

5.3.2.17.3.4.2.13 Call Budget Control

Setting the Call Budgets on the MFSS, WAN SS, and LSC involves setting the maximum number of calls (voice and video) that may be in service at one time within, and/or to/from a local service area (i.e., military installation).

Two call budget actions or functions can be performed: Setting the total call budget, and designating all or part of the call budget as inbound (local destination) and/or outbound (i.e., local origination) (to be able to implement an IP equivalent of directionalization). The default for the directionalization is no designation (i.e., calls can be inbound or outbound in any combination).

[Required: MFSS, WANS SS] The above defined call budget actions for the MFSS and WAN SS will be applied to the WAN-level ASAC. The WAN-level ASAC must be able to account for each subtended LSC under its control. Therefore, the MFSS and WAN SS ASAC must be able to set call budgets for multiple LSC locations via the VVoIP EMS and local EMS access points.

[Required: LSC] The above defined call budget actions for the LSC will be applied to the LSC-level ASAC. The LSC-level ASAC is required to only account for itself. Therefore, the LSC ASAC must be able to set call budgets for only the PEI/AEIs under its control via the VVoIP EMS and local EMS access points.

The MFSS and WAN SS WAN-level ASAC and the LSC-level ASAC session budgets and counts area as follows:

- VoIP Session Budgets
  - IPB. The total budget of VoIP sessions plus session attempts in the session setup phase that are allowed on the IP access link.
  - IPBo. The budget for outbound VoIP sessions plus session attempts in the session setup phase that are allowed on the IP access link.
  - IPBi. The budget for inbound VoIP sessions plus session attempts in the session setup phase that are allowed on the IP access link.
- TDM Session Budget
  - 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 LSC MG and the EO/SMEO/PBX1/PBX2.
- VSU Budgets
  - VDB. The total number of inbound and outbound VSUs plus the in-progress VSUs connection attempts that an LSC is allowed to have over the IP access link.

- VDBi. The total number of inbound VSUs plus the in-progress inbound VSUs connection attempts that an LSC is allowed to have over the IP access link.

- VDBo. The total number of outbound VSUs plus the in-progress outbound VSUs connection attempts that an LSC is allowed to have over the IP access link.

5.3.2.17.3.4.2.14 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.

[Required: LSC] 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 LSC system administrator.

[Required LSC] 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 LSC system administrator. This action or function can be performed by:

1. **[Required]** Setting the destinations to which calls are to be blocked by:

   a. **[Required]** NPA/NNX
   b. **[Conditional]** Blocked by a specific 7-digit directory number (NPA-NNX Dxxx)

Table 5.3.2.17-1, Control Function Crosswalk: TDM to IP VVoIP, summarizes the traffic flow controls that will be implemented in the IP environment along with the equivalent TDM-based controls.

5.3.2.17.3.5 Security Management

Security management provides for prevention and detection of improper use or disruption of network resources and services, for the containment of and recovery from theft of services or other breaches of security, and for security administration.
The VVoIP EMS is required to use the security services of access control, confidentiality, integrity, availability, and non-repudiation as specified in UCR 2008, Section 5.4, Information Assurance Requirements.

[Required] All management interactions shall meet the Information Assurance requirements in Section 5.4, Information Assurance Requirements.

Table 5.3.2.17-1. Control Function Crosswalk: TDM to VVoIP

	IP REAL TIME SERVICES CONTROL FUNCTIONS			
	ROUTER FUNCTION	LSC FUNCTIONS		
Existing TDM Control	CE BW Allocation	ASAC Budget	EI Origination	EI Destination
ACC	**X (bearer stream only)**	**X (bearer stream only)**		**X (from other LSCs/EIs – like Code Controls)**
SILC	**X (bearer stream only)**	**X (bearer stream only)**		
Trunk Reservation	**X**	**X**		
Precedence Access Threshold	**N/A to VVoIP**			
ESP	**N/A to VVoIP**			
Code Controls				**X**
CANT	**Applicable to all ASLAN edge traffic – Handled via base router management**			
CANF	**Applicable to all ASLAN edge traffic – Handled via base router management**			
SKIP	**Applicable to all ASLAN edge traffic – Handled via base router management**			
Total Office Manual Control Removal	**X**	**X**	**X**	**X**
Directionalization		**X**		
Reroute	**N/A to VVoIP – Handled via MPLS Functionality in DISN Core**			
Single via Reroute	**N/A to VVoIP – Handled via MPLS Functionality in DISN Core**			
Multiple via Reroute	**N/A to VVoIP – Handled via MPLS Functionality in DISN Core**			
Overflow vs. Immediate Reroute	**N/A to VVoIP – Handled via MPLS Functionality in DISN Core**			

LEGEND

ACC	Automatic Congestion Controls	CE	Customer Edge Router	MPLS	Multiprotocol Label Switching
ASAC	Assured Service Admission Control	DISN	Defense Information Systems Network	N/A	Not Applicable
ASLAN	Assured Service Local Area Network	EI	End Instrument	VVoIP	Voice and Video over IP
BW	Bandwidth	ESP	Essential Service Protection	SILC	Selective Incoming Load Control
CANF	Cancel From	IP	Internet Protocol		
CANT	Cancel To	LSC	Local Session Controller	TDM	Time Division Multiplexing

5.3.2.17.4 Data Classification

This section defines the data types provided by network appliances. The data types can be classified as generated data and parametric data. In addition, data that indicates the condition or state of an appliance is defined as representing operational, usage, and administrative states. In addition to these states, a network appliance uses more descriptive status values. Although the data types defined within each category may overlap, they reflect the type of information conveyed by the data, and the urgency with which the data must be presented to the user. These lists are not exhaustive, but cover the most frequently used measurement types and capabilities.

5.3.2.17.4.1 Parametric Data

Parametric data refers to the data that reside in a network appliance and defines its functional mode and its physical resources. Parametric data is composed of criteria data and reference data. Reference data describes the topology, capacity, routing patterns, and other attributes of the components (i.e., switching network appliances, traffic links) that make up a network.

Reference data values do not change as frequently as counts and state indicators and, thus, are relatively static. When reference data values change, the network appliance should notify the appropriate management application. It is desirable for the changed reference data to be sent to the appropriate application when the change occurs. It is acceptable, however, for a state indication to be sent instead alerting the application to the change; this will then cause the application to initiate a request for the changed reference data. In either case, only the reference data that has actually changed should be sent.

Criteria data (also called instruction data) consists of the parameter settings available within the network appliance that govern the various application support functions of the network appliance. This includes, but is not limited to, such parameters as data filters, thresholds, collection schedules, and report generation criteria. The specific parameters may vary across the applications supporting a network appliance. These parameters may be set or modified by the individual supporting applications. Therefore, the network appliance should allow the management system to view and alter these parameters as necessary.

5.3.2.17.4.2 Generated Data

Generated data refers to the data recorded or collected by the NE concerning the traffic it is carrying. This includes traffic counts, data about the use of the NE resources, and noted exceptions. The three data types defined as generated data are event counts, usage counts, and state indications. Counts are cumulative measurements driven by event occurrences. Two types of counts are those based on distinct event occurrences and those based on usage.

5.3.2.17.4.3 Entity States

Access to state information in network appliances provides the current operational, usage, or administrative state of a resource, together with supporting status information.
The following state definitions are from ITU-T Recommendation X.731.

5.3.2.17.4.3.1 Operational State

Two valid Operational states are enabled and disabled.

1. Enabled. The resource is partially or fully operable and ready for use.

2. Disabled. The resource is totally inoperable and unable to provide service to users.

Generally, Operational states may only be set by the network appliance that houses the resource, and are used to indicate that the resource is experiencing trouble that is impairing functionality.

5.3.2.17.4.3.2 Usage State

Three valid Usage states are idle, active, and busy.

1. Idle. The resource is not currently in use.

2. Active. A sharable resource has one or more users and has the ability to serve new users.

3. Busy. A non-sharable resource has a user or a sharable user is occupied to capacity with request for use.

Generally, Usage states are only able to be set by the network appliance housing the resource whose state is being monitored.

5.3.2.17.4.3.3 Administrative State

Three valid Administrative states are unlocked, shutting down, and locked.

1. Unlocked. The resource is permitted to perform services for users.

2. Shutting down. Use of the resource is allowed to existing users only, and no new users are allowed. After a period, use of the resource to existing users may be terminated.

3. Locked. The resource is administratively prohibited from performing services for its users.

In general, the Administrative state may be set by the VVoIP EMS, Craft Interface, or the network appliance whose resources are being monitored. Administrative states are used to shut down and restart network appliances or bootable components of the network appliance.

5.3.2.17.4.3.4 Status

In addition to the generic states mentioned earlier, the network appliance uses more descriptive status values. An example is Service status.

Applicable values for Service status are as follows:

1. Test. The resource is no longer available for user traffic, as tests are scheduled for this resource.

2. In-service. Use of the resource is allowed.

3. Out-of-service. The resource has been made unavailable for use.

The Service status may be set by the VVoIP EMS, or Craft Interface, and is used to indicate that tests are being conducted on the resource, or the resource is otherwise out of service.

5.3.2.17.5 Management of Appliance Software

Software management must be able to satisfy the following objectives, subject to possible imposed controls and conditions:

1. Request delivery of software to a specific managed system.

2. Control the installation of software on a managed system, including the installation of patches (e.g., upgrades), and control the rollback to a previous version of the software.

3. Initiate the execution of a software program.

4. Request the attributes of the software held on a managed system.

5. Create and delete software held on a managed system.

6. Validate software held on a managed system to check its integrity and to terminate validation.

7. Restrict use of software on a managed system for administrative purposes.

8. Back up software and restore software to a previously backed up version.

In all cases, the success or failure of the operation needs to be reported to the managing system.

Software management may use logging, accounting, auditing, and license management at each state of this process.

5.3.2.17.5.1 Management of Software Generics

In this document, a software generic is defined as a non-site-specific software release for a network appliance that encompasses executable instructions, utilities, routines, and application programs. It does not include specific data, such as site-specific equipment configuration and operational parameters.

The management information associated with software generics contains user-settable attributes as well as a pointer to the software generic itself. The management information attributes are entered and edited by users with appropriate user privilege.

The required software management information includes the following:

- Identities of all the network appliances that used the software modules
- Software generic supplier name
- Version number or release number of the software
- Date and time when the software was received from the supplier
- When the last update was made to the software generic
- A program executability attribute that represents the state of the software generic
- A program accessibility attribute that governs the security access to the software generic

[Required] A network appliance shall maintain management information associated with the software generics it is holding, including the following elements:

- Software generic ID (e.g., supplier name, software type, version number, date of last update)
- Program size
- Location

- Program executability
- Program accessibility (e.g., privilege codes)
- Date and time loaded.

The Location attribute can be thought of as the pointer (e.g., file system path) to the software generic.

The program Accessibility attributes specify the management systems, personnel, and other programs that may invoke the execution of the software generic.

The software generic ID uniquely identifies a software generic within the network appliance. The version of a software generic (e.g., new software generic, software update, software patch) labels the software generic release and its subsequent software updates and software patch releases so they can be unambiguously identified and related. The labeling scheme for software and for documentation should be the same for each type of software generic.

The program Executability attribute is used to indicate that a program is available for invocation and execution; is in a testing state; is unavailable for invocation or execution; and does not exist currently in a network appliance file store.

5.3.2.17.5.2 Software Installation

Initially when software is installed, it may be necessary to have technicians present onsite to monitor and control the installation. Therefore, a network appliance is required to support on-site installation of software generics. When this method is used, the network appliance shall inform the management operating system that the installation has taken place. Typically, only the first software generic is installed onsite. Future releases are downloaded from a remote location under the direction of a management system.

[Required] A network appliance shall provide functionality to support the on-site installation of software generics, using portable storage media, with control of the installation process accessible over a local CID.

[Required] A network appliance shall be capable of accepting remote downloads of software generics.

[Required] The network appliance verifies any new software generic to ensure that the new software generic was loaded error free.

[Required] In response to a request, a network appliance shall report the management information associated with all loaded software generics.

[Required] A network appliance shall autonomously inform a managing system of the status of its software download activities.

[Objective] The network appliance should activate a new software generic load upon receiving a request to do so from a managing system.

[Objective] The software generic should be automatically activated on the network appliance after the correctness of it has been verified. This activation may occur immediately or at a predefined time.

[Objective] If a new software generic fails to activate, a network appliance shall back out of the software generic, re-establish its previous software generic, and indicate the reason for the back-out.

[Required] The process of loading software generics, including updates and patches, in a network appliance shall cause no disruption to the Appliance’s functionality, or alter any existing option settings or configuration data.

5.3.2.17.5.2.1 Data Backup and Recovery

[Required] Programs, including application software and protocol software, and the corresponding software generic management information, shall be subject to the backup and recovery requirements.

5.3.2.17.5.2.2 Service Impacts

An established (stable) call is a call that is in the connected state (i.e., voice, video, or data is being transmitted), and no transient call activity is being initiated. A transient call is a call that is in a state of potential change.

[Required] During a software cutover, the network appliance shall preserve all stable calls.

[Objective] The software cutover process shall limit the duration of effects on transient calls for any size switching network appliance to less than 1 minute.

5.3.2.17.5.2.3 Databases/Directories

A network appliance may contain a Database Manager for its Management Information Base (MIB).

Occasionally, the data associated with the newly loaded software generic will be sufficiently different from that of the older software generic that the Database Manager will have to restructure the MIB. General database reconfiguration generic requirements are discussed in Telcordia Technologies GR-2932-CORE.

[Required] In the case where a newly loaded software generic requires restructuring of MIB data, a mechanized method shall be provided for reconfiguring the MIB from the older software generic configuration database to a structure that is compatible with the new software generic.

5.3.2.18 Network Management Requirements of Appliance Functions

5.3.2.18.1 **[Required: CE Router, EBC]** The NM requirements for the various functions of the CE Router and EBC are contained in this section.

[Required: CE Router, EBC] Faults will be reported IAW RFCs 1215 and 3418.

[Required: CE Router, EBC] Standard CM information shall be presented IAW RFCs 1213 and 3418.

[Required: CE Router, EBC] Standard PM information shall be presented IAW RFCs 1213 and 3418.

[Objective: CE Router, EBC] Nonstandard (vendor-specific) CM and PM information shall be presented as private vendor MIBs, as defined by the applicable RFCs.

[Required: NM] SNMPv3 format.

5.3.2.18.1.1 **[Required: CE Router]** The CE Router QOS queues must be readable and settable by the VVoIP EMS.

5.3.2.18.1.2 **[Required: CE Router, EBC]** The standard CM MIB variables shown in Table 5.3.2.18-1, Standard CM MIB Variables, are required for each CE Router and EBC.

Table 5.3.2.18-1. Standard CM MIB Variables

CM MIB VARIABLE	MIB DESCRIPTION
sysDescr	The textual description of the entity. This value should include the full name and version identification of the system's hardware type, software operating system, and networking software.
sysLocation	The physical location of this node (e.g., "lab, 3rd floor"). If the location is unknown, this value is a zero-length string.
sysName	The name by the administrator for this managed node. By convention, this is the node's fully-qualified domain name. If the name is unknown, this value is a zero-length string.
sysContact	A textual string containing contact information.
ifDescr	A textual string containing information about the interface. This string should include the names of the product and manufacturer, and the version of the interface hardware/software.
ifIndex	A unique value for each interface in the range 1 to ifNumber. The value for each interface must remain constant at least from one reinitialization of the entity's NMS to the next reinitialization.
ifSpeed	An estimate of the interface's current BW, b/s. For interfaces that do not vary in BW (or those that cannot be estimated accurately), this metric contains the nominal BW nvmSpeedOctets (ifSpeed/8).
ifType	An enumerated type that specifies the interface type.
ifPhysAddress	The interface's address at its protocol sublayer. For example, for an 802.x interface, this object normally contains a MAC address. The interface's media-specific MIB must define the bit and byte ordering and the format of the value of this object.
ifAdminStatus	An enumerated type that specifies the state of the interface. The possible values are 1) v up, the interface is up; and 2) v down, the interface is down. When a managed interface initializes, all interfaces start with a down state: v testing, the int.
sysUpTime	The time (in hundredths of a second) since the NM portion of the system was last reinitialized.
ifOperStatus	An enumerated type that specifies the current operational state of the interface. The possible values are 1) v up, the interface is up; and 2) v down. If ifAdminStatus is down, this metric will also be down. When the value of ifAdminStatus changes, the value if this metric will also change. v testing — The interface is in a testing state; no operational packets can be sent. v unknown — The interface state is unknown. v dormant — The interface is dormant. v notPresent — The interface is not present. v lowerLayerDown — The lower layer of the interface is down.

5.3.2.18.1.3 **[Required: CE Router, EBC]** The standard PM MIB variables shown in Table 5.3.2.18-2, Standard PM MIB Variables, are required for each CE Router and EBC per interface.

Table 5.3.2.18-2. Standard PM MIB Variables

PM MIB VARIABLE	MIB DESCRIPTION
ifInErrors	For packet-oriented interfaces, this is the number of inbound packets that contains errors that prevent them from being deliverable to a higher layer protocol. For character-oriented or fixed-length interfaces, this is the number of inbound transmissions.
ifLastChange	The value of sysUpTime when the interface entered its current operational state. If the current state was entered before the last reinitialization of the local NM subsystem, this metric is zero.
ifMtu	The size, in octets, of the largest packet that can be sent or received on the interface. For interfaces that are used for transmitting network datagrams, this is the size of the largest network datagram that can be sent on the interface.
ifInNUcastPkts	The number of packets delivered by this sublayer to a higher layer that was addressed to a multicast or broadcast address at this sublayer.
ifInUcastPkts	The number of packets delivered by this sublayer to a higher layer that was not addressed to a multicast or broadcast address at this sublayer.
ifInUnknownProtos	For packet-oriented interfaces, this is the number of packets received via the interface that were discarded because of an unknown or unsupported protocol.
ifOutDiscards	The number of outbound packets discarded even though no errors had been detected to prevent their being transmitted.
ifOutErrors	For packet-oriented interfaces, this is the number of outbound packets that could not be transmitted because of errors. For character-oriented or fixed-length interfaces, this is the number of outbound transmission units that could not be transmitted because of errors.
ifOutNUcastPkts	The total number of packets that higher level protocols requested to be transmitted that was addressed to a multicast or broadcast address at this sublayer, including those that were discarded or not sent.
ifOutUcastPkts	The total number of packets that higher level protocols requested to be transmitted that was not addressed to a multicast or broadcast address at this sublayer, including those that were discarded or not sent.
ipForwarding	Specifies whether the entity is acting as an IP router by forwarding datagrams received by, but not addressed to, this entity. IP routers forward datagrams, whereas IP hosts do not (except for those datagrams source-routed via the host).
ipForwDatagrams	The number of input datagrams forwarded to their final IP destination (this entity was not the final destination).
ipInAddrErrors	The number of input datagrams discarded because the IP address in their IP header’s destination field was not valid. This count includes both incorrect addresses and addresses of unsupported classes.
ipInDelivers	The total number of input datagrams successfully delivered to IP user-protocols (including Internet Control Message Protocol (ICMP)).
ipInDiscards	The number of input IP datagrams for which no problem was encountered to prevent their continued processing, but that were discarded (example.g., because of lack of buffer space).

PM MIB VARIABLE	MIB DESCRIPTION
ipInHdrErrors	The number of input datagrams discarded due to errors in their IP headers. The errors might include bad checksums, version number mismatch, other format errors, time-to-live exceeded, errors discovered in processing their IP options, and so on.
ipInReceives	The total number of input datagrams received from interfaces, including those received in error.
ipInUnknownProtos	The number of locally addressed datagrams received successfully, but discarded because of an unknown or unsupported protocol.
ipOutDiscards	The number of output IP datagrams for which no problem was encountered to prevent transmission to their destination, but that were discarded (example.g., because of lack of buffer space).
ipOutNoRoutes	The number of IP datagrams discarded because no route could be found to transmit them to their destination.
ipOutRequests	The total number of IP datagrams that local IP user protocols (including ICMP) supplied to IP in requests for transmission.

5.3.2.18.1.4 **[Required: CE Router, EBC]** The standard TRAPs shown in Table 5.3.2.18-3, Standard TRAPs Required for CE Router and EBC, are required for each CE Router and EBC.

Table 5.3.2.18-3. Standard TRAPs Required for CE Router and EBC

TRAP NAME	ENTERPRISE ID
ColdStart	1.3.6.6.3.1.1.5.1
WarmStart	1.3.6.6.3.1.1.5.2
LinkDown	1.3.6.6.3.1.1.5.3
LinkUp	1.3.6.6.3.1.1.5.4
Authentication Failure	1.3.6.6.3.1.1.5.5

[Required: LSC, MFSS, WAN SS] The NM requirements for the various functions of the LSC, the softswitch part of the MFSS, and the WAN SS are contained in this section. Requirements are defined for the following functions:

- ASAC function
- CCA function
- SG function
- MG function

5.3.2.18.2 Management Requirements for the ASAC

The MFSS, WAN SS, and LSC-ASAC must permit the reading of the following counts from the VVoIP EMS:

- VoIP Session Counts

  – IPC. The total number of interbase IP sessions in progress plus the number of session attempts in the session setup phase.

  – IPCo. The number of outbound IP sessions in progress plus the number of outbound session attempts in the session setup phase.

  – IPCi. The number of inbound IP sessions in progress plus the number of inbound session attempts in the session setup phase.

- TDM Session Counts

  – 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.

- VSU Counts

  – VBC. The total number of interbase VSU sessions in progress plus the number of session attempts in the session setup phase.

  – VBCo. The number of outbound VSU sessions in progress plus the number of outbound session attempts in the session setup phase.

  – VBCi. The number of inbound VSU sessions in progress plus the number of inbound session attempts in the session setup phase.

[Required] The ASAC must provide the separate counts for voice and video, in 5-minute intervals. The MFSS and WAN SS ASAC must provide these counts for each of the subtended LSCs under its control, while the LSC is only to provide these counts for the PEIs/AEIs that it controls. The ASAC reporting parameters are shown in Table 5.3.2.18-4, ASAC Reporting Parameters.

Table 5.3.2.18-4. ASAC Reporting Parameters

ASAC Reporting Parameters
Current Inbound Session Rate in CPS (Calls Per Second)
Current Active Outbound Sessions
Current Outbound Session Rate in CPS
Total Inbound Sessions
Total Inbound Sessions Rejected due to Insufficient Bandwidth
Highest Concurrent Inbound Sessions
Average Rate Inbound Sessions in CPS
Total Outbound Sessions
Total Outbound Sessions Rejected due to Insufficient Bandwidth
Highest Concurrent Outbound Sessions
Average Rate Outbound Sessions
Maximum Burst Rate of Inbound/Outbound Traffic
Total Seizures
Total Answered Sessions
Answer-to-Seizure Ratio Percentage
Average One-Way Signaling Latency (ms) (Time Period)
Maximum One-Way Signaling Latency (Time Period)
Max Burst Rate (in and out) (CPS)

5.3.2.18.3 Management Requirements of the CCA Function

A complete description of the CCA function is provided in the Section 5.3.2.9, Call Connection Agent.

5.3.2.18.3.1 CCA Support for Configuration Management

This section addresses CM under the following three topics:

- Capacity installation
- Service activation
- Status and control

5.3.2.18.3.1.1 CCA Support for Capacity Installation

Capacity installation supports the placement of equipment in the network. This includes the extension or reduction of resources, loading software, and coordination of changes.

The CCA needs to be able to access configuration data that it maintains about itself and other network appliances.

[Required] A switching network appliance shall acquire, activate, and manage a CCA software download as directed by the Local EMS. The CCA software may be managed on a per CCA hardware component basis.

NOTE: The CCA software is managed as a software generic described in the Section 5.3.2.9, Call Connection Agent.

The CCA is provisioned with a CCA Identification parameter that uniquely identifies the CCA to the Billing Agent. See Section 5.3.2.19, Accounting Management, for the accounting requirements. The CCA is provisioned with a Recording Office Identification parameter that uniquely identifies the billing agent to the CCA.

[Required] The CCA shall be able to manage the following parameters in the CCA from the VVoIP EMS:

- CCA Identification parameter
- Recording Office Identification parameter

5.3.2.18.3.1.1.1 MG-Related Configuration

This section specifies the data needed by the CCA to support access lines. This data is organized into the data the CCA needs to communicate with the MG, voice-grade analog line-specific data, ISDN-related data, trunk-related data, and trunk circuit-related information.

[Required] The CCA shall manage the IP address of an MG from the VVoIP EMS upon installation or removal of an MG or associated trunk equipment.

[Required] The CCA shall manage configuration data supporting voice-grade analog lines upon installation of CCA or MG access equipment.

[Required] The CCA shall support provisioning of MG ISDN interface resources.

[Required] The CCA shall be capable of managing trunk-related provisioning information for associated MGs.

[Required] The CCA shall be capable of managing provisioning information related to trunk circuits associated with its assigned MGs.

5.3.2.18.3.1.1.2 SG-Related Data

[Required] The CCA shall manage configuration information for the set of SGs associated with the CCA.

5.3.2.18.3.2 CCA Support for Service Activation

Service activation focuses on the interactions with, and functional requirements of, the CCA to activate, modify, and discontinue services based on customer or traffic demands.

[Required] The CCA shall manage the activation and deactivation of service features.

[Required] The CCA shall maintain data for the media server and UFS functions it interacts with.

[Objective] Activation of a new service feature shall not cause the CCA to disrupt customer services or operations support.

The CCA needs to be able to restore its configuration database to the last validated stable condition in the case of corruption of configuration data.

[Required] The CCA shall be able to create a backup and manage restoration of configuration data by placing its stable data and changes to the latest configuration in a nonvolatile storage device.

5.3.2.18.3.3 CCA Support for Fault Localization

It is the responsibility of fault localization to determine the root cause of a fault. Fault localization may need to acquire data or perform tests to determine the root cause.

Generic maintenance requirements for trouble isolation in switching systems are found in Telcordia Technologies GR-474-CORE. These requirements shall apply to a CCA.

[Required] A CCA shall meet all applicable Operations Technology Generic Requirements (OTGR) for switching system NE trouble isolation in Telcordia Technologies GR-474-CORE.

[Required] A CCA shall perform root-cause analysis for any faults within its purview, report the root cause, and suppress the reporting of non-root-cause conditions.

The preceding requirement implies that if a single fault or abnormality results in the impairment of multiple generic functions, the CCA shall generate a single alarm message that reports the fault or abnormality and that identifies all such impaired functions.

5.3.2.18.3.4 CCA Support for Testing

Testing is concerned with the testing of connections directly related to customer services or with transmission facilities and the related resources within affected functional elements. Testing is performed for acceptance of newly provisioned connections, new installation of physical facilities or network appliances, validating trouble reports, providing additional information to fault localization, or to verify a network repair.

[Required] A CCA shall support the ability to perform internal diagnostics on its call processing functionality and internal resources, initiated either locally or upon request by the VVoIP EMS.

5.3.2.18.3.5 CCA Support for Performance Management

Performance management criteria are used to evaluate and report on the behavior and effectiveness of the CCA, as well as the physical and logical entities it supports. Performance management includes gathering and analyzing statistical data for both performance monitoring (for network maintenance) and Network Traffic Management purposes.

Performance monitoring provides non-intrusive collection, analysis, and reporting of network performance information and traffic statistics. This data is used to assess and maintain the network as well as to document the quality of service to customers. Indications of service-affecting degradation are forwarded to Fault Management applications.

5.3.2.18.3.5.1 The MG-MGC Protocol and Traffic Monitoring

Protocol and traffic monitoring requirements shall apply to the Gateway Control interface. This interface refers to the control interface between the CCA's internal MGC function and an MG.

NOTE: The MG-MGC protocol may be H.248 or may be a priority protocol. The specific protocol to be used is a supplier/vendor decision.

The terminology used in this section for describing the communication between a CCA and an MG is briefly reviewed in the next paragraph.

A Command provides the ability to manipulate the logical entities of the protocol connection model. Examples are an Add Command that adds a Termination to a Context, or a Subtract Command that removes a Termination from a Context. Commands between the CCA and an MG are grouped into Transactions. Transactions consist of one or more Actions. An Action consists of a series of Commands that are limited to operating within a single Context. In addition, multiple Transactions can be concatenated into a Message.

Traffic counts will only be performed on Commands and Transactions.

[Required] The CCA shall provide counters for the following on each MG interface supporting the MG-MGC protocol:

- Number of requests sent
- Number of responses received
- Number of retransmits
- Number of received error conditions
- Number of service-changed commands
- Count of termination ID-related errors
- Count of context-related errors
- Count of descriptor-related errors
- Count of action-related errors
- Count of package-related errors
- Count of transaction-related errors
- Count of command-related errors
- Count of digit map-related errors
- Count of gateway-related errors

[Required] The CCA shall count each of the following specific command error codes on interfaces supporting the MG-MGC protocol. (Thresholds on these counts shall be set on a per-interface basis.)

- Bad Request
- Protocol Errors
- Unauthorized
- Insufficient Resources
- Not Implemented
- Not Ready
- Service Unavailable
- Insufficient Bandwidth
- Internal Hardware Failure

[Required] The CCA shall log information on a service change command each time it generates this Command. The log for a service change shall contain the following information:

- Service change reason

- Service change method

- Date and time of service change. The time shall be accurate to within 1 second, with respect to the CCA’s local clock.

5.3.2.18.3.5.2 Call-Related Performance Monitoring

The CCA needs to monitor internal call-related procedures, as well as performance associated with call processing.

[Required] The CCA shall provide a counter for each of the following to support monitoring of call processing:

1. No responses. The CCA fails to receive a response to a request or message that requires a response.

2. Incorrect messages. The CCA receives a message that cannot be understood or does not permit a valid response to be formed and sent to a specific MG.

3. Invalid messages. The CCA receives a transaction request or message that is invalid or cannot be successfully acted upon, but for which a valid response can be directed to the transmitting MG.

4. Sending error messages. The CCA receives a number of responses with error codes indicating a malformed request or message that suggests a problem in the CCA or in the sending entity.

[Required] The CCA shall provide basic switch-related traffic measurements as specified in Telcordia Technologies GR-477-CORE, Section 4.1.1. In particular, the CCA shall support the following GR-477-CORE requirements:

- Telcordia Technologies GR-477-CORE measurements related to CCA processor performance:

  – Call processing capacity

- Telcordia Technologies GR-477-CORE call direction measurements:

  – Total originating calls
  – Originating line to terminating line calls
  – Originating line to outgoing trunk calls
  – Total incoming calls
  – Incoming trunk to terminating line calls
  – Incoming trunk to outgoing trunk calls

- Telcordia Technologies GR-477-CORE basic failure to match and no circuit measurements:

  - Originating to terminating matching loss
  - Originating to outgoing matching loss
  - Incoming to terminating matching loss
  - Incoming to outgoing matching loss
  - Originating to outgoing calls encountering No Circuit (NC)
  - Incoming to outgoing calls encountering NC
  - Originating to terminating calls to line busy
  - Incoming to termination call to line busy

- Telcordia Technologies GR-477-CORE additional ineffective machine attempt measurements:

  - Final handling overflows
  - Incoming trunk permanent signaling time-outs
  - Outgoing trunk start signaling time-out
  - Miscellaneous equipment-related ineffective machine attempts
  - Vacant code treatments

[Required] The CCA shall provide trunk group-related traffic measurements as specified in Telcordia Technologies GR-477-CORE, Section 4.1.3. In particular, the CCA shall support the absolute requirement of GR-477-CORE, providing basic trunk group measurements, including the following:

- Access attempts for trunk group
- Overflow for trunk group
- Total usage for trunk group
- Incoming attempts for trunk group

[Required] For all calls originating at a CCA, the CCA shall monitor call set-up delay statistics, including delay incurred as part of the set-up of the core network bearer connection.

5.3.2.18.4 Management Requirements of the SG Function

The requirements identified in this section are **[Conditional: MFSS, LSC],** since an SG is also conditional.

The SG interacts with the Management function by doing the following:

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

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

3. Sending information to the Management function on a periodic basis (e.g., on a set schedule), and keeping the Management function up-to-date on SG activity. An example of this update would be a periodic transfer of audit reports from the SG to the Management function so that the Management function could either store the report locally, or transfer it to a remote NMS for remote storage and processing.

A complete description of the SG is provided in Section 5.3.2.13, Signaling Gateway Requirements.

5.3.2.18.4.1 SG Support for CM

This section addresses CM under the following topics:

- Identifiers
- Protocol Management – CCS7 Layers
- Status Monitoring

5.3.2.18.4.1.1 Identifiers

[Conditional] The SG shall allow the VVoIP EMS to configure the set of adjacent and remote CCS7 destinations in the CCS network. For each CCS7 destination, the SG shall allow the VVoIP EMS to configure the CCS7 destination address.

[Conditional] The SG shall allow the VVoIP EMS to configure its unique CCS7 primary SPC, in terms of the decimal equivalents of its Network Identifier, Network Cluster, and Network Cluster Member (NCM) codes.

5.3.2.18.4.1.2 Protocol Management – CCS7 Layers

The SG is required to support the provisioning via the VVoIP EMS of various resources associated with the SG's CCS7 network interfaces. Requirements are presented for the various types of CCS7 resources or functional parameter profiles.

5.3.2.18.4.1.2.1 CCS7 Link Interface Equipment Ports

[Conditional] The SG shall maintain the following management information for each configured CCS7 link interface equipment port:

- Link equipment port identifier
- Port equipment options/settings

5.3.2.18.4.1.2.2 CCS7 Link Sets

[Conditional] The SG shall allow the VVoIP EMS to configure its CCS7 link set terminations, including the specification of the following link set attributes:

- Network link set identifier
- Far-end point code
- Far-end node identifier
- Local link set identifier (optional)

5.3.2.18.4.1.2.3 CCS7 Signaling Routes

The configured link sets are to be regarded as the “signaling routes” to the CCS7 configured destinations. As two A-link link sets are assumed for the initial SG implementations, there are no requirements for the explicit provisioning of ordered (primary and alternate or loadshared) signaling routes to each CCS7 destination address. Equal loadsharing via the SLS code mechanism is implied for outbound signaling traffic distributed over the links in the configured A-link sets.

5.3.2.18.4.1.2.4 CCS7 Links

[Conditional] The SG shall allow the VVoIP EMS to configure its CCS7 link terminations, including the creation of member links within link sets and their assignment to CCS7 link equipment ports, along with the specification of the following link attributes:

- Network link set identifier
- Link member number/signaling link code (SLC)
- Link equipment port identifier
- Associated CCS7 MTP-Level 2 timer profile (optional)
- Associated CCS7 MTP link transmit congestion thresholds profile

Up to 16 links per link set are allowed by the size of the SLC and SLS codes used for A-link sets.

5.3.2.18.4.1.2.5 CCS7 MTP Level 2 Timer Profiles

[Conditional] The SG shall provide default values and allow the VVoIP EMS to configure one or more Level-2 parameter profiles described in T1.111.3 (i.e., T1, T2, T3, T4n, T4e, T5, T6, T7), each assignable to individual MTP2-based signaling links.

5.3.2.18.4.1.2.6 CCS7 MTP Link Transmit Congestion Threshold Profiles

[Conditional] The SG shall provide default values and allow the VVoIP EMS to configure one or more congestion-threshold parameter profiles (i.e., Level 1, Level 2, and Level 3), each assignable to individual MTP2-based signaling links.

The default values and configurable ranges for the CCS7 link transmit congestion thresholds should be selected by the SG supplier to maximize link throughput and minimize expected link output delays, subject to capacity and design constraints of the implementation's signaling message-handling process and the capacity of its transmit and retransmit buffers. The latter constraints are implementation-specific considerations.

5.3.2.18.4.1.2.7 CCS7 MTP3 Timer Profile

[Conditional] The SG shall provide default values and allow the IP network to configure a profile of MTP3 timer values to be used by the SG in its interactions across all CCS7 signaling links. The profile shall contain values of the parameters described in T1.111.4 (i.e., timers T1, T2, T3, T4, T5, T6, T10, T12, T13, T14, T15, T16, T17, T19, T20, T21, T22, T23, T26, T27, T28, T29, T31) and T1.111.7 (i.e., timers T1, T2), changeable on a per-node (per-SG) basis.

[Conditional] The SG shall support configurable ranges for the CCS7 MTP3 timers as specified in Telcordia Technologies GR-246-CORE, Table 4-2, Provisional Values for Signaling Link Test Timers, and Table 4-3, Provisional Values for MTP Level 3 Timers.

5.3.2.18.4.1.2.8 CCS7 Provisioning Operations

[Conditional] The SG shall support provisioning of the following CCS7 resources by the VVoIP EMS:

- Assign or change the self-identity SPC.
- Add CCS7 destinations.
- Change existing CCS7 destination attributes.
- Retrieve CCS7 destination attributes.
- Delete/remove CCS7 destinations.
- Retrieve link port attributes.
- Modify link port equipment settings.

- Create/add link sets.
- Modify link set attributes.
- Retrieve link set attributes.
- Remove/delete link sets with no member links.
- Assign/add member links to existing link sets.
- Modify link attributes.
- Retrieve link attributes.
- Delete/remove inactive signaling links.
- Create CCS7 MTP2 timer profiles.
- Modify CCS7 MTP2 timer profiles.
- Retrieve CCS7 MTP2 timer profiles.
- Delete CCS7 MTP2 timer profiles.
- Create CCS7 MTP link transmit congestion threshold profiles.
- Modify link transmit congestion threshold profiles.
- Retrieve link transmit congestion threshold profiles.
- Delete link transmit congestion threshold profiles.
- Create CCS7 MTP3 timer profile.
- Modify CCS7 MTP3 timer profile.
- Retrieve CCS7 MTP3 timer profiles.
- Delete CCS7 MTP3 timer profile.
- Set or change MTP3 control indicators.
- Retrieve MTP3 control indicators.

[Conditional] It shall be possible for the VVoIP EMS or local management to configure each CCS7 signaling link initially at the SG as follows:

1. Requesting an “inactive” state so the link terminal may be activated later when provisioning activity may be coordinated with the far-end NE (STP) and with interoffice facility systems.

2. Requesting an “active state” under which the SG shall attempt to immediately activate, align, and prove in the signaling link, subject to prevailing network conditions.

5.3.2.18.4.1.3 Status Monitoring

The SG is expected to support status management functions via its interface with the VVoIP EMS. A CID may be supported for direct control of the interface of the SG. References to the configuration interface in this document shall be meant to correspond to either interface.

5.3.2.18.4.1.3.1 General State Variables

[Conditional] The SG shall be capable of monitoring the following states for each of its configured resources:

- Operational state
- Usage state
- Administrative state
- Service status
- Procedural status

NOTE: The preceding conditional requirement does not imply that all these states and their values need to be applied to each configured resource or component at the SG. In fact, the definitions of these states are likely to apply to only certain types of resources or traffic-carrying components. When applied to specific SG resources, they will be subject to interpretation. These states are not exhaustive in terms of all the relevant state information that needs to be monitored for the SG's resources.

5.3.2.18.4.1.3.2 SG CCS7 Signaling Point States

[Conditional] An SG shall maintain its own (local) CCS7 MTP3 signaling point status, ITU-T Recommendation X.731 administrative state, and X.731 operational state.

5.3.2.18.4.1.3.3 CCS7 Link Equipment Port States

[Conditional] For each CCS7 link port detected by the SG's Management function, the SG shall maintain the following states:

- Equipage state: Unequipped or Equipped
- Provisioning state: Assigned or Spare

5.3.2.18.4.1.3.4 CCS7 Link States

[Conditional] For each configured CCS7 signaling link, the SG shall maintain the status variables with indicated state values as recognized by the MTP3 of the CCS7 protocol, per Telcordia Technologies GR-246-CORE, Volume 1, T1.111.4, Section 3.2, Status of Signaling Links.

[Conditional] For each configured CCS7 signaling link, the SG shall maintain the following status information:

- Link Activity Status: Inactive or Active
- Management-Inhibit Status: Locally, Remotely, Both, or Not
- Transmit Congestion Status: Level 1 onset, Level 1 discard, Level 2 onset, Level 2 discard, Level 3 onset, Level 3 discard, or Not
- Service Status: In-Service or Out-of-Service
- Local Processor Outage Status: Spontaneous outage, Interworking-induced outage, Management-induced outage, or None
- Remote Processor Outage Status: Remotely blocked or Not remotely blocked
- Receiving Congestion Status: Congested or Not-congested
- Link Terminal Status: Active or Inactive

5.3.2.18.4.1.3.5 CCS7 Link Set States

[Conditional] For each configured CCS7 signaling link set, the SG shall maintain a Link Set Availability indicator: Available or Unavailable.

5.3.2.18.4.1.3.6 CCS7 Destination/Route-Set States

[Conditional] For each configured CCS7 destination, the SG shall maintain the status of that destination's signaling route-set. This status variable shall convey one of the following values: Unavailable, Available, Congested-Level-1, Congested-Level-2, or Congested-Level-3.

5.3.2.18.4.1.3.7 CCS7 Signaling Route States

[Conditional] For each configured CCS7 signaling route (destination/link set combination) the SG shall maintain the status of that route. This status variable shall convey one of the following status values: Allowed, Prohibited, or Restricted.

5.3.2.18.4.1.3.8 Status Retrieval–- General

[Conditional] The SG shall support query capabilities from the VVoIP EMS to retrieve current SG status information about installed major components and process at the SG.

5.3.2.18.4.1.3.9 Autonomous Notification of State Changes

The SG needs to be able to provide the VVoIP EMS notification of changes of state as the result of recognition that a state has changed, such as a change from "enabled" to "disabled" in the event of a failure.

[Conditional] The SG shall be capable of providing to the VVoIP EMS notification of changes to the Operational and Administrative states of major components and other monitored resources associated with the SG.

5.3.2.18.4.1.3.10 Status Management Actions – General

[Conditional] The SG shall be capable of placing components in or out of service in a graceful manner when instructed to do so by the VVoIP EMS.

5.3.2.18.4.1.3.11 Status Management Actions for CCS7 Interfaces

[Conditional] The SG shall support the following state management interactions for the specified CCS7 resources as initiated by the VVoIP EMS:

1. Request local management inhibiting of a signaling link not yet locally inhibited.

2. Request local management uninhibiting of a locally inhibited signaling link.

3. Request activation of an inactive signaling link.

4. Deactivate (render inactive and remove from service) a signaling link already unavailable to MTP user part message traffic for other reasons.

5. Unconditionally force a manually induced local processor outage condition in a signaling link.

6. Clear a manually induced local processor outage condition for a manually blocked link set or member link, allowing link restoration (subject to prevailing network conditions).

7. Unconditionally deactivate a signaling link and remove it from service, regardless of its current MTP3 availability status or the status of its supported route sets.

5.3.2.18.4.2 SG Support for Fault Management

Fault management for the SG includes the following:

- Alarm surveillance
- Fault localization
- Testing

The focus of these requirements will be on alarm and event surveillance, in terms of the reporting by the SG of detected alarm and event conditions. Fault localization and testing capabilities are addressed only on a best-effort basis.

5.3.2.18.4.2.1 SG Alarm Surveillance

Alarm surveillance provides the capability to monitor failures detected in network appliances in NRT. This information, along with other information, allows Voice network management personnel to determine the nature and severity of the fault. The term "alarm" actually refers to all types of events that are associated with specific events. Although most alarms are associated with specific events, some alarms are based on a cumulative count of specified events exceeding a preset threshold during a designated period.

[Conditional] The SG shall conform to all applicable objectives for trouble detection, verification, and notification in a switching network appliance, as specified in Telcordia Technologies GR-474-CORE, *OTGR*. Specifically, the applicable GR-474-CORE requirements are R474-[83] through O474-[85], O474-[88], R474-[90], R474-[92], and R474-[93].

[Conditional] Upon detection of or clearing of an alarm condition, the SG shall generate an alarm event notification. Each alarm notification generated by the SG shall contain the following information:

1. SG Identity. The unique identifier of the SG generating the event notification.

2. Event Type Identifier. A unique identifier or code conveying the specific type of event reported (e.g., the failure of a specific type of component or resource).

3. Sequence Number. A unique sequence number for the reported alarm/event notification, so that the notification may be properly sequenced by the VVoIP EMS, and so missing or discarded notifications may be detected.

4. Timestamp. The date, time, and time zone at which the event was detected by the SG based on its internal system clock.

5. Alarm Severity. Conveying the seriousness of the reported alarm/event condition and the intended priority of management action to address the alarm. Applicable values include the following:

a. Critical
b. Major
c. Minor
d. Information only (non-alarmed)
e. Recovery – Critical
f. Recovery – Major
g. Recovery – Minor
h. Recovery – Non-Alarmed

6. Impacted Resource. A locally or globally unique identifier identifying the specific instance of the impacted NE component or resource, or external network resource, for which the fault or trouble condition was detected.

The alarm severity and impacted resource(s) will differ according to the specific alarm/event type. Requirements for additional output parameters may apply on an alarm/event-type specific basis, such as the detected or probable cause of a fault condition, results of diagnostic procedures run on the resource, and supporting information that may be used to support trouble verification, localization, and isolation.

[Conditional] The SG shall support queries for alarm status and state information.

[Conditional] The SG shall monitor, detect, and generate alarm conditions and states associated with hardware. The minimum faults monitored are as follows:

- Link interface line card out of service
- Control CPU out of service

5.3.2.18.4.2.2 Notification Retention

[Objective] The SG shall log alarm/event notifications in a local database, in case the operations interface or the VVoIP EMS is unavailable for a period.

5.3.2.18.4.2.3 Alarm Surveillance for CCS7 Interfaces

An SG is expected to generate an alarm or event notification concerning its CCS7 interfaces and associated resources.

[Conditional] The SG shall generate an alarm notification to the VVoIP EMS immediately when one of the following situations occurs:

1. The SG becomes isolated from both member STPs of its serving STP pair (Critical).

2. The SG becomes isolated from an adjacent STP (Major).

3. A CCS7 destination (i.e., signaling point or network cluster) other than the adjacent STP's unique DPC becomes unavailable (Major).

4. A route set to a CCS7 destination (i.e., signaling point or network cluster) other than the adjacent STP's unique DPC becomes unavailable (Major).

5. A CCS7 route set to a remote (non-adjacent) CCS7 point code destination becomes congested or increases its congestion level (Minor).

6. All links comprising a CCS7 link set have become unavailable to MTP user-part message traffic (Major).

7. A previously available CCS7 signaling link has become unavailable to CCS7 user part message traffic, as perceived by MTP3 (Minor).

8. A CCS7 link previously regarded as "in-service" at MTP2 has failed (Minor).

9. A failed CCS7 link, or a previously inactive CCS7 link for which activation has been initiated by MTP3, has failed its first alignment attempt following the link failure or attempted activation, or that alignment is not possible due to prevailing network conditions (Minor).

10. A failed CCS7 link, or a previously inactive CCS7 link for which activation has been initiated by MTP3, has failed one or more alignment and proving attempts and has remained out of service for a duration exceeding the MTP3 Failed Link Craft Referral Timer (Minor).

11. A CCS7 signaling link has been remotely blocked due to an MTP3 or higher level processor outage at the far end (Minor).

12. A CCS7 signaling link has been locally blocked due to a spontaneous or induced local processor outage (Minor).

13. A CCS7 signaling link is deactivated and removed from service by Operations management (Minor).

14. The SG's own local CCS7 MTP3 has become unavailable (Critical alarm).

15. A thresholdnumber (value to be set by network control personnel) of incoming CCS7 messages that fail MTP message discrimination is reached.

16. A thresholdnumber (value to be set by network control personnel) of outgoing CCS7 messages that fail MTP routing procedures is reached.

[Conditional] The SG shall generate an alarm recovery notification to the VVoIP EMS immediately when it recovers from a reported alarm condition.

[Conditional] The SG shall allow the VVoIP EMS to suppress reporting of the alarm and event notification.

5.3.2.18.4.2.4 SG Fault Localization

Fault localization determines the root cause of a failure. Where the initial failure information is insufficient for fault localization, it has to be augmented with information obtained by additional failure localization routines.

5.3.2.18.4.2.4.1 General

[Conditional] An SG shall, on request or on a predefined schedule, run diagnostics on hardware checks on software and report the result to the VVoIP EMS.

5.3.2.18.4.2.4.2 For CCS7 Interfaces

The SG, as a CCS7 network node, should provide capabilities by which it can assist network maintenance personnel in distinguishing faults associated with local Signaling Link Terminal Equipment (SLTE), from faults that may be attributed to link transmission facilities or far-end SLTE.

[Conditional] If a failed signaling link or an inactive signaling link for which activation has been initiated fails to align and correct after a period of T19 as specified in GR-246-CORE, Volume 1, T1.111.4 (provisional value of 8 minutes), the SG shall temporarily suspend the restoration or activation attempt and automatically run diagnostics on the SLTE. After the diagnostics are completed, the SG shall generate an output message (i.e., event notification) to inform management of the sustained failure and convey the results of the diagnostics.

5.3.2.18.4.3 SG Support for Testing

Testing is concerned with the testing of transmission facilities and related resources within the SG. Testing may be carried out for the following purposes:

1. Testing connecting facilities in preparation for installation of new equipment.

2. Accepting newly installed facilities or service circuits.

3. Validating trouble reports.

4. Supporting fault localization.

5. Verifying repair.

5.3.2.18.4.3.1 General

[Conditional] The SG shall provide both local and remote loopback capabilities for the signals that terminate at the SG physical ports.

The SG shall support the ability to perform internal diagnostics on its internal resources.

[Conditional] The SG shall provide diagnostics that can examine the state of each significant element of hardware, and that can identify faults and isolate failures to within the smallest replaceable unit of hardware.

[Conditional] The SG shall permit the VVoIP EMS to initiate diagnostics.

[Conditional] The SG shall provide test access to external test equipment for passively monitoring the traffic through the SG interfaces. This passive monitoring shall not degrade the performance of traffic.

5.3.2.18.4.3.2 For CCS7 Interfaces

[Conditional] The SG shall support the initiation, via the VVoIP EMS and the CID, of CCS7 signaling data link test procedures to be performed over its DS0 interfaces, including loopback test procedures, as specified in Telcordia Technologies GR-246-CORE, Chapter T1.111.7, Section 2.1, and the reporting of test results via those interfaces.

5.3.2.18.4.4 SG Support for Performance Management

This section addresses the performance management criteria used to evaluate and report on the behavior and effectiveness of the SG, as well as the physical and logical entities it supports.

The main focus will be on traffic and performance monitoring. Traffic and performance monitoring provides a systematic assessment of a particular entity’s ability to carry out its assigned function through the continuous collection and analysis of appropriate performance measurement data. Traffic and performance monitoring procedures are intended to quantify the traffic offered to, and handled by, a network appliance and its components, as well as capture intermittent error conditions and troubles resulting from the gradual deterioration of network equipment. Proactive maintenance techniques, such as traffic and performance monitoring, enable the network provider to detect troubles early before they escalate in severity.

5.3.2.18.4.4.1 General Monitoring Requirements (Common)

This section defines some common requirements for performance management, including counters and monitoring intervals, and generation of threshold crossing alerts.

5.3.2.18.4.4.1.1 Counters and Monitoring Intervals

All counters need to be designed so they remain at their maximum value, so they do not "roll over" to "000...000." It is stressed that the term "counter" does not imply an implementation. For example, if three counts are required, as well as an associated sum of errors counter, this could be implemented as two registers for two simple counts, and one register for the sum of errors. The third simple count could be inferred from the other two.

[Conditional] Upon receiving a request from the VVoIP EMS, the SG shall provide a report of a parameter's present or history counters.

Most traffic and performance measurement data collected by the SG for performance management purposes (e.g., for traffic engineering, and planning and performance monitoring) shall be collected on a 15-minute accumulation interval. The following requirement applies to the storage and accuracy of those measurements.

[Conditional] For all counters, the SG shall store 8.25 hours worth of 15-minute data, the current 15-minute interval plus the past thirty-two 15-minute intervals.

5.3.2.18.4.4.2 SG Traffic and Performance Monitoring

This section provides requirements and objectives for the SG's collection, monitoring, and reporting of traffic and performance measurements, which include the following:

1. Scheduled measurements are to be collected routinely by the SG and made available to the VVoIP EMS on an ongoing basis. Some of these measurements shall be thresholded for the purposes of exception reporting and Threshold Crossing Alerts (TCAs).

2. Exception measurement reports are to be generated and reported only when key measurement counters are non-zero or exceed specified thresholds.

3. Threshold Crossing Alerts (TCAs) are generated as event notifications when thresholds are first crossed for key performance measurements.

For each applicable resource type, measurements are specified in terms of the measurement definition, the accumulation basis (e.g., per component type), and the applicable accumulation interval (e.g., 5, 15, or 60 minutes, or 24 hours) based on the specific intended use in Performance Management functions. The following abbreviations are used within the stated measurement requirements (enclosed within square brackets) to denote the appropriate measurement accumulation intervals and the typical uses for such measurements:

1. [5] equals 5 minutes. Typically used for near-real-time Network Traffic Management (NTM) surveillance.

2. [15] equals 15 minutes. Typically used for traffic engineering/capacity monitoring and short-term performance monitoring.

3. [h] equals hourly. Typically used for network maintenance surveillance.

4. [m] equals hourly-marginal. Typically used for exception-oriented performance management, reported only when key marginal performance indicators are exceeded.

5. [d] equals daily. Typically used for network maintenance surveillance, including longer term trending of traffic measurements and those performance measurements indicating faults and error conditions.

When no interval is specified, the 15-minute accumulation interval is implied by default.

5.3.2.18.4.4.2.1 SG Product Totals

[Conditional] The SG shall support the collection and reporting of the following performance measurements on a total product basis for the indicated intervals:

- SG availability {15, d}.

- CCS7 MTP3 user part messages discarded due to SG node internal failures {15, d}.

- CCS7 MTP3 user part messages discarded due to SG node internal congestion or overload {15, d}.

- Duration of SG node internal failure, defined as the total time that messages could not be switched to the appropriate interface for transmission, independent of interface failures {15, d}.

5.3.2.18.4.4.3 CCS7 Interface Measurements

The requirements and objectives in this section address measurements concerning the SG's CCS7 interfaces and associated resources.

5.3.2.18.4.4.3.1 CCS7 Link Measurements

[Conditional] The SG shall support the collection and reporting of the following traffic and performance measurements on a per-CCS7-link basis for the indicated intervals:

- MSUs received {15, d, m}
- MSUs transmitted (including retransmissions) {15, d, m}
- MSUs retransmitted {m}
- MSU octets received {15, d}
- MSU octets transmitted (including retransmitted MSUs) {15, d}
- MSU octets retransmitted {m}
- Signal Units (SUs) received in error {15, m, d}
- Number of hourly marginal performance thresholds exceeded for SUs received in error {d}
- Negative acknowledgements received from the far end {15, m, d}
- Number of hourly marginal performance thresholds exceeded for negative acknowledgements received {d}
- Duration of link unavailability to MTP3 user part message traffic (seconds) {5, 15, m, d}
- Duration of link out-of-service at MTP2 (seconds) {15, m, d}
- Link Maintenance Usage: duration of link unavailability attributed to management action, including inhibiting (local or remote), management-induced local processor outage, or deactivation/removal from service (seconds) {15, m, d}

- Number of automatic link changeovers {15, m, d}

- Number of hourly marginal-performance thresholds exceeded for automatic changeovers {d}

- Event count for entry into level 1 transmit congestion (onset threshold crossings) {15}

- Event count for entry into level 2 transmit congestion (onset threshold crossings) {15}

- Event count for entry into level 3 transmit congestion (onset threshold crossings) {15}

- MSUs discarded due to local link transmit congestion (all priorities) {15}

- Priority 0 MSUs discarded due to local link transmit congestion {15}

- Priority 1 MSUs discarded due to local link transmit congestion {15}

- Priority 2 MSUs discarded due to local link transmit congestion {15}

- Priority 3 MSUs discarded due to link transmit buffer overflow {15}

- Link transmit buffer maximum observed occupancy {15}

- Link transmit buffer average occupancy {15}

- Duration of receipt of Status Indication “Busy” (SIB) Link Status Signaling Units (LSSUs) (remote receiving congestion) (seconds) {15}

- Duration of transmission of SIB LSSUs (local receiving congestion) (seconds) {15}

- Duration of receipt of SIPO LSSUs (remote processor outage) (seconds) {15}

- Duration of transmission of SIPO LSSUs (local processor outage) (seconds) {15}

5.3.2.18.4.4.3.2 Performance Reporting of TCAs

[Conditional] The SG shall allow the VVoIP EMS to set performance thresholds, and if a performance threshold is defined for a specific measurement, the SG shall compare the counter values of the indicated measurement to the corresponding thresholds. Whenever the threshold limit is exceeded during an interval, the SG shall report to a TCA to the VVoIP EMS.

5.3.2.18.4.4.3.3 CCS7 Link Set Measurements

[Conditional] The SG shall support the collection and reporting of the following traffic and performance measurements on a per-CCS7-link-set basis for the indicated intervals, aggregated across member links where necessary:

- MSUs received {15}
- MSUs transmitted (including retransmissions) {15}
- MSUs retransmitted {15}
- MSU octets received {15}
- MSU octets transmitted (including retransmitted MSUs) {15}
- MSU octets retransmitted {15}
- Duration of link set outage (all links unavailable to MTP3 user-part message traffic) {15}
- Duration of member link unavailability (summed across member links) {15}
- Number of assigned links in the link set {15}

5.3.2.18.4.4.3.4 CCS7 Destination/Route-Set Measurements

[Conditional] The SG shall support the collection and reporting of the following traffic measurements for the indicated intervals aggregated on a per configured-CCS7-destination/route-set basis (i.e., per configured DPC and cluster destination).

NOTE: For network cluster destinations, counts shall be aggregated over cluster members.

- MTP3 user part messages received (from matching OPC) {15}
- MTP3 user part messages transmitted (to matching DPC) {15}

- MTP3 MTP NM messages received (from matching OPC) {5,15}
- MTP3 MTP NM messages transmitted (to matching DPC) {15}

5.3.2.18.4.4.3.5 MTP3 and Interworking Measurements

[Conditional] The SG shall support the collection and reporting of the following traffic and performance measurements concerning its CCS7 Network Interface functions and their interactions with the SG's Interworking function.

NOTE: These measurements are to be aggregated across all CCS7 interfaces for the indicated intervals.

- Incoming CCS7 MTP3 messages received from the CCS7 network {15, d}
- Incoming invalid CCS7 MTP3 messages from the CCS7 network failing message discrimination due to invalid DPC (not matching the SG's primary SPC) or network indicator {15}
- Incoming valid CCS7 MTP3 messages submitted by MTP3 to the interworking function {15}
- Incoming valid CCS7 MTP NM (MTP-NM messages) {15}
- Incoming valid CCS7 Testing and Maintenance (T&M) messages {15}.
- Outbound CCS7 MTP3 messages submitted to MTP3 by the interworking function {15}
- Outbound CCS7 MTP3 messages discarded due to routing translation failures (unknown DPC or unrecognized network indicator) {15}
- Outbound CCS7 MTP3 messages discarded due to inaccessible CCS7 destinations {15}
- Outbound CCS7 MTP3 messages discarded due to CCS7 route-set congestion (local or remote) {15}
- Duration of SG isolation from serving STP pair {15, d}
- Unavailability of the SG's local CCS7 MTP3 to user part message traffic (seconds) {15, d}

5.3.2.18.5 Management Requirements of the MG Function

The MG interacts with the Appliance Management function by

1. Making changes to its configuration and to its trunks' configuration in response to commands from the Management function that request these changes.

2. Returning information to the Management function on its FCAPS in response to commands from the Management function that request this information.

3. Sending information to the Management function on a periodic basis (e.g., on a set schedule), and keeping the Management function up-to-date on MG activity. An example of this update would be a periodic transfer of trunk media error logs from the MG to the Management function, so the Management function could either store the records locally or transfer them to a remote NMS for remote storage and processing.

A complete description of the MG is provided in Section 5.3.2.12, Media Gateway Requirements.

5.3.2.18.5.1 MG Support for CM

The requirements in this section apply to MGs in general.

[Required] An MG shall manage logical and physical resource inventory information.

[Required] An MG shall issue an autonomous notification to the VVoIP EMS whenever a new inventory or capabilities are added, or configuration is changed through local management activity.

[Required] An MG maintains the information related to service features and data, including the management of service logic.

5.3.2.18.5.1.1 Status and Control

An MG shall be capable of managing and reporting the operational state and administrative state information for associated components that will at least include all hosts and processes.

5.3.2.18.5.1.2 Core Network Interface Resources

[Required] An MG shall manage current MG state and status information about its installed major components, line and plug-in cards, and processes.

[Required] An MG shall conform to all applicable OTGR requirements for trouble detection, verification, and notification in a switching system NE given in Telcordia Technologies GR-474-CORE. Specifically, the requirements from GR-474-CORE are R474-[83] through O474-[85], O474-[88], R474-[90], R474-[92], and R474-[93].

5.3.2.18.5.2 MG Support for Fault Management

5.3.2.18.5.2.1 MG Alarm Surveillance

[Required] Upon the detection or clearing of alarm conditions, the MG shall generate and forward, based on filtering criteria, a notification to the VVoIP EMS.

[Required] An MG shall support queries for alarm status, state, and current problem information.

[Required] An MG shall monitor, detect, and generate alarm conditions and states associated with hardware, functional components, system interfaces, and logical resources (e.g., trunk terminations, tone and announcement generators, media content detectors, signal processors, echo control devices).

5.3.2.18.5.2.2 MG Fault Localization

Fault localization determines the root cause of a failure. Where the initial failure information is insufficient for fault localization, it has to be augmented with information obtained by additional failure localization routines.

[Required] An MG shall perform root-cause analysis for any faults within its purview, report the root cause, and suppress the reporting of non-root-cause conditions.

5.3.2.18.5.2.3 MG Support for Testing

Testing is concerned with the testing of transmission facilities and related resources within the MG. Testing may be carried out for the following purposes:

- Testing connecting facilities in preparation for installation of new equipment
- Accepting newly installed facilities or service circuits
- Validating trouble reports
- Supporting fault localization
- Verifying repair

[Required] An MG shall, on request or per a pre-established schedule, run diagnostics on internal resources, hardware, or software, and report the result to the VVoIP EMS.

[Required] An MG shall provide both local and remote loopback capabilities for the digital interfaces that terminate at the MG ports.

[Objective] An MG shall provide test access to external test equipment for passively monitoring the traffic through the MG interfaces. This passive monitoring shall not degrade the performance of traffic.

5.3.2.18.5.3 MG Support for Performance Management

This section addresses the performance management criteria used to evaluate and report on the behavior and effectiveness of the MG, which includes gathering and analyzing of statistical data on interfaces that the MG supports.

5.3.2.18.5.3.1 Counters and Monitoring Intervals

All counters need to be designed so they remain at their maximum value, so they do not "roll over" to "000...000." It is stressed that the term "counter" does not imply an implementation. For example, if three counts are required, as well as an associated sum of errors counter, this could be implemented as two registers for two simple counts and one register for the sum of errors. The third simple count could be inferred from the other two.

[Required] Upon receiving a request from the VVoIP EMS or by an established schedule, an MG shall provide a report of a parameter's present or history counters.

[Required] For all counters, the MG shall store the current interval and 8 hours of history data.

5.3.2.18.5.3.2 Generation of Threshold Crossing Alerts

This section contains general requirements on the generation of TCAs. A particular count should generate a TCA if the requirement defining the count indicates that the count should be thresholded.

[Required] An MG shall generate TCAs to notify the VVoIP EMS when a thresholded count exceeds its threshold during a measurement interval.

5.3.2.18.5.4 Trunk Configuration Requirements

[Required] The MG shall manage interexchange trunk (between MG and SSP), trunk group, trunk, and physical resource inventory and configuration data.

[Required] The MG shall manage MG termination-related status information. This information includes the following:

- Context-ID Operational and Service status
- Trunk Administrative, Operational, and Service status
- Termination ID Administrative, Operational, and Service status

5.3.2.18.5.5 MG Trunk Fault Management

[Required] The MG shall include in the alarm notifications sufficient information to isolate failed replaceable units.

[Required] The MG shall support queries for alarm status, state, and current problem information.

[Required] The MG shall generate an alarm condition for any of the following failure conditions:

- Power loss
- Environmental condition not conducive to normal operation
- Loss of data integrity
- Interface faults (core, trunk, MG-CCA)
- Hardware and line card faults
- Functional Component and Resource faults
- Protocol alarm conditions

[Required] An MG shall, on request or on schedule, run diagnostics on internal resources and hardware, run checks on software, and report the results to the VVoIP EMS.

The MG shall provide both local and remote loopback capabilities for the physical signals that terminate at the MG ports.

[Required] The MG shall provide test access to external test equipment for passively monitoring the traffic through the MG interfaces. This passive monitoring shall not degrade the performance of traffic.

5.3.2.18.5.6 Trunk Performance Management (MG)

All Trunk Performance Management requirements are covered by the MG requirements.

5.3.2.18.5.7 Access Configuration Requirements

[Required] The MG shall receive voice-grade analog line configuration data from the VVoIP EMS upon service activation.

5.3.2.18.5.7.1 Conventional DS1 Interface to PBX

[Required] The MG shall receive Digital Signal 1 (DS1) Interface configuration data from the VVoIP EMS upon service activation.

5.3.2.18.5.7.2 ISDN PRI Trunks

[Required] The MG shall receive ISDN PRI trunk configuration data from the VVoIP EMS upon service activation.

5.3.2.18.5.7.3 Interface Status Parameters

[Required] The MG shall set the status parameters necessary for support of ISDN digital subscriber lines basic rate and DS1 interfaces.

5.3.2.18.5.8 Access Fault Management

Many circuit troubles are detected by the customer, but others may be detected by per-call or automatic routine tests.

[Required] The MG shall provide diagnostic tests to detect and verify faults, such as low loop resistance or ground conditions, or any other faults within the MG that could cause false ring trip or false answer.

The actual tests needed to satisfy the previous requirement depend on the MG implementation; hence, they are not specified in this generic requirements document.

[Required] The Integrated Digital Terminal (IDT) function in the MG shall support all the protection switching requirements as specified in Telcordia Technologies GR-303-CORE.

[Required] An MG providing DS1 interfaces shall detect line and path defects as specified in Telcordia Technologies GR-820-CORE, Section 4.1.2, *DS1 Performance Defects*.

The DS1 defects include LOS, Out of Frame (OOF), Severely Errored Frame (SEF), AIS, and Alarm Indication Signal - Customer Installation (AIS-CI).

[Required] An MG providing DS1 interfaces shall support the DS1 failure declaration process (i.e., line, near-end path, far-end path) specified in Telcordia Technologies GR-820-CORE, Section 4.

The DS1 failures include LOS, OOF, AIS, AIS-CI, RAI, and Remote Alarm Indication - Customer Installation (RAI-CI).

[Required] An MG providing DS1 interfaces shall generate DS1 trouble notifications (i.e., alarms) upon the declaration of a DS1 failure condition. Trouble notifications shall be consistent with the DS1 line and path trouble notification criteria specified in Telcordia Technologies GR-474-CORE, Section 8.2.

[Required] The MG shall generate alarm conditions for Digital Signal 3 (DS3) signals by monitoring the paths and lines for failures, as specified in Telcordia Technologies GR-820-CORE, Section 5.

5.3.2.18.5.8.1 ISDN Primary Rate Access Testing

There are multiple ways that test accesses are provided to the MG to support ISDN Primary Rate Access (PRA) testing. They are as follows:

- Monitor Access function
- Split Access function
- Digital Test Unit (DTU) Loopback function

The MG shall conform to the test access, access supervision, test signal and bit error insertion, line loopback control, signal monitoring and measuring, and service state control requirements as specified in Telcordia Technologies TR-NWT-001219.

5.3.2.18.5.9 MG Access Performance Management

The following requirement applies to all interfaces from the MG to the MFSS or LSC ASLAN.

In addition, the DS1 physical layer protocol monitoring requirements shall apply to the MG ISDN PRI interfaces and non-ISDN PBX trunk interfaces (CAS trunk interfaces) supported by DS1 transport.

[Required] The MG shall support the collection of the standard DS1, DS3, Physical Layer Convergence Protocol (PLCP), SONET, and ISDN BRI line performance monitoring requirements, as defined in Telcordia Technologies GR-820-CORE, for applicable interfaces.

5.3.2.19 Accounting Management

This section provides the minimum set of requirements to capture the basic call information for accounting purposes. Additional information on this call accounting is contained in Telcordia Technologies GR-3058-CORE.

Accounting management identifies a set of events during which call detail information is collected. These events are call connect, call attempt, and call disconnect. When these events are detected, specific call data will be provided by the network appliances that were involved in the event. Each appliance has a certain function within the network, therefore will be in the natural position to have knowledge of particular call data. The collections of this call information from all appliances will provide the data necessary to formulate a billing record.

The requirements provided in this section allow for the functional elements to be individual components within the network, or be packaged together in an integrated system solution. In either case, each component will have a certain role in the call and be privy to specific call data that is needed to construct a billing record.

This section assumes that the Media Server function, the UFS function, and the Directory function together provide the necessary information and services needed for billing and jointly provide the functional equivalent to a Service Agent (SA). An SA is defined as follows:

- The SA supports the execution of service logic both for transactions that occur completely within the IP network, and for those that require signaling to CCS7 SEPs (e.g., SG, SCP) that are external to the IP network. The SA may be part of the network appliance that provides CCA functionality, or it may be deployed in a separate appliance that communicates with the CCA.

It is assumed that an LSC, MFSS, and WAN SS each has its own means of gathering call information (e.g., originating party, terminating party, time of call, date of call, call answered, call unanswered) and process the information into a call record. This function is equivalent to that of a Billing Agent (BA). A BA is defined as follows:

- A BA supports much of the billing functionality needed in the VoIP network. It collects the necessary call data from the CCAs and other network appliances, and processes them for use by downstream billing systems.

This section assumes that the VVoIP EMS will provide the same functionality as that of the BA. Therefore, throughout the remainder of this document, reference to the BA should be viewed as the functional equivalent that resides within the VVoIP EMS. The communications between the functional entities (e.g., CCA, MGC) and the BA will be internal to the appliance, and all the necessary accounting data is assumed to be made readily available to the BA.

However, there may be network appliances that are externally linked to the SSs (e.g., an external MG connecting into the MGC of the LSC). Depending on the purpose of these network appliances, they may be in the best position to obtain specific accounting data on calls that involve the use of this external network appliance. Therefore, this data should be provided to the BA (whether this information is passed to the BA directly, or passed to the CCA or MGC, which then passes it to the BA).

The following section lists the requirements for accounting data that should be provided by the functional entities to the BA. The Section 5.3.2.19.2, Processing of Data Sets, applies to external network appliances (e.g., MG) that need to provide accounting data to the BA. As mentioned before, functional entities within a network appliance are assumed to have their own means of sharing accounting data; however, the requirements in the following section can be used to ensure that the specific data is made available to the BA (within the internal communications and sharing) so that the proper accounting can be accomplished.

5.3.2.19.1 Accounting Data

[Objective] A network appliance shall support the data sets described in this section for supplying accounting information to the necessary functional entity that will generate call detail recordings.

The call data captured for calls that are detected by the CCA and other functional entities are the individual pieces of data that, when logically assembled by the BA, provide the details required to account for the use of a service. Some of this call data is captured based on call events, usually determined from the content of received signaling messages. Other call data is determined from local information maintained at the CCA.

Whenever the CCA or other functional entities generate call data, the CCA or other functions would package the call data into what is known as a DS, which is then transmitted to the BA. A Data Set is another name for a Protocol Data Unit (PDU), which is specified in Telcordia Technologies GR-3058-CORE.

NOTE: The term Data Set (or PDU) is used in the generic sense to describe a unit of related information, and is not meant to imply the use of any specific protocol for the communications between the functional entities and the BA. The actual protocol for communications between the functional entities and the BA is considered to be a vendor decision.

The functional entities generate the data sets based on an event. The following three events generate the Data sets:

- Call Connect
- Call Disconnect
- Call Attempt (e.g., call was attempted, but unsuccessful)

The following lists the three data sets:

- Call Connect Data Set. Used for call data that represents a call connection event.

- Call Disconnect Data Set. Used for call data that represents a call disconnection event.

- Call Attempt Data Set. Used for call data that represents a call attempt event.

A successful voice call would have two events (each of which would result in data sets): the Call Connection event and the Call Disconnection event. For unsuccessful voice calls, the call event would result in the generation of the Call Attempt Data Set(s). This can also apply to a Video session. For example, when a user wants to open a Video session, a connection attempt will need to be made to the application that will provide the video.

Either a Call Connection Data Set (if the video connection is made) or a Call Attempt Data Set (if the video connection is attempted, but is not successfully connected) would be generated. If a video connection is made and the video is played, a Call Disconnect Data Set will be generated once the video connection is over.

The following subsections provide the formatting and field definitions for the Call Connect Data Set (the Call Attempt Data Set has the same format as the Call Connect Data Set) and the Call Disconnect Data Set. The formatting is provided in Table 5.3.2.19-1, Call Connect Data Set Information, with the following column headings:

1. The first column identifies the call data.

2. The second column identifies whether this data is conditionally required (C) or optional (O) for the DISN.

3. The third column specifies the call data as either fixed (F) or variable (V) in length.

4. The fourth column identifies the section in Telcordia Technologies GR-3058-CORE that provides more information on the fields.

5. The fifth column provides a summary of how the field is populated.

6. The sixth column reflects what is currently believed to be the most appropriate network component for each data element. "PRI" indicates the NC network appliance that is considered the "primary" source for the data element.

7. The seventh column reflects what is currently believed to be the "secondary" source or source of the data for that particular element. It is labeled as "SEC."

Table 5.3.2.19-1. Call Connect Data Set Information

USAGE DATA ELEMENT	DEPEND REQ'D/ OPTIONAL	FIXED/ VARIABLE	REFERENCE SECTION IN GR-3058-CORE	POPULATION SUMMARY	PRI	SEC
Call Event Type	R	F	3.3.6	1 = Call Completion 3 = Call Attempt	CCA	MG MGC
Correlation ID	R	F	3.3.6.2	UUID = 128 bits (Variable depending on implementation) Unique value for each call composed of: 1. Network Component Network Appliance ID 2. Timestamp 3. Random Number	CCA	MG MGC
Element Identifier	R	F	3.3.6	Range of 000001 through 999999	CCA	MG MGC
Directional Indicator	R	F	3.3.6.4	1 = Egress (originating) 2 = Ingress (terminating) 3 = Transiting (MGC) 4 = Intra-gateway (AGW)	CCA	MG MGC
Study/Test Indicator	R	F	3.3.7.1	Default = zeros (or null-value)	CCA	MG MGC
Timing Guard	R	F	3.3.7.1	0 = no timing irregularities detected 2 = timing irregularities detected	CCA	MG MGC
Customer Connect Date Customer Connect Time	R	F	3.3.7.2	MMDDYYYY - Month, Day, and Full Year HHMMSSms – Hours, Minutes, Seconds, and milliseconds (depending on implementation).	MG	CCA MGC
Incoming Destination Number	R	V	3.3.8.7	For services other than toll-free – destination routing address (if NANP based, this is pre-NP query – NOT the LRN) For toll-free – NANP routing number (pre-NP query – NOT the LRN) returned from toll-free query	MG	CCA MGC
Destination Address [IN and AIN queries only]	R	V	3.3.9.1	For toll-free – NANP routing number (pre-LNP query – NOT the LRN) returned from toll-free query	CCA	SA MGC
Calling Station ID	R	V	3.3.7.6	Used for CPN	MG	CCA MGC

USAGE DATA ELEMENT	DEPEND REQ'D/ OPTIONAL	FIXED/ VARIABLE	REFERENCE SECTION IN GR-3058-CORE	POPULATION SUMMARY	PRI	SEC
Called Station ID up to 15 digits	R	V	3.3.7.7 3.3.10.4	Egress calls Ingress calls dealing with NP	MG	CCA MGC
Overseas Indicator	R	F	3.3.7.7	0 = North America World Zone 1 1 = International (01 or 011 prefix dialed)	MG	CCA MGC
Operator Involvement	R	F	3.3.7.7	0 = No Involvement 1 = 0+ or 0- dialed	MG	CCA MGC
Dialing Indicator	R	F	3.3.7.7	0 = No CAC 1 = 10XXXX dialed	MG	CCA
Dialed Carrier Identification Code	R	F	3.3.7.7	Carrier Identification Code (if dialed) Default = zeros (or null-value)	MG	CCA MGC
Presubscription Indicator	R	F	3.3.7.7	0 = No presubscription on line 1 = PIC present	MG	CCA
PIC - Presubscribed Carrier Identification Code	R	F	3.3.7.7	Carrier Identification Code when PIC = 1 Default = zeros (or null-value)	MG	CCA MGC
ANI (Charge Number)	R	F	3.3.7.9	ANI for Originating Call ChN received for transiting and terminating calls	MG	MGC
Service Provider Identification – Switching System ID	R	V	3.3.7.10	Operating Company Number of CCA owner	MG	CCA MGC
Service Provider Information – Account Owner	R	V	3.3.7.10	Operating Company Number of the Calling Station's Service Provider	MG	CCA MGC

USAGE DATA ELEMENT	DEPEND REQ'D/ OPTIONAL	FIXED/ VARIABLE	REFERENCE SECTION IN GR-3058-CORE	POPULATION SUMMARY	PRI	SEC
Service Feature	R	F	3.3.7.11	Reference Table 12 of GR-1100-CORE for a representative list of service features that could be provisioned on a line at the AG. A few notable features of importance are: 7 Call Forwarding 8 Call Hold 9 Call Transfer 10 Call Waiting 11 Conference Call	MG	CCA MGC
Calling Station Porting Status	R	F	3.3.10.1	0 = Not Ported 1 = Ported 2 = Not on AG	MG	CCA MGC
Called Number Porting Status	R	F	3.3.10.1	0= Not Ported 1 = Ported 2 = Not on AG	MG	SA
Incoming Calling Party Number	R	V	3.3.7.9	CPN parameter in CCS7 or functional equivalent	MGC	CCA MGC
Facility Allocation Date Facility Allocation Time	R	F	3.3.7.3	MMDDYYYY – Month, Day, and Full Year HHMMSSms – Hours, Minutes, Seconds, and milliseconds (depending on implementation)	MGC	CCA
Service Type	R	F	3.3.7.5	1 = No CS-PSTN Interface 2 = Interface to CS-PSTN (via MGC)	MGC	CCA
Called Party Offhook	R	F	3.3.7.8	0 = Called Party Offhook detected 1 = Called Party Offhook not detected	MGC	CCA
Egress Trunk Group Number	R	F	3.3.8.1	Provisioned TG number at MGC (TG)	MGC	CCA
Egress Trunk Group Designation	R	F	3.3.8.1	See Table 3-3 in GR-3058-CORE	MGC	CCA
Egress Signaling Protocol	R	F	3.3.8.4	See Table 3-4 in GR-3058-CORE	MGC	CCA
Egress Interfacing Network ID	R	V	3.3.8.2	Operating Company Number assigned to the interfacing Network Provider	MGC	CCA

USAGE DATA ELEMENT	DEPEND REQ'D/ OPTIONAL	FIXED/ VARIABLE	REFERENCE SECTION IN GR-3058-CORE	POPULATION SUMMARY	PRI	SEC
Egress Trunk Group Billing Number	R	F	3.3.8.2	Billing Number assigned to the facility	MGC	CCA
Egress QoS Statistics	R	F	3.3.8.5	Variable – See Table 3-5 in GR-3058-CORE	MGC	CCA
Ingress Trunk Group Number	R	F	3.3.8.1	Provisioned TG number at MGC (TG)	MGC	CCA
Ingress Trunk Group Designation	R	F	3.3.8.1	See Table 3-3 in GR-3058-CORE	MGC	CCA
Ingress Signaling Protocol	R	F	3.3.8.4	See Table 3-4 in GR-3058-CORE	MGC	CCA
Ingress Interfacing Network Id	R	V	3.3.8.2	Operating Company Number assigned to the interfacing Network Provider	MGC	CCA
Ingress Trunk Group Billing Number	R	V	3.3.8.2	Billing Number assigned to the facility	MGC	CCA
Ingress QoS Statistics	R	V	3.3.8.5	Variable – See Table 3-5 in GR-3058-CORE	MGC	CCA
Release Cause	R	V	3.3.8.6	Variable – See Table 3-6 in GR-3058-CORE for examples	MGC	CCA
Jurisdiction Designation of MGC	R	F	3.3.8.3	NPA-NXX representative of the Jurisdiction of the MGC	MGC	CCA
CCA-LRN	R	F	3.3.10.2	When Directional Indicator = 1, then LRN of the originating CCA-MGC-AG combination When Directional Indicator = 2 or = 3, then zeros	MGC	CCA
Incoming JIP	R	F	3.3.10.3	When Directional Indicator = 2 or = 3, then the digits contained in the JIP parameter (CCS7) or equivalent	MGC	CCA
Toll-Free Query Indicator	R	F	3.3.9.1	141 = Handoff to IC 142 = LEC Transport	SA	CCA
Toll-Free CIC	R	F	3.3.9.1	Toll-Free Transport provider	SA	CCA
LRN – DB	R	F	3.3.10.2 3.3.10.3 3.3.10.4	Ported = LRN of destination switch Non-Ported – Called Number	SA	CCA

USAGE DATA ELEMENT	DEPEND REQ'D/ OPTIONAL	FIXED/ VARIABLE	REFERENCE SECTION IN GR-3058-CORE	POPULATION SUMMARY	PRI	SEC
LNP Query Status	R	F	3.3.10.2 3.3.10.3 3.3.10.4	See Table 3-7 in GR-3058-CORE	SA	CCA
Originating Customer/ Business Group Identification	R	F	7.1.1.1	10-Digit Originating Customer/Business Group Identification number	MG	CCA MGC
Terminating Customer/ Business Group Identification	R	F	7.1.1.2	10-Digit Terminating Customer/Business Group Identification number	MG	CCA MGC
CCA IPv4 Address	R	F	3.3.7.10	IPv4 address assigned to the CCA	CCA	CCA
CCA IPv6 Address	R	F	3.3.7.10	IPv6 address assigned to the CCA	CCA	CCA
Bearer Capability/Call Type	R	V	3.3.7.12	Bearer call type and bearer capabilities delivered to the user	MG	CCA MGC
Network Interworking	R	V	3.3.7.12	Identifies the different interworking situations encountered by the user's call	MGC	CCA
Signaling or Supplementary Service Capabilities Usage	R	V	3.3.7.12	Records the use of signaling or supplementary service capabilities on a yes/no or other outcome basis, and it is designed to record one, all, or any combination of these capabilities in a single record.	MGC	CCA
Call Characteristic	R	F	7.1.1.3	1 = Voice 2 = Video	MG	CCA MGC
Bandwidth Reservation	R	V	7.1.1.4	Used to indicate the rate (in kbps/sec) that is reserved for this session (e.g., a voice call or a Video session may have a fixed amount of bandwidth).	MGC	CCA AGW
Service Level Priority	R	F	3.3.7.14	Value used to indicate the service level of the call	MGC	CCA AGW

The fifth column, Population Summary, does not necessarily preclude the vendor from using the CCA as the sole source of the data elements and have all other functional elements provide data to the CCA for population in the PDUs sent to the BA. The data elements in the PDU need to arrive at the BA to generate an accurate, timely, and verifiable CDR. The choice of the particular method to get the data elements to the BA is left to the vendor.

NOTE: For a field that has been designated as conditionally required, the field should be populated with the appropriate data if that data is available and applicable to the call. For example, if a call originates from the PSTN and terminates into the VoIP network, the MGC would be used in completing this call. This means that information (e.g., the Ingress Trunk Group number) would be available. Since the Data Set field for the Ingress Trunk Group number is required, that field should be populated with the trunk group number.

5.3.2.19.1.1 Call Connect Data Set

Table 5.3.2.19-1, Call Connect Data Set Information, provides the formatting and fields for the Call Connect Data Set.

[Objective] For every call attempt, call completion, and transiting call detected by the CCA, the CCA and any other functional entities (if applicable) shall provide information to properly populate the Call Connect Data Set following the rules outlined in Table 5.3.2-56, Call Connect Data Set Information.

5.3.2.19.1.2 Originating Customer/Business Group Identification

The Originating Customer/Business Group identification identifier is a 10-digit value that identifies the Customer or Business Group associated with a service. This ID is usually provided through some service application or some database. If this is available, it will be populated in the Originating Customer/Business Group Identification field.

[Objective] If an Originating Customer/Business Group Identification number is available, it will be populated in the Originating Customer/Business Group Identification field.

5.3.2.19.1.3 Terminating Customer/Business Group Identification

The Terminating Customer/Business Group Identification identifier is a 10-digit value that identifies the customer or business group associated with a service. This ID is usually provided through some service application or some database. If this is available, it will be populated in the Terminating Customer/Business Group Identification field.

[Objective] If a Terminating Customer/Business Group Identification number is available, it will be populated in the Terminating Customer/Business Group Identification field.

5.3.2.19.1.4 Call Characteristic

The Call Characteristic identifies how a particular call is set up. For example, the Call Characteristic will identify whether the call is a voice call or a video call.

[Objective] The Call Characteristic field will be populated with a value of one (1) to indicate that this particular data set represents a Voice call.

[Objective] The Call Characteristic field will be populated with a value of two (2) to indicate that this particular data set represents a Video session.

5.3.2.19.1.5 Bandwidth Reservation

On VoIP voice calls or calls that use video calls, there is a need to record the bandwidth that is allocated for the type of service call. This information can be used for maintenance or for projections on future usage and growth. This field bandwidth is measured in units of kbps.

[Objective] The Bandwidth Reservation field will be populated with the amount of bandwidth reserved in kbps.

5.3.2.19.1.6 Call Disconnect Data Set

Table 5.3.2.19-2, Call Disconnect Data Set, provides the formatting and fields for the Call Disconnect Data Set.

Table 5.3.2.19-2. Call Disconnect Data Set

USAGE DATA ELEMENT	REQUIRED/ OPTIONAL	FIXED/ VARIABLE	REFERENCE SECTION IN GR-3058-CORE	POPULATION SUMMARY	PRI	SEC
Call Event Type	R	F	3.3.6.1	1 = Call Completion 2 = Call Disconnect 3 = Call Attempt	CCA	MG MGC
Correlation ID	R	F	3.3.6.2	UUID = 128 bits (Variable depending on implementation) Unique value for each call composed of: 1. Network Component Network Appliance Id 2. Timestamp 3. Random Number	CCA	MG MGC
Element Identifier	R	F	3.3.6.3	Range of 000001 through 999999	CCA	MG MGC
Directional Indicator	R	F	3.3.6.4	1 = Egress (originating) 2 = Ingress (terminating) 3 = Transiting (MGC) 4 = Intra-gateway (AGW)	CCA	MG MGC
Service Type	R	F	3.3.7.5	1 = No CS-PSTN Interface 2 = Interface to CS-PSTN (via MGC)	CCA	MG MGC
Timing Guard	R	F	3.3.7.1	0 = no timing irregularities detected 2 = timing irregularities detected	CCA	MG
Disconnect Detection Date Disconnect Detection Time	R	F	3.3.7.4	MMDDYYYY – Month, Day, and Full Year HHMMSSms – Hours, Minutes, Seconds, and Milliseconds (depending on implementation).	CCA	MG MGC
Release Cause	R	V	3.3.8.6	Variable – See Table 3-6 for examples	CCA	MG MGC

[Objective] For every call disconnect detected by the CCA, the CCA and any other network appliances (if applicable) shall provide information to properly populate the Call Connect Data Set following the rules outlined in Table 5.3.2.19-2, Call Disconnect Data Set.

5.3.2.19.1.7 Billing Agent

The functions of the BA are to provide processing, formatting, storage, and outputting of usage records for delivery to downstream processing systems. In the VoIP product design, it may be so the functional entities (e.g., CCA, MGC) of a network appliance are responsible for generating the call data and transmitting this data to the BA in the form of a data set or through the network appliance's internal means of communication and data sharing (assuming all these functional entities are internally connected). It is then up to the BA to gather all the accounting data and process it to determine the proper recording format.

The BA may be a separate entity within a network; or, it may be internally connected to the other functional entities within a network appliance. In either case, the BA should be able to process, format, store, and output generated usage records based on either the data sets or the accounting data that it will receive. If the network uses data sets as defined in Section 5.3.2.19.1, Accounting Data, the Dependent Requirements in Section 5.3.2.19.2.1, Call Data, and the requirements in the rest of Section 5.3.2.19.2.2, Record Format, shall apply. Otherwise, only the requirements in Section 5.3.2.19.2.2, Record Format, shall apply.

5.3.2.19.2 Processing of Data Sets

To process data sets, the BA must have the capability to match and correlate multiple data sets (generated from multiple functional entities) that are associated with the same call. In addition, a Call Connect Data Set will often have a corresponding Call Disconnect Data Set that will be delivered at one point or another. The BA must be able to correlate these sets of records together. The ability to correlate all these data sets is made possible by the use of the Correlation ID. Telcordia Technologies GR-3058-CORE has additional information about the format and use of the Correlation ID.

As the BA processes the data sets, it assembles the call data from the various data sets, formats it into an appropriate record, and stores it in the appropriate format. Processing of assembled call data for a particular call is activated immediately upon receipt of the Call Disconnect Data Set for that call. The following requirements are taken from Telcordia Technologies GR-3058-CORE, and they pertain to the processing and assembling of the call data:

1. **[Objective]** The BA shall activate usage assembly within 250 ms of receiving a disconnect Data Set from the network component network appliances.

2. **[Objective]** The BA shall correlate all usage measurements related to a single VoIP call to produce the appropriate usage record(s).

5.3.2.19.2.1 Call Data

Regardless of the recording format that is chosen, there is information that is important for proper billing and accounting. Also, there is information that may be necessary for one type of call, but may not be necessary for another type of call. The following requirement lists the call data that are needed in the recording. (Of course, there are other call data that are also desired and should be captured in the record; however, the data items listed in the following requirement are the call data that *must* be provided.):

[Required] For the selected recording format that is chosen, of all the call information that will be provided, the following call data shall be provided in the record data:

1. Host Name of the CCA controlling the call processing.

2. Start Date of call (In Julian or Calendar).

3. Start Time of Call (Hour + Minute + Second).

4. Elapsed Time of Call and/or Stop Time of call.

5. Calling Number.

6. Called Number (included all dialed digits).

7. **[Conditional]** Call Answered/Unanswered Indicator.

8. Precedence level of call. (NOTE: This may be accomplished either by a specific precedence level designation field in the call, or by providing the dialed precedence level access digits in the called number field.)

9. **[Conditional]** Indication of either a VoIP or Video over IP “call.”

10. **[Conditional]** Indication of the assigned bandwidth for the entire duration of the Video over IP “call.”

[Required] For the selected recording format that is chosen, of all the call information that will be provided, the following call data shall be provided in the record data if it applies to the call:

1. **[Required]** Conference Call Indicator.

2. **[Conditional]** Customer/Business Group Identification.

The Conference Call Indicator is used to identify callers that are participants in a conference call. This will be useful for tracking purposes, or if there is special billing associated for conference calls.

For Customer/Business Group identification, the originating party (or even the terminating party) may be part of a customer or business group. Special billing or charges may apply to a member of a particular group; thus, for calls where the originating party and/or terminating party is assigned a Customer/Business Group Identification, the Customer/Business Group Identification information should be provided in the CDR as per the previous requirement.

The following subsections describe the types of VoIP calls (e.g., PSTN to IP, IP to PSTN), and provide additional call information that should be captured in the CDR.

5.3.2.19.2.1.1 Quality of Service

For VoIP calls, compression of voice traffic is used to conserve bandwidth. However, compression at one end and decompression at the other end usually results in a degradation of voice quality. Since stronger compression usually results in further degradation of voice quality, service providers need to find a balance between the two. To determine if the voice quality is sufficient to warrant the level of compression, there needs to be some means by which the quality of the call can be measured.

The “product” in the requirements below is the combination of the LSC, MFSS, or WAN SS, and the set of PEIs and AEIs that it serves.

[Required: LSC, MFSS, WAN SS, 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 LSC, MFSS, or WAN SS 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 in accordance with TIA TSB-116-A.

NOTE: This requirement is only related to VoIP EIs and is not applicable to MGs. For AEIs, the information will be transmitted at the completion of a session to the CCA.

[Required: LSC, MFSS, WAN SS, 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 TCLw. (Definitions of latency and packet loss are found in Appendix A, Definitions, Abbreviations and Acronyms, and References, and the methods of calculation are described in Section 5.3.3, Network Infrastructure End-to-End Performance Requirements.) For AEIs, the information will be transmitted at the completion of a session to the CCA.

[Required: LSC, MFSS, WAN SS, AEI] The product shall provide the jitter for the session. (See Appendix A, Definitions, Abbreviations and Acronyms, and References, for the definition of jitter. The method of calculation is described in Section 5.3.3, Network Infrastructure End-to-

End Performance Requirements.) For AEIs, the information will be transmitted at the completion of a session to the CCA.

For example, at the end of an EI Voice session, the EI can generate an initial voice quality record that contains the latency, packet loss, Ie, TCLw, and jitter values, but not the R-factor. The EI can use the Voice media packets that it sent and received over the duration of the Voice session to compute these values. The EI can send this initial Voice quality record to its LSC, MFSS, or WAN SS as part of the EI signaling that ends the Voice session.

The LSC, MFSS, or WAN SS can use this initial Voice quality record to calculate the R-Factor for the session. The LSC, MFSS, or WAN SS can generate a final voice quality record containing the latency, packet loss, Ie, TCLw, and jitter values received from the EI, and the R-Factor that it calculated. Then the LSC, MFSS, or WAN SS can generate a CDR for the session that contains the final Voice quality record.

This example shows how the EI and LSC/MFSS/WAN SS can jointly generate the Voice quality record and the CDR, and meet the previous product requirements.

[Required: LSC, MFSS, WAN SS] 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.

5.3.2.19.2.1.2 VoIP to PSTN

VoIP to PSTN calls refers to calls routed to the PSTN from a VoIP network. An example of this is a call that originates in the VoIP network and uses the PSTN to complete the call. Another example could be a call that originates from another network (be it a PSTN or another VoIP network), enters this VoIP network, and transits out to the PSTN.

For the transiting case, there may be two CDRs generated. One CDR would represent the incoming call into the VoIP network, and the other CDR would represent the outgoing call to the PSTN. For information on what call data to capture for the incoming portion of the call, please refer to Section 5.3.2.19.2.1.3, PSTN to VoIP, for incoming calls from the PSTN, and Section 5.3.2.19.2.1.4, VoIP to VoIP, for calls incoming from a VoIP network.

When a call originates in the VoIP network and continues into the PSTN for completion, there is certain information related to the PSTN that should be captured in the CDR, which is generated in the VoIP network. The following requirement indicates the specific call information:

1. **[Required]** In addition to the call data specified previously, the following call data must be provided in the record data for calls that are routed to the PSTN from the VoIP network:

a. IP address of originating subscriber (if the call originated from the subscriber on the VoIP network).

b. IP address of the gateway connecting to the PSTN.

c. Outgoing trunk group of the call.

d. Outgoing trunk group member of the call.

In the PSTN environment, calls are routed from one network to another via a trunk. A trunk group is a group of trunks and is normally identified by a specific number. Similarly, a member of a trunk group is identified by another specific number. Identification of these trunk groups and trunk group members may be important for billing purposes (depending on the tariffs agreed upon between the VoIP service providers and the PSTN service providers), as well as for troubleshooting purposes.

5.3.2.19.2.1.3 PSTN to VoIP

PSTN to VoIP refers to the type of call where the call that originates in the PSTN network enters the VoIP network for completion. An example of this would be a call that originates from the PSTN network and terminates to a subscriber in the VoIP network. Another example would be a call from the PSTN that enters the VoIP network, but transits to another VoIP network or back out to the PSTN. For these cases, there may be two separate CDRs. One CDR would represent the incoming call into the VoIP network, and another CDR would represent the call outgoing to the PSTN or to another VoIP network.

This section addresses the incoming part of the call to the VoIP network. For the call data related to the outgoing part of the call, refer to Section 5.3.2.19.2.1.2, VoIP to PSTN, for calls to the PSTN, and to Section 5.3.2.19.2.1.4, VoIP to VoIP, for calls to another VoIP network.

As was the case for VoIP to PSTN scenario calls, there is certain information related to the PSTN that should be captured in the CDR that is generated in the VoIP network. The following requirement indicates the specific call information:

1. **[Required]** In addition to the call data specified above, the following call data must be provided in the record data for calls that are routed from the PSTN to the VoIP network:

   a. IP address of terminating subscriber (if the call terminates to a subscriber on the VoIP network).

   b. IP address of the gateway connecting to the PSTN.

c. Incoming trunk group of the call.

d. Incoming trunk group member of the call.

In the PSTN environment, calls are routed from one network to another network via a trunk. A trunk group is a group of trunks and is identified by a specific number. Similarly, a member of a trunk group is identified by a specific number. Identification of these trunk groups and trunk group members may be important for billing purposes (depending on the tariffs agreed upon between the VoIP service providers and the PSTN service providers) as well as for troubleshooting purposes.

5.3.2.19.2.1.4 VoIP to VoIP

A VoIP to VoIP call can be one of the following three basic scenarios:

1. Subscriber in this VoIP network originates a call to another VoIP network.

2. Subscriber in this VoIP network originates a call and terminates in the same VoIP network.

3. Call from another VoIP network that terminates a call to a subscriber that belongs in this VoIP network.

The first scenario could result in a CDR that captures originating type information. The second scenario could result in a CDR that captures terminating type information. Finally, the third scenario could result in two separate CDRs (i.e., one for originating, and another for terminating), or one CDR that captures both the originating and terminating information.

The next requirement identifies the call information that should be captured in the CDR that is generated for the originating call.

1. **[Required]** In addition to the call data specified previously, the following call data must be provided in the record data for calls that originate from the 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)

The following requirement identifies the call information that should be captured in the CDR that is generated for incoming calls from another VoIP network:

1. **[Required]** In addition to the call data specified previously, the following call data must be provided in the record data for calls that originate in one VoIP network, and terminate in another VoIP network:

    a. IP address of terminating subscriber
    b. IP address of the gateway connecting to the other VoIP network (if applicable)

For the third scenario, if there are two separate CDRs generated, one CDR would represent the originating part of the call, and the other CDR would represent the terminating part of the call. In this case, the originating CDR would contain the same call information as required previously for calls that originate in the VoIP network. The terminating CDR would contain the same call information as defined previously for calls that terminate in the VoIP network.

However, if the third scenario resulted in one CDR to capture both the originating and terminating information of the call, then the following requirement identifies the call information that should be captured in that singular CDR:

1. **[Required]** In addition to the call data specified previously, the following call data must be provided in the CDR (that captures both the originating and terminating information) for calls that originate from the VoIP network and terminate within the same VoIP network:

    a. IP address of originating subscriber
    b. IP address of terminating subscriber

5.3.2.19.2.2 Record Format

The actual format of the CDRs that the BA will create (either based on the call data acquired from the processing and assembly of the data sets, or through internal call data sharing between functional entities) will be the format that is agreed upon between the DoD Network and the vendors of the BA. If the agreed upon format is Bellcore AMA Format (BAF), then the requirements in Telcordia Technologies GR-3058-CORE on the use of BAF will apply. For further information on the use of BAF, please refer to GR-3058-CORE, Section 4.3. The following subsections provide some of the basic formatting found in GR-3058-CORE.

[Objective] If BAF is chosen as the Call Detail Recording format, the BAF requirements in GR-3058-CORE shall apply, with the noted exception in the following subsections.

5.3.2.19.2.2.1 BAF Structure 0625

Originating and terminating calls (whether they are voice or video) that originate in another service provider’s network or terminate in another service provider’s network, or calls that use the PSTN, would result in a Structure Code 0625.

Structure Code 0625 is used to capture the call information for

- Calls that originate from the VoIP network and terminate in the PSTN,
- Calls that originate from the PSTN and terminate in the VoIP network, and
- Calls that both originate and terminate within the VoIP network.

Table 5.3.2.19-3, BAF Structure 0625 and Field Populations, shows the format of Structure Code 0625 and the requirements on the field population. Further details on field population can be found in Telcordia Technologies GR-3058-CORE.

Table 5.3.2.19-3. BAF Structure 0625 and Field Populations

FIELDS OF THE STRUCTURE	REFERENCE SECTION IN GR-3058-CORE	BAF TABLE	POPULATION SUMMARY
Record Descriptor Word	4.3.3.1	000	Populate as described in GR-1100-CORE
Hexadecimal Identifier	4.3.3.2	00	Populate as described in GR-1100-CORE
Structure Code	4.3.3.3	0	00625 if no Module Codes are appended to this Structure 40625 if Module Codes are appended to this Structure
Call Type	4.3.6 4.3.7 4.3.8 4.3.9 4.3.15	1	Use the following: 110 = Originating Access Service 119 = Terminating Access Service 589 = Originating Connecting Network Access Service 720 = Terminating Connecting Network Access Service 060 = Basic Long Distance Service - Ingress 529 = VoIP Unidentified Call
Sensor Type	4.3.3.4	2	Sensor Type value associated with the network appliance
Sensor Identification	4.3.3.5	3	Populate Character 1 as described in GR-1100-CORE. Populate Characters 2-7 with the value of the Element Identifier in the Element Identifier usage element of the network component that is identified in the Sensor Type.
Recording Office Type	4.3.3.6	4	Value assigned for the specific network appliance that contains the BA functionality that generated this record.

FIELDS OF THE STRUCTURE	REFERENCE SECTION IN GR-3058-CORE	BAF TABLE	POPULATION SUMMARY
Recording Office Identification	4.3.3.7	5	Populate Character 1 as described in GR-1100-CORE. Populate Characters 2-7 with the value of the Recording Office ID.
Connect Date	4.3.3.8	6	Populate Character 1 with the least significant digit of the year represented in the date the connection is made by the customer. Populate Characters 2-3 with the month represented in the date the connection is made by the customer. Populate Characters 4-5 with the day represented in the date the connection is made by the customer.
Timing Indicator	4.3.3.9	7	If timing irregularities have been detected, the BA shall populate Timing Indicator (Table 7) to indicate that a Timing Guard condition exists.

FIELDS OF THE STRUCTURE	REFERENCE SECTION IN GR-3058-CORE	BAF TABLE	POPULATION SUMMARY
Study Indicator	4.3.3.10	8	Populate Characters 1 through 4 with the value of the Study/Test Indicator usage element. Populate Character 5 with 0. Populate Character 6 as follows: — with 0, if complete originating and terminating numbers were received — with 1, if an all-zero originating number and a non-all-zero terminating number were received — with 3, if an all-zero terminating number and a non-all-zero originating number were received — with 4, if an all-zero originating number and an all-zero terminating number were received — with 5, if a terminating number with an all-zero station number and an originating number with a non-all-zero station number were received — with 6, if an originating number with an all-zero station number and a terminating number with a non-all-zero station number were received — with 7, if a terminating number with an all-zero station number and an originating number with an all-zero station number were received. Populate Character 7 with 0.
Called Party Off-Hook Indicator	4.3.3.11	9	Populate Called Party Off-Hook (Answer) Indicator (Table 9) with 0, if call was completed, and 1, if call was not completed.
Service Observed/Traffic Sampled	4.3.3.12	10	Populate Service-Observed/Traffic-Sampled Indicator (Table 10) with the “default” value per GR-1100-CORE.
Operator Action	4.3.3.13	11	Populate Operator Action (Table 11) to indicate no operator involvement per GR-1100-CORE.
Service Feature	4.3.3.14	12	Populate Service Feature Code (Table 12) with the value in Table 12 of GR-1100-CORE that maps to the service that applies to the call (e.g., 012 for Call Forwarding, 056 = Call Waiting, 605 = Call Hold, 160 = Call Transfer, etc.)

FIELDS OF THE STRUCTURE	REFERENCE SECTION IN GR-3058-CORE	BAF TABLE	POPULATION SUMMARY
Originating NPA	4.3.3.15 4.3.9	13	Populate Originating NPA (Table 13) as follows: — NPA of the ANI (Charge Number) if non-zero; otherwise, use the NPA of the Calling Station Id. This is when the ANI (or the CPN if ANI is not available) is 10 or less digits. — Per fill procedures described in GR-1100-CORE if the ANI (or CPN if ANI is not available) is 11 digits or higher. See the section related to Ingress Trunk Group Billing Number in GR-3058-CORE when using the Ingress Trunk Group Billing Number usage element.
Originating Number	4.3.3.16 4.3.9	14	Populate Originating Number (Table 14) as follows: — NXX-XXXX of the ANI if non-zero; otherwise, use the CPN (this is when ANI (or CPN if ANI is not available) is 10 digits or less]. — Per fill procedures described in GR-1100-CORE if the ANI (or CPN if ANI is not available) is 11 digits or higher. See the section related to Ingress Trunk Group number in GR-3058-CORE when using the Ingress Trunk Group
Overseas (International Call) Indicator	4.3.3.17	15	Populate Overseas Indicator (Table 15) with the value: 0 = North America World Zone 1. 1 = International (01 or 011 prefix dialed).
Terminating NPA	4.3.3.18	16	Populate Terminating NPA (Table 16) as follows: — If the value is 12 digits or less, the Called Station Id as per GR-1100-CORE — per fill, procedures described in GR-1100-CORE if the Called Station Id is 13 digits or more.

FIELDS OF THE STRUCTURE	REFERENCE SECTION IN GR-3058-CORE	BAF TABLE	POPULATION SUMMARY
Terminating Number	4.3.3.19	17	Populate Terminating Number (Table 17) as follows: — If the value is 12 digits or less, the Called Station Id as per GR-1100-CORE. — Per fill procedures described in GR-1100-CORE if the Called Station Id is 13 digits or more.
Connect Time	4.3.3.20	18	Populate Characters 1-2 with the hour represented in the rounded value of the Customer Connect Time or Circuit Seizure Time usage element. Populate Characters 3-4 with the minute represented in the rounded value of the Customer Connect Time or Circuit Seizure Time usage element. Populate Characters 5-6 with the second represented in the rounded value of the Customer Connect Time or Circuit Seizure Time usage element. Populate Character 7 with the tenth-of-second represented in the rounded value of the Customer Connect Time or Circuit Seizure Time usage element.
Elapsed Time	4.3.3.21	19	Populate Character 1 with 0. Populate Characters 2-6 with the number of minutes of the rounded value of the customer-elapsed time of the call. Populate Characters 7-8 with the number of seconds of the rounded value of the customer-elapsed time of the call. Populate Character 9 with the number of tenths-of-seconds of the rounded value of the customer-elapsed time of the call.
IC/INC Prefix	4.3.6.1	57	Populate Characters 1-4 with the value of the CIC that was used in the call. If there is no CIC available, then the fill procedure in GR-1100-CORE shall be implemented. Populate Character 5 with the value of: 0 if operator was involved 1 if operator was not involved.

FIELDS OF THE STRUCTURE	REFERENCE SECTION IN GR-3058-CORE	BAF TABLE	POPULATION SUMMARY
Carrier Connect Date	4.3.6.2	6	Populate Character 1 with the least significant digit of the year represented in the date the call attempt is made by the customer. Populate Characters 2-3 with the month represented in the date the call attempt is made by the customer. Populate Characters 4-5 with the day represented in the date the call attempt is made by the customer.
Carrier Connect Time	4.3.6.3	18	Populate Characters 1-2 with the hour represented in the rounded value of the call attempt time or Circuit Seizure Time usage element. Populate Characters 3-4 with the minute represented in the rounded value of the call attempt time or Circuit Seizure Time usage element. Populate Characters 5-6 with the second represented in the rounded value of the call attempt time or Circuit Seizure Time usage element. Populate Character 7 with the tenth-of-second represented in the rounded value of the call attempt time or Circuit Seizure Time usage element.
Carrier Elapsed Time	4.3.6.4	19	Populate Character 1 with 0. Populate Characters 2-6 with the number of minutes of the rounded value of the carrier-elapsed time of the call. Populate Characters 7-8 with the number of seconds of the rounded value of the carrier-elapsed time of the call. Populate Character 9 with the number of tenths-of-seconds of the rounded value of the carrier-elapsed time of the call.
IC/INC Call Event Status	4.3.6.5	58	Populate as follows: — If the call has been completed, the BA shall populate BAF Table 58 with the value = 010. — If the call has been attempted, but not completed, the BA shall populate BAF Table 58 with the value = 007.

FIELDS OF THE STRUCTURE	REFERENCE SECTION IN GR-3058-CORE	BAF TABLE	POPULATION SUMMARY
Trunk Group Number	4.3.6.6	83	Populate Character 1 with the value = 9 to indicate Signaling type not specified. Populate Characters 2-5 with the value of the Trunk Group Number. If there is no Trunk Group Number available, this table should use the BAF fill procedure (e.g., Hex-F).
Routing Indicator	4.3.6.7	59	If the call involved the PSTN, this table shall be populated with the value - 0 = if the call was direct to the PSTN - 1 = if the call was Tandem. Otherwise, the BAF fill procedure should be used for this table (e.g., Hex-F).
Dialing and Presubscription Indicator	4.3.6.8	85	Used to indicate whether the calling party dialed a Carrier Access Code. The BA shall populate Table 85 with the values that best match the dialing pattern as per GR-1100-CORE.
ANI/CPN Indicator	4.3.6.9	60	Populate as per - 0 = Neither ANI nor CPN was provided in the signaling. - 1 = Only ANI was provided in the signaling. - 2 = Only CPN was provided in the signaling. - 3 = Both ANI and CPN were provided in the signaling.

[Objective] The BA shall generate BAF Structure 0625 and populate the fields as per Table 5.3.2.19-1, BAF Structure 0625 and Field Populations, for the following types of calls:

- Calls that terminate into another service provider’s network
- Calls that originated from another service provider’s network
- Calls that used the PSTN
- IP calls that cannot be identified

Toll-free calls are calls that are placed to toll-free numbers (in the format 8YY-NXX-XXXX, where YY = 88, 77, 66). They will cause the CCA to launch a query to the toll-free database to determine how to transport the call. In the requirements in this section, it is assumed that an IN/1 query/response format is used to follow the requirements found in Telcordia Technologies GR-533-CORE.

However, it is assumed that the DISN voice network will not be providing toll-free queries using the IN/1 query/response; instead, it will be sending the calls to toll-free numbers to the PSTN to determine the final routing information. Calls to toll-free numbers should generate Structure Code 0625 as if the toll-free number was a typical, normally dialed number.

5.3.2.19.2.2.1.1 Precedence Level of a Call

As identified in the previous section, one of the required items to be provided in an Automatic Message Accounting (AMA) record is the precedence level of the call. The precedence level can be identified in one of two ways: 1) a specific Precedence Level Designation field in the call, and 2) providing the dialed precedence level access digits in the called number field.

If the first method is used to identify the precedence level, then this information can be contained in Module Code 616.

[Objective] Module Code 616 shall be used to capture the precedence level if there is a specific Precedence Level Designation field in the call. In Module Code 043,

1. Table 569 will be populated with the value that indicates the precedence level of a call in Characters 1-2, and Character 3 will give the number of significant digits in Table 803.

2. Table 803 will be populated with either the precedence level designation or the dialed precedence level access digits.

5.3.2.19.2.2.2 VoIP/Video over IP

[Objective] In the VoIP environment, a call can be a VoIP or a Video over IP. For Video over IP calls, the BA would append Module Code 610 to BAF Structure 0625 and populate it as per the following dependent requirements.

[Objective] Module Code 204 shall be used to indicate that the BAF record represents a Video over IP “call.” As such, BAF Table 610 of Module Code 204 shall be populated with a value specified in Telcordia Technologies GR-1100-CORE that indicates a Video call.

For Video calls, the BA may have the option of appending Module Code 611, which will identify the assigned bandwidth of the Video call.

[Objective] The BA may have an option to provide an indication in the AMA record that will identify the assigned bandwidth of a Video call.

[Objective] If the call is a Video call, then the BA shall append Module Code 611 to indicate the assigned bandwidth of the Video call. The BA shall populate

1. BAF Table 237 of Module Code 611 with a value code specified in Telcordia Technologies GR-1100-CORE that indicates the assigned bandwidth values.

2. BAF Table 126 of Module Code 611 with the corresponding assigned bandwidth value code.

5.3.2.19.2.2.3 Customer/Business Group Identification

It may be necessary to capture the Customer/Business Group Identification information related to a call. Module Code 027 should be used to capture this information.

[Objective] Module Code 027 shall be used to capture the Customer/Business Group Identification. In Module Code 027, Table 87 shall be populated according to Telcordia Technologies GR-1100-CORE.

5.3.2.19.2.2.4 BAF Structure 0588

BAF Structure 0588 is used to capture the usage information (e.g., the name of the service provided) when a service is activated, deactivated, or has an instance of use by the SA. Additional information on the generation and population rules can be found in Telcordia Technologies GR-3058-CORE.

[Objective] If a functional entity equivalent to the SA has usage information to be recorded, the BA shall generate BAF Structure 0588 according to the requirements defined in Telcordia Technologies GR-3058-CORE. The population of BAF Structure 0588 shall follow the population requirements in GR-3058-CORE.

5.3.2.19.2.2.5 BAF Structure 9000

If there is a need to generate AMA records for time changes (e.g., Daylight savings), then the BA should use BAF Structure 9000.

[Objective] If there is a need to record time changes, the BA shall generate BAF Structure 9000. The population of BAF Structure 9000 shall follow the population requirements in Telcordia Technologies GR-3058-CORE.

5.3.2.19.2.3 Storage

Once the BA has generated the call records of a chosen format, it may need to retain or store those records until it is time to provide them to the downstream processing. Normally, these records are stored together as files and wait to be transported for downstream processing. The process of transporting or sending the records to downstream processing systems is left to be agreed upon between the DoD and the vendors.

While in retention, additional CDRs may accumulate in this storage area. The BA must have enough storage capacity to store a reasonable quantity of CDRs. In addition, the storage device must be non-volatile, so the CDRs are protected from power disturbances and other transient conditions.

[Required] The mass storage in the BA must be non-volatile.

[Required] The mass storage in the BA must be able to retain at least five average-busy-season business days of AMA data. (NOTE: This is needed to provide adequate capacity for high-volume storage of CDRs.)

5.3.2.19.2.4 Outputting Records

Once the BA has the records stored in files, these files, at some time, will need to be outputted for downstream processing. Outputting the call records is the process of delivering those files to a processing center within the network that specializes in processing the record for billing and accounting purposes. Electronic transfer of those records would provide the most convenient method of transfer. However, electronic transfer must have security measures to prevent unauthorized access to the record during transfer. One security measure is to transfer the file over a secured protocol, such as SSHv2.

[Required] The BA should be able to output the records electronically over a secured connection.

NOTE: This is needed to allow transfer of CDRs from one location to another in a secure manner (e.g., to prevent intruder detection, theft, and/or manipulation of CDRs).

In addition to electronic transfer, it may become necessary to transfer the records to a physical media that is also removable, such as a tape or CD. Such situations may include a third party that requires access to the records, but an electronic transfer to that third party is not an option. Thus, the following requirement should apply.

[Required] The BA should have the ability to transfer the records to a physical storage media that is also removable.

NOTE: This is needed to allow manual transfer of CDRs from one location to another in the case where automated electronic transfer is not available (e.g., there is an IP network outage between the CDR source and the CDR destination).

5.3.2.20 RTS Stateful Firewall Requirements

5.3.2.20.1 Introduction

The specifications for an RTS Stateful Firewall (RSF) are being added to Change 1 of UCR 2008. The use of the RSF was discussed in the UCR 2008 that was signed in January 2009. For example, the placement of the RSF within the local area network topology was displayed in Figure 5.4.5-2, Notional Example of Voice, Video, Softphone, Videophone, and Data ASLAN Segmentation. However, the RSF requirements were not specified. The purpose of this section is to add these requirements as part of Change 1.

5.3.2.20.2 Role of the RSF

The UCR 2008 contains the specifications for a voice and video firewall called an EBC. The EBC is placed at the edge of the enclave B/P/C/S and sits between the LANs and the WAN. The EBC protects voice and video devices from attacks that originate outside of the enclave. The EBC requirements are presented in Section 5.3.2.15, EBC Requirements.

The role of the RSF is to protect an LSC, SS, or MFSS from attacks that originate from inside of the enclave. JITC has validated that LSCs, SSs, and MFSSs have acceptable Information Assurance risks for most deployments. Therefore, the use of the RSF is not a mandatory requirement. However, some sites may determine that additional protection is required because of the risks associated with their unique scenario. When this occurs, the RSF may be deployed to provide additional protection.

The RSF is considered an appliance. Appliances are described in UCR 2008 Section 4.4.1.2 (Relationship between SBU UC System Description and Products to be Tested for APL Certification). Appliances are part of UC APL products, which are also called SUTs. The RSF is part of the LSC SUT, the SS SUT, and the MFSS SUT.

5.3.2.20.3 Detailed RSF Requirements

5.3.2.20.3.1 RSF General Requirements

1. **[Required: RSF]** The RSF shall meet all EBC requirements with the exception of the requirements specified in Section 5.3.2.20.3.2, RSF Shall Not Requirements.

2. **[Required: RSF]** The RSF shall maintain a persistent TLS session with the EBC within the RSF’s enclave. Persistent means that the TLS session is established when the RSF system joins the signaling network and is not established on a VVoIP/AS-SIP session-by-session basis.

3. **[Required: RSF]** The RSF shall fulfill the same availability requirements as the LSC that the RSF is protecting. If the LSC's availability requirement is 99.999, then the RSF's availability requirement is also 99.999.

NOTE: With a few exceptions, the RSF and the EBC perform the same functions. The functions performed by the RSF are a very large subset of the functions performed by the EBC. These functions are performed by the same hardware and software on both the RSF and the EBC. Although the software is the same, the RSF's software configuration is a little different from the EBC's software configuration.

The hardware configuration used at a specific site is determined by the site's specific availability requirements, as defined in Section 5.3.2.15.6, Availability. At a specific site, both the RSF and the EBC 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 RSF and the EBC is not required.

The EBC functions that the RSF shall not perform are presented in Section 5.3.2.20.2, Role of the RSF. Because the RSF is part of the LSC, SS, or MFSS SUT, the RSF shall not participate in the softswitch failover process and shall not perform NAT/NAPT.

5.3.2.20.3.2 RSF Shall Not Requirements

1. **[Shall Not: RSF]** The RSF shall not take any corrective actions upon the LSC failover from the primary softswitch to the secondary softswitch. The EBC-required actions upon failover from the primary softswitch to the secondary softswitch are described in Sections 5.3.2.3.2.6-2b and 3b. The RSF shall not perform these actions.

2. **[Shall Not: RSF]** The RSF 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 EBC requirements for bidirectionally anchoring the media are described in Sections 5.3.2.15.1-1a, 1b, and 1c. The RSF shall not perform these actions.

3. **[Shall Not: RSF]** The RSF shall not maintain a persistent TLS session with EBCs that are outside of the RSF's enclave. The EBC's requirements for maintaining persistent TLS connections with EBCs that are outside of the local enclave are described in Sections 5.3.2.15.1-6a and 6b. The RSF shall not perform these actions.

5.3.2.21 V.150.1 Modem Relay Secure Phone Support Requirements

This section provides an architecture and requirements for "V.150.1 Modem Relay Secure Phone Support," to ensure that RTS MGs can support SCIP-based secure phones for all scenarios required by the NSA.

V.150.1 Secure Phone Support relies on

- SCIP-216 Modem Relay capabilities in RTS MGs, TAs, and IADs
- SCIP-215 Modem Relay capabilities in RTS SEI.

V.150.1 is an ITU Recommendation that describes different methods for carrying Modem traffic over IP networks. SCIP-215 and SCIP-216 are the NSA's technical documents on "V.150.1 Minimum Essential Requirements (MER) for VoIP Gateways" and "V.150.1 MER for VoIP Secure Phones," respectively.

V.150.1 supports three different methods or modes for carrying modem traffic over IP networks:

- Audio (commonly known as Modem Pass-Through),
- Voice Band Data, and
- Modem Relay.

The SCIP-216 and SCIP-215 requirements are added here to improve support for calls between secure DoD SCIP phones in DISA's RTS Network.

The UCR 2008 allows an analog SCIP phone on the DSN or the PSTN to call an IP SCIP phone on the RTS network, and allows an IP SCIP phone on RTS to call an analog SCIP phone on the DSN or the PSTN. The UCR 2008 does not provide AS-SIP requirements for carrying SCIP calls from one RTS LSC to another, and does not provide Modem Relay features in TA, IADs, and MG line cards that support analog SCIP phones on RTS.

The UCR, 2008 Change 1, removes these two limitations by extending AS-SIP to carry SCIP calls between LSCs, and by adding Modem Relay features to TAs, IAD, and MG line cards that support analog SCIP phones.

5.3.2.21.1 Modem Relay for Secure Phone Support

5.3.2.21.1.1 Need for Modem Relay Requirements

The UCR 2008 supports TAs, IADs, and MGs that support voice calls and modem passthrough (audio) calls using the G.711 uncompressed, G.723 compressed, and G.729 compressed VoIP codecs. The UCR 2008 also contains high-level requirements for the LSC and MFSS MG (for trunk-side DSN and PSTN terminations only) that support SCIP Modem Relay per NSA SCIP-216, and commercial modem relay per ITU Recommendation V.150.1.

The MG trunk-side requirements for SCIP-216 are extended here to support SCIP calls fully on RTS in 2010-2011. The MG trunk-side requirements for V.150.1 also are extended here to better support commercial modem calls on RTS (e.g., V.90 and V.92 calls to/from 56k modems).

Terminal Adapter, IAD, and MG line-side requirements for SCIP-216 Modem Relay are added here to allow end users with analog SCIP phones to use these phones behind RTS TAs, IADs, and MG line-side connections (e.g., analog lines that interconnect analog SCIP phones with MG analog line cards via existing twisted-pair copper-wire plant on a B/P/C/S). Internet Protocol-capable SCIP phones (based on NSA SCIP-215) may be available to RTS users, but there is also a need to support analog SCIP phones behind RTS TAs, IADs, and the line sides of MGs using modem relay.

5.3.2.21.1.2 Architecture for Supporting SCIP/V.150.1 Modem Relay

The architecture change needed to support SCIP phones and V.150.1 is to add Modem Relay capabilities wherever modem passthrough (Audio) capabilities are already supported. This means that Modem Relay capabilities should be added to (or enhanced in) the following RTS NEs:

1. Media Gateway – Trunk Side (MG-TS) The portion of the MG that provides trunk-side connections to the DSN and the PSTN using ISDN PRI (Required in UCR 2008), DoD CCS7 (Conditional in UCR 2008), and CAS (Conditional in UCR 2008) Trunk Groups. Support for Modem Relay in the MG-TS is Required in UCR 2008 Change 1.

2. Media Gateway – Line Side (MG-LS) The portion of the MG that provides line-side connections to analog phones, analog secure phones, analog fax machines, and analog modems on the B/P/C/S, using analog line cards at the MG and the existing twisted-pair copper-wire plant at the B/P/C/S. Support for Modem Relay in the MG-LS is Conditional in UCR 2008 Change 1.

3. Analog Terminal Adapter (ATA) A device on the RTS end user's premise that supports interconnection between the ASLAN and the end user's analog phone, analog secure phone, analog fax machine, or analog modem. This device supports a single RJ-45 Ethernet interface on the ASLAN side and a single analog RJ-11 interface on the end user side. Support for Modem Relay in the ATA is Conditional in UCR 2008 Change 1.

4. Integrated Access Device (IAD) A device on the RTS end user's premise that supports interconnection between the ASLAN and multiple end user analog phones, analog secure phones, analog fax machines, and analog modems. This device supports a single Ethernet RJ-45 interface on the ASLAN side, and multiple (from 4 up to 16) analog RJ-11 interfaces on the end user side. Support for Modem Relay in the IAD is Conditional in UCR 2008 Change 1.

5. AS-SIP Components of the LSC and MFSS The LSC and MFSS CCAs need to be enhanced to support new AS-SIP and SDP signaling for modem relay calls. This is not an extensive change since it requires that SDP lines for the modem relay media type be added to existing SDP lines for the audio media type in AS-SIP INVITE, UPDATE, 180 Ringing, 183 Session Progress, 200 OK, and ACK messages, but it is a necessary change.

Modem relay capabilities do not need to be added to the following RTS network element:

- **Edge Boundary Controller (EBC)** The RTS EBCs only need to ensure the transparent passing of the V.150.1 Simple Packet Relay Transport (SPRT) and State Signaling Event (SSE) messages in modem relay media streams. This can be accomplished in RTS by having the modem relay endpoints (MGs, TAs, IADs, and IP SCIP Phones) make secure SCIP calls using the same UDP port and protocol numbers for the nonsecure portion of the call (which uses Secure RTP for media transfer) and the secure portion of the call (which uses SPRT and SSE for media transfer). Having the modem relay end points use the same UDP port and protocol numbers for the unsecure and secure portions of the call should make passing of modem relay SPRT and SSE messages transparent to RTS EBCs.

One other architecture change is the addition of Secure IP Phones to the RTS Network. (In UCR 2008, Secure IP Phones are supported on a vendor-proprietary basis; in UCR 2008, Change 1, Secure IP Phones are also supported on a multivendor-interoperable basis.) These Change 1 Secure IP Phones are SCIP-based, support both proprietary signaling and AS-SIP signaling for communication with LSCs, and support SCIP-215 (V.150.1 Modem Relay) media for communication with MGs, ATAs, IADs, EBCs, and other Secure IP Phones. Here, these Secure IP phones are also called IP SCIP Phones.

Two Figures, 5.3.2.21-1, Architecture for SCIP Phones in UCR 2008 using Modem Passthrough, and Figure 5.3.2.2.21-2, Architecture for SCIP Phones Using Modem Relay, show the RTS Architecture for supporting analog and IP SCIP phones in a UCR 2008 network (using modem passthrough and proprietary Phone ⇔ LSC signaling) and a UCR 2008, Change 1, network (using modem relay and either proprietary Phone ⇔ LSC signaling or AS-SIP Phone ⇔ LSC signaling). The UCR 2008, Change 1, network continues to support modem passthrough in MGs, ATAs, IADs, LSCs, and EBCs, for backward compatibility with UCR 2008 network operation.

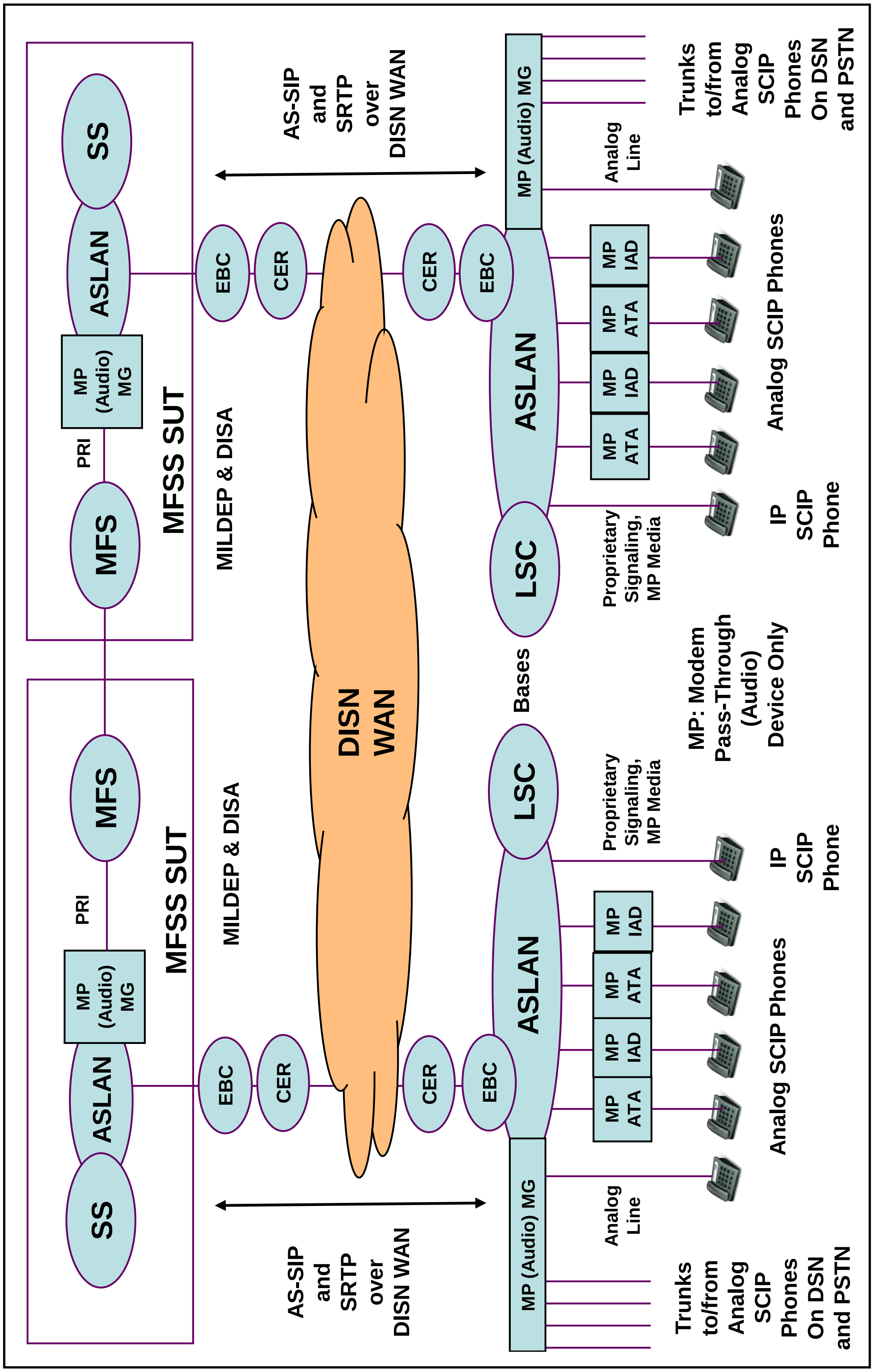

MFSS SUT
SS
ASLAN
MP (Audio) MG
PRI
MFS
MILDEP & DISA
EBC
CER
AS-SIP and SRTP over DISN WAN
DISN WAN
MP (Audio) MG
Analog Line
Trunks to/from Analog SCIP Phones On DSN and PSTN
LSC
Bases
MP IAD
MP ATA
Analog SCIP Phones
Proprietary Signaling, MP Media
IP SCIP Phone
MP: Modem Pass-Through (Audio) Device Only

Figure 5.3.2.21-1. Architecture for SCIP Phones in UCR 2008 Using Modem Pass-Through

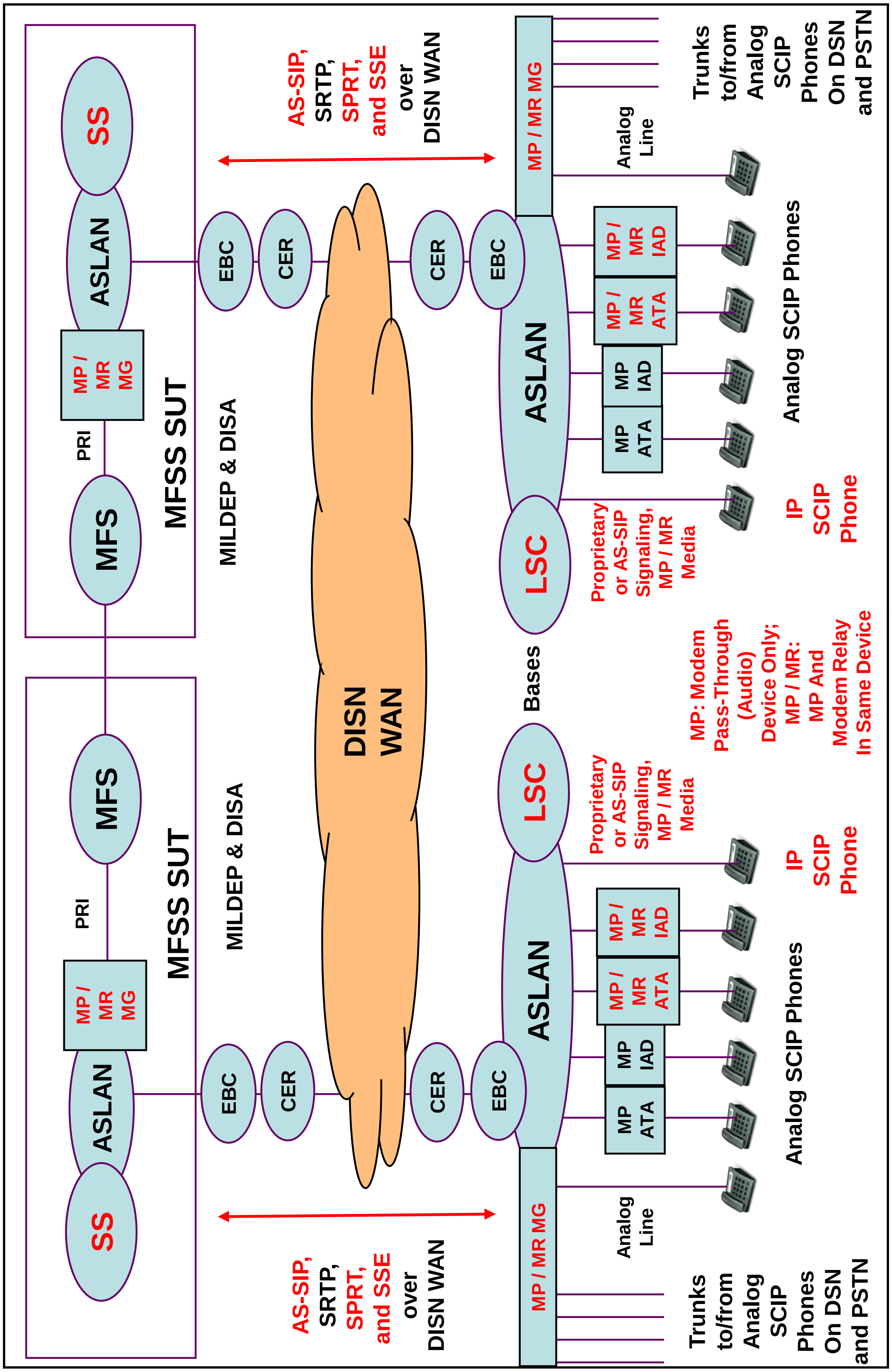

SS
ASLAN
MP / MR MG
PRI
MFS
MFSS SUT
MILDEP & DISA
EBC
CER
AS-SIP, SRTP, SPRT, and SSE over DISN WAN
DISN WAN
CER
EBC
MP / MR MG
ASLAN
LSC
Analog Line
Trunks to/from Analog SCIP Phones On DSN and PSTN
MP / MR IAD
MP / MR ATA
MP IAD
MP ATA
Analog SCIP Phones
Proprietary or AS-SIP Signaling, MP / MR Media
IP SCIP Phone
Bases
MP: Modem Pass-Through (Audio) Device Only; MP / MR: MP And Modem Relay In Same Device
MFS
PRI
MP / MR MG
MFSS SUT
MILDEP & DISA
ASLAN
SS
EBC
CER
CER
EBC
LSC
Proprietary or AS-SIP Signaling, MP / MR Media
IP SCIP Phone
ASLAN
MP / MR IAD
MP / MR ATA
MP IAD
MP ATA
Analog SCIP Phones
MP / MR MG
Analog Line
AS-SIP, SRTP, SPRT, and SSE over DISN WAN
Trunks to/from Analog SCIP Phones On DSN and PSTN

Figure 5.3.2.21.2. Architecture for SCIP Phones Using Modem Relay

5.3.2.21.2 RTS SCIP Gateway Requirements

This section contains the RTS SCIP Gateway requirements for UCR 2008 Change 1, based on the NSA document.

- SCIP-216

All references to "SCIP-216" that follow are references to SCIP-216, Revision 2.1.

In this section, a "SCIP Gateway" is any VoIP Gateway that conforms to SCIP-216. The SCIP Gateways may be used on the PSTN or on the DSN. An example of a SCIP Gateway is a VoIP Trunk Gateway that supports SCIP-216, is connected to a base IP LAN, and receives trunk-side service from a TDM switch on the Base, per UCR 2008, Section 5.2.12.8, DSN Line Side Voice over Internet Protocol Requiremen*t.*

In this section, an "RTS SCIP Gateway" is a VoIP Gateway that conforms to SCIP-216, conforms to the requirements in this section, and is served by an RTS LSC. Media Gateways, ATAs, and IADs that support SCIP-216 and are served by an RTS LSC are examples of RTS SCIP Gateways.

One key difference between the SCIP Gateway and the RTS SCIP Gateway is that the SCIP Gateway only supports trunk-side connections to the PSTN and the DSN. The RTS SCIP Gateway not only supports these trunk-side connections, but also supports line-side connections to analog phones, analog secure phones, analog fax machines, and analog modems.

These requirements cover four different types of RTS SCIP Gateways:

1. Media Gateway – Trunk-Side (MG-TS). This is the portion of the LSC or MFSS MG that supports trunk-side connections to the DSN and the PSTN via ISDN PRI trunk groups (which are required in UCR 2008), DoD Common CCS7 trunk groups (which are Conditional in UCR 2008), and CAS trunk groups (which are Conditional in UCR 2008). Support for Modem Relay in the MG-TS is Required in UCR 2008 Change 1.

2. Media Gateway – Line-Side (MG-LS). This is the portion of the LSC or MFSS MG that supports line-side connections to analog phones, analog secure phones, analog fax machines, and analog modems (which are Required in UCR 2008), and ISDN BRI phones and secure phones (when supported) (which are Conditional in UCR 2008). These line-side connections are provided by the existing twisted-pair copper-wire plant on the B/P/C/S where the LSC or MFSS is located. Support for Modem Relay in the MG-LS is Conditional in UCR 2008 Change 1.

NOTE: Newer B/P/C/Ss may not need an MG-LS if they are fully IP-based and do not have any existing copper-wire plant.

3. Analog Terminal Adapter (ATA). This is a device on the RTS end user's premise that supports interconnection between the ASLAN and the end user's analog phone, analog secure phone, analog fax machine, or analog modem.
   Support for Modem Relay in the ATA is Conditional in UCR 2008 Change 1.

   This device supports a single RJ-45 Ethernet interface on the ASLAN side, and a single analog RJ-11 interface on the end user side. The Ethernet side of the ATA gives the analog-side devices VoIP connectivity to the LSC, MG, and EBC on the ASLAN on the B/P/C/S.

4. Integrated Access Device (IAD). This is a device on the RTS end user's premise that supports interconnection between the ASLAN and multiple end-user analog phones, analog secure phones, analog fax machines, and analog modems.

   This device supports a single Ethernet RJ-45 interface on the ASLAN side, and multiple (from 4 up to 16) analog RJ-11 interfaces on the end-user side. Like the ATA, the Ethernet side of the IAD gives the analog-side devices VoIP connectivity to the LSC, MG, and EBC on the ASLAN on the B/P/C/S.

Support for Modem Relay in the IAD is Conditional in UCR 2008 Change 1.

5.3.2.21.2.1 Basic Minimum Essential Requirements

The following requirements are based on the Basic Minimum Essential Requirements in SCIP-216 Section 3 .

5.3.2.21.2.1.1 IP Transport Layer Protocol Requirements

[Required: MG-TS – Conditional: MG-LS, ATA, IAD] The RTS SCIP Gateway shall meet all the requirements for "IP Transport Layer Protocol" in SCIP-216, Section 3.1.

[Required: MG-TS – Conditional: MG-LS, ATA, IAD] The RTS SCIP 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.

5.3.2.21.2.1.2 V.150.1 Operational Mode Requirements

[Required: MG-TS – Conditional: MG-LS, ATA, IAD]The RTS SCIP Gateway shall meet all the requirements for "V.150.1 Operational Mode" in SCIP-216, Section 3.2.

[Required: MG-TS – Conditional: MG-LS, ATA, IAD] The RTS SCIP Gateway shall support the V.150.1 Audio and Modem Relay (MR) modes, per SCIP-216, Section 3.2.

5.3.2.21.2.1.3 Modem Relay Gateway Type Requirements

[Required: MG-TS – Conditional: MG-LS, ATA, IAD] The RTS SCIP Gateway shall meet all the requirements for "Modem-Relay Gateway Type" in SCIP-216, Section 3.3.

[Required: MG-TS – Conditional: MG-LS, ATA, IAD] The RTS SCIP Gateway shall support the V.32 and V.34 duplex modulation types in the MR mode, per SCIP-216, Section 3.3.

[Required: MG-TS – Conditional: MG-LS, ATA, IAD] The RTS SCIP 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.

[Conditional: MG-TS MG-LS, ATA, IAD] The RTS SCIP 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 TU-T Recommendation V.150.1, Section 9.1 of I (where they are also optional).

5.3.2.21.2.1.4 Simple Packet Relay Transport Requirements

The following requirements are based on the SPRT requirements in SCIP-216, Section 3.4.

[Required: MG-TS – Conditional: MG-LS, ATA, IAD] The RTS SCIP Gateway shall meet all the requirements for "Transport Channel" in SCIP-216, Section 3.4.1.

[Required: MG-TS – Conditional: MG-LS, ATA, IAD] The RTS SCIP 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.

[Required: MG-TS – Conditional: MG-LS, ATA, IAD] The RTS SCIP 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.

[Required: MG-TS – Conditional: MG-LS, ATA, IAD] The RTS SCIP Gateway shall meet all the requirements for "SPRT Modem Relay Messages" in SCIP-216, Section 3.4.2.

[Required: MG-TS – Conditional: MG-LS, ATA, IAD] In the MR mode, the RTS SCIP 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.

[Required: MG-TS – Conditional: MG-LS, ATA, IAD] The RTS SCIP Gateway shall meet all the requirements for "SPRT Timers" in Section 3.4.3 of SCIP-216.

5.3.2.21.2.1.5 State Signaling Event Requirements

The following requirements are based on the "State Signaling Event (SSE)" requirements in Section 3.5 of SCIP-216.

[Required: MG-TS – Conditional: MG-LS, ATA, IAD] The RTS SCIP 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.

[Required: MG-TS – Conditional: MG-LS, ATA, IAD] The RTS SCIP Gateway shall meet all the requirements for "SSE Call Discrimination Messages" in Section 3.5.1 of SCIP-216.

[Required: MG-TS – Conditional: MG-LS, ATA, IAD] The RTS SCIP Gateway shall meet all the requirements for "SSE Reliability" in Section 3.5.2 of SCIP-216.

[Required: MG-TS – Conditional: MG-LS, ATA, IAD] The RTS SCIP Gateway shall meet all the requirements for "SSE Reason Identifier Codes" in Section 3.5.3 of SCIP-216.

[Required: MG-TS – Conditional: MG-LS, ATA, IAD] The RTS SCIP Gateway shall meet all the requirements for "SSE Timers" in Section 3.5.4 of SCIP-216.

5.3.2.21.2.1.6 Call Setup Protocol Requirements

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.

[Required: MG-TS – Conditional: MG-LS, ATA, IAD] The RTS SCIP Gateway shall meet all the requirements for "V.150.1 Version Declaration" in Section 3.6.1 of SCIP-216.

[Required: MG-TS – Conditional: MG-LS, ATA, IAD] The RTS SCIP Gateway shall advertise a V.150.1 version number of "1" or higher, per Section 3.6.1 of SCIP-216.

[Required: MG-TS – Conditional: MG-LS, ATA, IAD] The RTS SCIP Gateway shall meet all the requirements for "Transcompression Capability" in Section 3.6.2 of SCIP-216.

[Required: MG-TS – Conditional: MG-LS, ATA, IAD] The RTS SCIP Gateway shall meet all the requirements for "Modem Relay Type Declaration" in Section 3.6.3 of SCIP-216.

[Required: MG-TS – Conditional: MG-LS, ATA, IAD] The RTS SCIP Gateway shall meet all the requirements for "Modulation Support Indication" in Section 3.6.4 of SCIP-216.

[Required: MG-TS; Conditional: MG-LS, ATA, IAD] The RTS SCIP Gateway shall meet all the requirements for "RFC 2833 Events" in Section 3.6.5 of SCIP-216.

[Required: MG-TS – Conditional: MG-LS, ATA, IAD] In the Audio state, the RTS SCIP 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 RTS SCIP Gateway shall be able to:

- Transmit the RFC 2833 Event over its IP interface after detecting the corresponding Answer event on its Data Communications Equipment (DCE) interface, and

- Transmit the Answer event on its DCE interface after detecting the corresponding RFC 2833 Event on its IP interface.

[Conditional: MG-TS, MG-LS, ATA, IAD] The RTS SCIP Gateway shall meet all the requirements for "SPRT Payload and Window Size Parameter" in Section 3.6.6 of SCIP-216.

[Required: MG-TS – Conditional: MG-LS, ATA, IAD] The RTS SCIP Gateway shall meet all the requirements for "JM Delay Support" in Section 3.6.7 of SCIP-216.

[Required: MG-TS – Conditional: MG-LS, ATA, IAD] The RTS SCIP Gateway shall meet all the requirements for "Call Discrimination Mode Parameters" in Section 3.6.8 of SCIP-216.

[Required: MG-TS – Conditional: MG-LS, ATA, IAD] The RTS SCIP Gateway shall meet all the requirements for "SSE Capability Indications" in Section 3.6.9 of SCIP-216.

[Required: MG-TS – Conditional: MG-LS, ATA, IAD] The RTS SCIP Gateway shall meet all the requirements for "SPRT Protocol Support Parameters" in Section 3.6.10 of SCIP-216.

[Required: MG-TS – Conditional: MG-LS, ATA, IAD] The RTS SCIP Gateway shall meet all the requirements for "NoAudio Support" in Section 3.6.11 of SCIP-216.

5.3.2.21.2.1.7 Data Communications Equipment (DCE) Interface Requirements

The following requirements are based on the "DCE Interface Requirements" in Section 3.7 of SCIP-216.

[Conditional: MG-TS, MG-LS, ATA, IAD] The RTS SCIP 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 Conditional**.**

[Required: MG-TS – Conditional: MG-LS, ATA, IAD] The RTS SCIP Gateway shall meet all the requirements for "Answer Tone Generation" in Section 3.7.2 of SCIP-216.

[Required: MG-TS – Conditional: MG-LS, ATA, IAD] The RTS SCIP Gateway shall meet all the requirements for "Absence of V.42" in Section 3.7.3 of SCIP-216.

5.3.2.21.2.2 Procedural Minimum Essential Requirements

The following requirements are based on the "Procedural Minimum Essential Requirements" in Section 4 of SCIP-216.

5.3.2.21.2.2.1 SSE State Transition Requirements

[Required: MG-TS – Conditional: MG-LS, ATA, IAD] The RTS SCIP Gateway shall meet all the requirements for SSE State Transition in Section 4.1 of SCIP-216.

[Required: MG-TS – Conditional: MG-LS, ATA, IAD] The RTS SCIP 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.

5.3.2.21.2.2.2 SPRT Procedures Requirements

The following requirements are based on the "SPRT Procedures Requirements" in Section 4.2 of SCIP-216.

[Conditional: MG-TS – Conditional: MG-LS, ATA, IAD] The RTS SCIP 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 Conditional**.**

[Required: MG-TS; Conditional: MG-LS, ATA, IAD] The RTS SCIP Gateway shall meet all the requirements for "SPRT Message Ordering" in Section 4.2.2 of SCIP-216.

[Required: MG-TS – Conditional: MG-LS, ATA, IAD] In the MR mode, the RTS SCIP 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.

[Conditional: MG-TS, MG-LS, ATA, IAD] The RTS SCIP Gateway shall meet all the requirements for "SPRT Window and Payload Size Negotiation" in Section 4.2.3 of SCIP-216.

[Required: MG-TS – Conditional: MG-LS, ATA, IAD] The RTS SCIP 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).

[Required: MG-TS – Conditional: MG-LS, ATA, IAD] The RTS SCIP Gateway shall meet all the requirements for SPRT Data Signaling Rate Indication in Section 4.2.4 of SCIP-216.

[Required: MG-TS – Conditional: MG-LS, ATA, IAD] The RTS SCIP Gateway shall use the MR_EVENT and CONNECT messages to indicate the data rate negotiated on its DCE interface in bits per second, per Section 4.2.4 of SCIP-216. The RTS SCIP Gateway shall also adhere to the Rate Matching Rule defined in Section 12.3.2.1 of ITU-T Recommendation V.150.1.

5.3.2.21.2.2.3 RFC 2833 Event Transmission Procedures

[Required: MG-TS – Conditional: MG-LS, ATA, IAD] The RTS SCIP Gateway shall meet all the requirements for RFC 2833 Event Transmission Procedures in Section 4.3 of SCIP-216.

5.3.2.21.2.2.4 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.

[Required: MG-TS – Conditional: MG-LS, ATA, IAD] The RTS SCIP 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.

[Required: MG-TS – Conditional: MG-LS, ATA, IAD] The RTS SCIP Gateway SSE state shall always start in the Audio mode, per Section 4.4.1 of SCIP-216.

[Required: MG-TS – Conditional: MG-LS, ATA, IAD] The RTS SCIP Gateway shall meet all the requirements for "SSE Audio to Modem Relay Transitions" in Section 4.4.1 of SCIP-216.

[Required: MG-TS – Conditional: MG-LS, ATA, IAD] The RTS SCIP Gateway shall meet all the requirements for "Procedures for SPRT Modem Relay Setup" in Section 4.4.2 of SCIP-216.

5.3.2.21.2.2.5 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.

[Required: MG-TS – Conditional: MG-LS, ATA, IAD] The RTS SCIP Gateway shall meet all the requirements for "Procedures for PSTN Initiated Cleardown" in Section 4.5.1 of SCIP-216.

[Required: MG-TS – Conditional: MG-LS, ATA, IAD] The RTS SCIP Gateway shall meet all the requirements for "Procedures for IP Initiated Cleardown" in Section 4.5.2 of SCIP-216.

5.3.2.21.2.2.6 Transition to On-Hook While in a Modem-Based Session

The following requirements are based on the "Transition to On-Hook While in a Modem-Based Session" in Section 4.6 of SCIP-216.

[Required: MG-TS – Conditional: MG-LS, ATA, IAD] The RTS SCIP Gateway shall meet all the requirements for "Procedures for IP Initiated On-Hook" in Section 4.6.1 of SCIP-216.

[Required: MG-TS – Conditional: MG-LS, ATA, IAD] The RTS SCIP Gateway shall meet all the requirements for "Procedures for PSTN Initiated On-Hook" in Section 4.6.2 of SCIP-216.

5.3.2.21.2.2.7 SPRT CLEARDOWN Procedures

[Conditional: MG-TS, MG-LS, ATA, IAD] The RTS SCIP Gateway shall meet all the requirements for "SPRT CLEARDOWN Procedures" in Section 4.7 of SCIP-216.

5.3.2.21.2.2.8 Call Menu – Joint Menu Procedures

[Required: MG-TS – Conditional: MG-LS, ATA, IAD] The RTS SCIP Gateway shall meet all the requirements for "Call Menu (CM) – Joint Menu (JM)" Procedures in Section 4.8 of SCIP-216.

5.3.2.21.2.2.9 NoAudio Payload Type Requirements for SCIP-216 Compliant Gateways

[Required: MG-TS – Conditional: MG-LS, ATA, IAD] The RTS SCIP Gateway shall meet all the requirements for NoAudio Payload Type in Section 4.9 of SCIP-216.

[Required: MG-TS – Conditional: MG-LS, ATA, IAD] The RTS SCIP 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 a SCIP-216 end point that immediately transitions to the Modem Relay state without transmitting information in the Audio state.

5.3.2.21.2.2.10 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.

[Conditional: MG-TS, MG-LS, ATA, IAD] The RTS SCIP 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 conditional**.**

[Required: MG-TS – Conditional: MG-LS, ATA, IAD] The RTS SCIP 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.

[Conditional: MG-TS – MG-LS, ATA, IAD] The RTS SCIP 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 conditional**.**

[Required: MG-TS – Conditional: MG-LS, ATA, IAD] The RTS SCIP 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.

[Required: MG-TS – Conditional: MG-LS, ATA, IAD] The RTS SCIP Gateway shall meet all the requirements for "Lost Packet Processing with I_OCTET-CS" in Section 4.10.3 of SCIP-216.

5.3.2.21.2.3 SSE and SPRT Message Content

The following requirements are based on the "SSE and SPRT Message Content" requirements in Section 5 of SCIP-216.

5.3.2.21.2.3.1 SSE Messages

The following requirements are based on the "SSE Messages" requirements in Section 5.1 of SCIP-216.

[Required: MG-TS – Conditional: MG-LS, ATA, IAD] The RTS SCIP Gateway shall meet all the requirements for the SSE Audio Message in Section 5.1.1 of SCIP-216.

[Required: MG-TS – Conditional: MG-LS, ATA, IAD] The RTS SCIP Gateway shall meet all the requirements for the "SSE Modem Relay Message" in Section 5.1.2 of SCIP-216.

5.3.2.21.2.3.2 SPRT Messages

The following requirements are based on the "SPRT Messages" requirements in Section 5.2 of SCIP-216.

[Required: MG-TS – Conditional: MG-LS, ATA, IAD] The RTS SCIP Gateway shall meet all the requirements for the "SPRT INIT Message" in Section 5.2.1 of SCIP-216.

[Required: MG-TS – Conditional: MG-LS, ATA, IAD] The RTS SCIP Gateway shall meet all the requirements for the "SPRT JM_INFO Message" in Section 5.2.2 of SCIP-216.

[Required: MG-TS – Conditional: MG-LS, ATA, IAD] The RTS SCIP Gateway shall meet all the requirements for the "SPRT CONNECT Message" in Section 5.2.3 of SCIP-216.

[Required: MG-TS – Conditional: MG-LS, ATA, IAD] The RTS SCIP Gateway shall meet all the requirements for the "SPRT MR_EVENT Message" in Section 5.2.4 of SCIP-216.

[Required: MG-TS – Conditional: MG-LS, ATA, IAD] The RTS SCIP 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.

[Conditional: MG-TS, MG-LS, ATA, IAD] If the SPRT I_RAW-OCTET Message is supported, the RTS SCIP 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.)

[Required: MG-TS – Conditional: MG-LS, ATA, IAD] The RTS SCIP Gateway shall meet all the requirements for the SPRT I_OCTET Message in Section 5.2.7 of SCIP-216.

[Required: MG-TS – Conditional: MG-LS, ATA, IAD] The RTS SCIP Gateway shall meet all the requirements for the SPRT I_OCTET-CS Message in Section 5.2.8 of SCIP-216.

5.3.2.21.2.4 Use of Common UDP Port Numbers for SRTP, SSE, and SPRT Messages

[Required: MG-TS – Conditional: MG-LS, ATA, IAD] The RTS SCIP Gateway shall use the same UDP port numbers and protocol numbers for

- The SRTP media packets sent and received during the Audio mode (when the call is "in the clear"),
- 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"), and
- The SPRT media packets sent and received during the Modem Relay mode (when the call is "secure").

The UDP port numbers shall be the UDP port numbers negotiated by the RTS SCIP Gateway and the remote party (RTS SCIP EI or remote RTS SCIP Gateway) using SDP during AS-SIP session establishment.

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 1883], this field is called the "Next Header" field."

[Required: MG-TS – Conditional: MG-LS, ATA, IAD] When an RTS SCIP Gateway transitions the media stream between a normal session using SRTP and a secure session using SPRT, the RTS SCIP 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 EBC (when the EBC is located in the media stream for those sessions).

[Required: MG-TS – Conditional: MG-LS, ATA, IAD] The RTS SCIP 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.

[Required: MG-TS – Conditional: MG-LS, ATA, IAD] The RTS SCIP 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.

SCIP-216 allows this multiple UDP port number approach, but the RTS SCIP Gateway shall not use this approach because it adds complexity to session establishment, and has a negative effect on RTS EBCs.

5.3.2.21.2.5 Use of V.150.1 SSE Messages for Media Transitions between Audio and Modem Relay

[Required: MG-TS – Conditional: MG-LS, ATA, IAD] Per Section 5.4, Information Assurance Requirements, RTS SCIP Gateways shall protect RTS Audio and Video media streams using SRTP, when exchanging these media streams with RTS SCIP Phones and other RTS SCIP Gateways.

(When RTS SCIP Gateways exchange modem relay media streams with RTS SCIP 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.)

[Required: MG-TS – Conditional: MG-LS, ATA, IAD] When RTS SCIP Gateways exchange RFC 2833 Events and V.150.1 SSE messages with RTS SCIP 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.

[Required: MG-TS – Conditional: MG-LS, ATA, IAD] For all IP-TDM and TDM-IP interworking calls, RTS SCIP 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. RTS SCIP 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.

[Required: MG-TS – Conditional: MG-LS, ATA, IAD] After one end of the call (the TDM SCIP phone or IP SCIP phone) decides to go secure, the RTS SCIP 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 RTS SCIP Gateway shall begin this processing by exchanging SSE messages with the RTS SCIP Phone, EBC, or other RTS SCIP Gateway, per ITU-T Recommendation V.150.1 and SCIP-216.

[Required: MG-TS – Conditional: MG-LS, ATA, IAD] As part of the Audio-media-to-Modem-Relay-media conversion process, the RTS SCIP Gateway shall not send an outgoing AS-SIP re-INVITE message that requests Audio-to-Modem-Relay media conversion.

[Required: MG-TS – Conditional: MG-LS, ATA, IAD] As part of the Audio-media-to-Modem-Relay-media conversion process, the RTS SCIP Gateway shall not require the receipt of an incoming AS-SIP re-INVITE message that requests Audio-to-Modem-Relay media conversion.

[Required: MG-TS – Conditional: MG-LS, ATA, IAD] The RTS SCIP 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.

[Required: MG-TS – Conditional: MG-LS, ATA, IAD] After one end of the call (the TDM SCIP phone or IP SCIP phone) decides to return to "voice in the clear," the RTS SCIP 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 RTS SCIP Gateway shall begin this processing by exchanging SSE messages with the RTS SCIP Phone, EBC, or other RTS SCIP Gateway, per ITU-T Recommendation V.150.1 and SCIP-216.

[Required: MG-TS – Conditional: MG-LS, ATA, IAD] As part of the Modem-Relay-media-to-Audio-media conversion process, the RTS SCIP Gateway shall not send an outgoing AS-SIP re-INVITE message that requests Modem-Relay-to-Audio media conversion.

[Required: MG-TS – Conditional: MG-LS, ATA, IAD] As part of the Modem-Relay-media-to-Audio-media conversion process, the RTS SCIP Gateway shall not require the receipt of an incoming AS-SIP re-INVITE message that requests Modem-Relay-to-Audio-media conversion.

[Required: MG-TS – Conditional: MG-LS, ATA, IAD] The RTS SCIP 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.

[Required: MG-TS – Conditional: MG-LS, ATA, IAD] The RTS SCIP 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.

5.3.2.21.2.6 Modem Relay and Modem Passthrough for RTS SCIP Gateways

[Required: MG-TS; Conditional: MG-LS, ATA, IAD] When an RTS SCIP 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 RTS SCIP Gateway shall instead provide Modem Passthrough treatment for that call. In this case, the RTS SCIP Gateway shall handle the MoIP call in the LSC or MFSS in the same way that it would handle a G.711 VoIP call in the LSC or MFSS, with these clarifications:

1. 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 5.3.2.12.13, Echo Cancellation).

2. The Gateway may disable silence suppression on the MoIP side of the call.

NOTE: End-to-end synchronization of the calling and called modems (or modem-equipped SCIP phones) is not guaranteed on a modem passthrough call. Even though a modem passthrough 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 modem passthrough calls. It is expected that these calls will complete using AS-SIP signaling and SRTP media exchange like VoIP calls in RTS 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.

[Required: MG-TS] The RTS SCIP 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 Modem Passthrough treatment.

NOTE: The acquiring activity for the RTS SCIP 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 Digital Signal Processing [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 LSC or MFSS, and analog SCIP phones behind TAs, IADs, and MG line cards on an LSC or MFSS.

5.3.2.21.2.7 Modem Relay Support for V.92 and V.90 Modulation Types

[Required: MG-TS – Conditional: MG-LS, ATA, IAD] On SCIP-216 modem relay calls where the V.92 Digital (Required) is used, and on SCIP-216 modem relay calls where the V.92 Analog (Conditional) modulation type is used, the TDM side of the MG-TS shall act as the digital interface to the remote V.92 Server modem, and the TDM side of the MG-LS, ATA, 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).

The SCIP-216 modem relay communication between the MG-TS and the MG-LS, ATA, or IAD shall support V.92-Server-modem-to-V.92-Client-modem communication in the MG-TS-to-MG-LS/TA/IAD direction, and V.92-Client-modem-to-V.92-Server-modem communication in the MG-LS/TA/IAD-to-MG-TS direction.

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 also be greater than 33.6 kbps and less than 53.3 kbps.

[Required: MG-TS – Conditional: MG-LS, ATA, IAD] On SCIP-216 modem relay calls where the V.90 digital modulation type (Required) is used, and on SCIP-216 modem relay calls where the V.90 analog modulation type (Conditional) is used, the TDM side of the MG-TS shall act as the digital interface to the remote V.90 server modem, and the TDM side of the MG-LS, ATA, 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).

The SCIP-216 modem relay communication between the MG-TS and the MG-LS, ATA, or IAD shall support V.90-Server-modem-to-V.90-Client-modem communication in the MG-TS-to-MG-LS/TA/IAD direction, and V.90-Client-modem-to-V.90-Server-modem communication in the MG-LS/TA/IAD-to-MG-TS direction.

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 US 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.

5.3.2.21.3 RTS SCIP EI Requirements

This section contains the RTS SCIP EI requirements for UCR 2008, Change 1, based on the following NSA document:

- SCIP-215, Revision 2.1.

All references to "SCIP-215" in the following paragraphs are references to SCIP-215, Revision 2.1.

In this section, a "SCIP EI" is any Secure IP Phone that conforms to SCIP-215. The SCIP EIs may be used on commercial VoIP networks or on the DSN. An example of a SCIP EI is a Secure IP Phone that supports SCIP-215, is connected to a base IP LAN, and receives line-side VoIP service from a TDM DSN switch on the base, per UCR 2008, Section 5.2.12.8, DSN Line Side Voice over Internet Protocol Requirement.

In this section, an "RTS SCIP EI" is a Secure IP Phone that conforms to SCIP-215, conforms to the requirements in this section, and is served by an RTS LSC.

An RTS SCIP EI also communicates with the RTS LSC using either

- Vendor-proprietary signaling and transport protocols or
- AS-SIP signaling over TLS

A SCIP EI might only communicate with a TDM switch on the base (which provides DSN line-side VoIP) using vendor-proprietary signaling and transport protocols.

An RTS SCIP 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"). An SCIP EI on a commercial VoIP network or the DSN might instead exchange media with other SCIP end points using RTP over UDP during the audio part of the call, and using SSE and SPRT over UDP during the modem relay part of the call.

NOTE: The requirements for an RTS SCIP EI to support AS-SIP signaling over TLS are included in Section 5.3.2.22, Generic AS-SIP End Instrument and Video Codec Requirements. This section provides generic AS-SIP EI requirements for RTS Phones, RTS Secure Phones

(RTS SCIP EIs), and RTS Video Phones. The requirements for an RTS SCIP EI to support SSE and SPRT media over UDP are included in the following paragraphs, as part of this section.

5.3.2.21.3.1 Basic Minimum Essential Requirements (MER)

The following requirements are based on the basic MER in Section 4 of SCIP-215.

5.3.2.21.3.1.1 IP Transport Layer Protocol Requirements

[Required: RTS SCIP EI] The RTS SCIP EI shall meet all the requirements for "IP Transport Layer Protocol" in Section 4.1 of SCIP-215.

5.3.2.21.3.1.2 V.150.1 Operational Mode Requirements

[Required: RTS SCIP EI] The RTS SCIP EI shall meet all the requirements for "V.150.1 Operational Mode" in Section 4.2 of SCIP-215.

5.3.2.21.3.1.3 Modem-Relay Gateway Type Requirements

[Required: RTS SCIP EI] The RTS SCIP EI shall meet all the requirements for "Modem-Relay Gateway Type" in Section 4.3 of SCIP-215.

5.3.2.21.3.1.4 Simple Packet Relay Transport Requirements

The following requirements are based on the SPRT requirements in Section 4.4 of SCIP-215.

[Required: RTS SCIP EI] The RTS SCIP EI shall meet all the requirements for "Transport Channel" in Section 4.4.1 of SCIP-215.

[Required: RTS SCIP EI] The RTS SCIP EI shall meet all the requirements for "SPRT Modem Relay Messages" in Section 4.4.2 of SCIP-215.

[Required: RTS SCIP EI] The RTS SCIP EI shall meet all the requirements for "SPRT Timer" in Section 4.4.3 of SCIP-215.

5.3.2.21.3.1.5 SSE Requirements

The following requirements are based on the SSE requirements in Section 4.5 of SCIP-215.

[Required: RTS SCIP EI] The RTS SCIP EI shall meet all the requirements for "SSE Call Discrimination Messages" in Section 4.5.1 of SCIP-215.

[Required: RTS SCIP EI] The RTS SCIP EI shall meet all the requirements for "SSE Reliability" in Section 4.5.2 of SCIP-215.

[Required: RTS SCIP EI] The RTS SCIP EI shall meet all the requirements for "SSE Reason Identifier Code" in Section 4.5.3 of SCIP-215.

[Required: RTS SCIP EI] The RTS SCIP EI shall meet all the requirements for "SSE Timer" in Section 4.5.4 of SCIP-215.

5.3.2.21.3.1.6 Call Setup Protocol Requirements

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.

[Required: RTS SCIP EI] The RTS SCIP EI shall meet all the requirements for "V.150.1 Version Declaration" in Section 4.6.1 of SCIP-215.

[Required: RTS SCIP EI] The RTS SCIP EI shall meet all the requirements for "Transcompression Capability" in Section 4.6.2 of SCIP-215.

[Required: RTS SCIP EI] The RTS SCIP EI shall meet all the requirements for "Modem Relay Type Declaration" in Section 4.6.3 of SCIP-215.

[Required: RTS SCIP EI] The RTS SCIP EI shall meet all the requirements for "Modulation Support Indication" in Section 4.6.4 of SCIP-215.

[Required: RTS SCIP EI] The RTS SCIP EI shall meet all the requirements for "RFC 2833 Events" in Section 4.6.5 of SCIP-215.

[Conditional: RTS SCIP EI] The RTS SCIP EI shall meet all the requirements for "SPRT Payload and Window Size Parameter" in Section 4.6.6 of SCIP-215.

[Required: RTS SCIP EI] The RTS SCIP EI shall meet all the requirements for "JM Delay Support" in Section 4.6.7 of SCIP-215.

[Required: RTS SCIP EI] The RTS SCIP EI shall meet all the requirements for "Call Discrimination Mode Parameter" in Section 4.6.8 of SCIP-215.

[Required: RTS SCIP EI] The RTS SCIP EI shall meet all the requirements for "SSE Capability Indication" in Section 4.6.9 of SCIP-215.

[Required: RTS SCIP EI] The RTS SCIP EI shall meet all the requirements for “SPRT Protocol Support Parameters” in Section 4.6.10 of SCIP-215.

[Required: RTS SCIP EI] The RTS SCIP EI shall meet all the requirements for “NoAudio Support” in Section 4.6.11 of SCIP-215.

5.3.2.21.3.1.7 SCIP Operational Mode Requirements

[Required: RTS SCIP EI] The RTS SCIP EI shall meet all the requirements for “SCIP Operational Mode” in Section 4.7 of SCIP-215.

5.3.2.21.3.1.8 V.14 Requirements

[Conditional: RTS SCIP EI] The RTS SCIP EI shall meet all the requirements for “V.14” in Section 4.8 of SCIP-215.

5.3.2.21.3.2 Procedural MER

The following requirements are based on the Procedural MER in Section 5 of SCIP-215.

5.3.2.21.3.2.1 SSE State Transition Requirements

[Required: RTS SCIP EI] The RTS SCIP EI shall meet all the requirements for “SSE State Transition” in Section 5.1 of SCIP-215.

5.3.2.21.3.2.2 SPRT Procedures Requirements

The following requirements are based on the “SPRT Procedures Requirements” in Section 5.2 of SCIP-215.

[Conditional: RTS SCIP EI] The RTS SCIP 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**.**

[Required: RTS SCIP EI] The RTS SCIP EI shall meet all the requirements for “SPRT Message Ordering” in Section 5.2.2 of SCIP-215.

[Conditional: RTS SCIP EI] The RTS SCIP EI shall meet all the requirements for “SPRT Window and Payload Size Negotiation” in Section 5.2.3 of SCIP-215.

[Required: RTS SCIP EI] The RTS SCIP EI shall meet all the requirements for “SPRT Data Signaling Rate Indication” in Section 5.2.4 of SCIP-215.

5.3.2.21.3.2.3 RFC 2833 Event Transmission Procedures

[Required: RTS SCIP EI] The RTS SCIP EI shall meet all the requirements for “RFC 2833 Event Transmission Procedures” in Section 5.3 of SCIP-215.

5.3.2.21.3.2.4 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.

[Required: RTS SCIP EI] The RTS SCIP EI shall meet all the requirements for SSE Audio to modem relay Transitions in Section 5.4.1 of SCIP-215.

[Required: RTS SCIP EI] The RTS SCIP EI shall meet all the requirements for Procedures for SPRT modem relay Setup in Section 5.4.2 of SCIP-215.

5.3.2.21.3.2.5 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.

[Required: RTS SCIP EI] The RTS SCIP EI shall meet all the requirements for “Procedures for PSTN Initiated Cleardown” in Section 5.5.1 of SCIP-215.

[Required: RTS SCIP EI] The RTS SCIP EI shall meet all the requirements for “Procedures for IP Initiated Cleardown” in Section 5.5.2 of SCIP-215.

5.3.2.21.3.2.6 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.

[Required: RTS SCIP EI] The RTS SCIP EI shall meet all the requirements for Procedures for IP Initiated On-hook in Section 5.6.1 of SCIP-215.

[Required: RTS SCIP EI] The RTS SCIP EI shall meet all the requirements for “Procedures for PSTN Initiated On-Hook” in Section 5.6.2 of SCIP-215.

5.3.2.21.3.2.7 SPRT CLEARDOWN Procedures

[Conditional: RTS SCIP EI] The RTS SCIP EI shall meet all the requirements for “SPRT CLEARDOWN Procedures” in Section 5.7 of SCIP-215.

5.3.2.21.3.2.8 Call Menu (CM) – Joint Menu (JM) Procedures

[Required: RTS SCIP EI] The RTS SCIP EI shall meet all the requirements for “Call Menu (CM) – Joint Menu (JM) Procedures” in Section 5.8 of SCIP-215.

5.3.2.21.3.2.9 Use of the NoAudio Payload Type by “Modem Relay-Preferred” Terminals

[Required: RTS SCIP EI] The RTS SCIP 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.

5.3.2.21.3.2.10 Bandwidth Negotiation Requirements

[Required: RTS SCIP EI] The RTS SCIP EI shall meet all the requirements for “Bandwidth Negotiation” in Section 5.10 of SCIP-215.

5.3.2.21.3.3 SSE and SPRT Message Content

The following requirements are based on the “SSE and SPRT Message Content” requirements in Section 6 of SCIP-215.

5.3.2.21.3.3.1 SSE Messages

The following requirements are based on the “SSE Messages” requirements in Section 6.1 of SCIP-215.

[Required: RTS SCIP EI] The RTS SCIP EI shall meet all the requirements for the “SSE Audio Message” in Section 6.1.1 of SCIP-215.

[Required: RTS SCIP EI] The RTS SCIP EI shall meet all the requirements for the “SSE modem relay Message” in Section 6.1.2 of SCIP-215.

5.3.2.21.3.3.2 SPRT Messages

The following requirements are based on the “SPRT Messages” requirements in Section 6.2 of SCIP-215.

[Required: RTS SCIP EI] The RTS SCIP EI shall meet all the requirements for the “SPRT INIT Message” in Section 6.2.1 of SCIP-215.

[Required: RTS SCIP EI] The RTS SCIP EI shall meet all the requirements for the “SPRT JM_INFO Message” in Section 6.2.2 of SCIP-215.

[Required: RTS SCIP EI] The RTS SCIP EI shall meet all the requirements for the "SPRT CONNECT Message" in Section 6.2.3 of SCIP-215.

[Required: RTS SCIP EI] The RTS SCIP EI shall meet all the requirements for the "SPRT MR_EVENT" message in Section 6.2.4 of SCIP-215.

[Required: RTS SCIP EI] The RTS SCIP 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.

[Conditional: RTS SCIP EI] If the SPRT I_RAW-OCTET message is supported, the RTS SCIP EI shall meet all the requirements for that message in Section 6.2.6 of SCIP-215. (Support for the I_RAW-OCTET data type is currently optional in SCIP-215, but may become a requirement later.)

[Required: RTS SCIP EI] The RTS SCIP EI shall meet all the requirements for the "SPRT I_OCTET" message in Section 6.2.7 of SCIP-215.

[Required: RTS SCIP EI] The RTS SCIP EI shall meet all the requirements for the "SPRT I_OCTET-CS" message in Section 6.2.8 of SCIP-215.

5.3.2.21.3.4 Use of Common UDP Port Numbers for SRTP, SSE, and SPRT Messages

[Required: RTS SCIP EI] The RTS SCIP 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").

The UDP port numbers shall be the UDP port numbers negotiated by the RTS SCIP EI and the remote party (RTS SCIP Gateway or other RTS SCIP EI) using SDP during AS-SIP session establishment.

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).

[Required: RTS SCIP EI] When an RTS SCIP EI transitions the media stream between a normal session using SRTP and a secure session using SPRT, the RTS SCIP 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 Edge Boundary Controller (when the EBC is located in the media stream for those sessions).

[Required: RTS SCIP EI] The RTS SCIP 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.

[Required: RTS SCIP EI] The RTS SCIP EI 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.

SCIP-215 allows this multiple UDP port number approach, but the RTS SCIP EI shall not use this approach because it adds complexity to session establishment, and has a negative effect on RTS EBCs.

5.3.2.21.3.5 Use of V.150.1 SSE Messages for Media Transitions between Audio and Modem Relay

[Required: RTS SCIP EI] Per Section 5.4, Information Assurance Requirements, RTS SCIP EIs shall protect RTS audio and video media streams using SRTP when exchanging these media streams with RTS SCIP Gateways and other RTS SCIP EIs.

NOTE: When RTS SCIP EIs exchange modem relay media streams with RTS SCIP 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.

[Required: RTS SCIP EI] When RTS SCIP EIs exchange RFC 2833 events and V.150.1 SSE messages with RTS SCIP 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.

[Required: RTS SCIP EI] For all IP-TDM interworking, TDM-IP interworking, and IP-IP calls, RTS SCIP 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 RTS SCIP 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.

[Required: RTS SCIP EI] Once one end of the call decides to go secure, the RTS SCIP EI shall begin the process of changing the established media stream from audio media to modem relay media. The RTS SCIP EI shall begin this processing by exchanging SSE messages with the RTS SCIP Gateway or other RTS SCIP EI, per V.150.1 and SCIP-215.

[Required: RTS SCIP EI] As part of the Audio-media-to-Modem-Relay-media conversion process, the RTS SCIP EI shall not send an outgoing AS-SIP re-INVITE message that requests Audio-to-Modem-Relay media conversion.

[Required: RTS SCIP EI] As part of the Audio-media-to-modem-relay-media conversion process, the RTS SCIP EI shall not require the receipt of an incoming AS-SIP re-INVITE message that requests Audio-to-Modem-Relay media conversion.

[Required: RTS SCIP EI] The RTS SCIP 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.

[Required: RTS SCIP EI] Once one end of the call decides to return to "voice in the clear," the RTS SCIP EI shall begin the process of changing the established media stream from modem relay media to audio media. The RTS SCIP EI shall begin this processing by exchanging SSE messages with the RTS SCIP Gateway or other RTS SCIP EI, per V.150.1 and SCIP-215.

[Required: RTS SCIP EI] As part of the Modem-Relay-media-to-Audio-media conversion process, the RTS SCIP EI shall not send an outgoing AS-SIP re-INVITE message that requests Modem-Relay-to-Audio media conversion.

[Required: RTS SCIP EI] As part of the Modem-Relay-media-to-Audio-media conversion process, the RTS SCIP EI shall not require the receipt of an incoming AS-SIP re-INVITE message that requests Modem-Relay-to-Audio media conversion.

[Required: RTS SCIP EI] The RTS SCIP 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.

[Required: RTS SCIP EI] The RTS SCIP 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.

5.3.2.22 AS-SIP End Instrument and Video Codec Requirements

This section provides an architecture and requirements for "AS-SIP End Instruments and Video Codecs" to ensure that AS-SIP Voice EIs, Secure Voice EIs, and Video Codecs (also known as Video EIs) can connect to and interoperate with any VVoIP vendor's LSC.

This section contains LSC and AS-SIP EI requirements to support a generic, multivendor-interoperable interface between a VVoIP LSC 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 LSC ⇔ EI protocols. NOTE: ITU Recommendation H.323 and IETF SIP (commercial SIP, not DISA-specified AS-SIP) are both considered vendor-proprietary LSC ⇔ EI protocols here.

5.3.2.22.1 Architecture for Supporting EIs and Video Codecs Using AS-SIP

This section provides the architecture for supporting AS-SIP Voice EIs (both hardphone EIs and softphone EIs), AS-SIP Secure Voice EIs (hardphone EIs only), and AS-SIP Video EIs (video codecs, both hardphone EIs and softphone EIs) on LSCs, using the AS-SIP signaling protocol between the LSC and the AS-SIP EIs.

The basic architecture change needed to support AS-SIP EIs is to add LSC-to-AS-SIP-EI interfaces where proprietary LSC-to-EI interfaces are currently supported. Therefore, AS-SIP EI capabilities need to be added to the following VVoIP Network Elements:

- The LSC CCA, called just the LSC here.
- The Voice EI (Voice EI, for both the hardphone EI and the softphone EI).
- The Secure Voice EI (Secure Voice EI, for the hardphone EI only).
- The Video EI (Video EI, for both the Hardphone EI and the Softphone EI), also known as the Video Codec.

Secure Video EIs (e.g., Video EIs that use SCIP to encrypt video media streams) are outside the scope of this section.

The AS-SIP EI capabilities do not need to be added to the following VVoIP NEs:

- The MG-TS and MG - MG-LS
- ATAs
- IADs

The signaling interfaces between the LSC CCA and the MG-TS, between the LSC CCA and the MG-LS, between the LSC CCA and the ATA, and between the LSC CCA and the IAD are vendor-proprietary and will still be vendor-proprietary here. The “line-side” AS-SIP EI enhancements described here are required for Voice EIs, Secure Voice EIs, and Video EIs, and are not required for MG-TSs, MG-LSs, ATAs, or IADs.

NOTE: The LSC-to-EBC interface already uses AS-SIP as the signaling protocol. As a result, the AS-SIP EI requirements here have no effect on the LSC-to-EBC interface.

This section uses three new terms to distinguish vendor-proprietary EIs from AS-SIP EIs:

1. An AS-SIP Voice EI is an RTS Voice phone (hardphone or softphone) that uses AS-SIP signaling instead of vendor-proprietary signaling. A Voice EI is an RTS Voice phone that uses vendor-proprietary signaling.

2. An AS-SIP Secure Voice EI is an RTS Secure Voice phone (hardphone only) that uses AS-SIP signaling instead of vendor-proprietary signaling. A Secure Voice EI is an RTS Secure Voice phone that uses vendor-proprietary signaling.

   NOTE: The AS-SIP Secure Voice EIs and (proprietary) Secure Voice EIs both use V.150.1 modem relay for secure voice media transfer, per the Government’s SCIP-215 specification and ITU Recommendation V.150.1. The AS-SIP Secure Voice EIs also operate in the same manner as AS-SIP Voice EIs, during nonsecure parts of the voice call where E2E voice communication is done “in the clear.”

3. An AS-SIP Video EI is an RTS Video phone (hardphone or softphone) that uses AS-SIP signaling instead of vendor-proprietary signaling. A Video EI is an RTS Video phone that uses vendor-proprietary signaling.

   NOTE: The AS-SIP Video EIs and (proprietary) Video EIs are Video phones (hardphones or softphones), and are not RTS MCUs. RTS MCUs are more complex than RTS Video Phones, and involve point-to-multipoint video conferences instead of point-to-point video calls. As a result, the AS-SIP EI requirements here apply to RTS Video Phones (hardphone and softphones), but do not apply to RTS Video MCUs.

Another aspect of this architecture is that the AS-SIP EIs (Voice, Secure Voice, and Video) are required to follow all the pre-existing requirements for EIs (Voice and Video, with Secure Voice EIs following the existing requirements for Voice EIs), except for those requirements that involve vendor-proprietary LSC-to-EI signaling. The pre-existing requirements for EIs include, but are not limited to, the following capabilities:

1. Display of the Calling Number and Precedence Level on incoming sessions.

2. Use of DSCPs in signaling and media streams.

3. Support for audio (G.711, G.722.1, G.723.1, G.729, G.729A) and Video (H.261, H.263, H.263-2000, H.264) codecs.

4. Support for 10/100-T Mbps Ethernet interfaces to the ASLAN.

5. Support for locally generated tones and announcements (e.g., tones generated by the EI and not by the LSC or its Media Server).

6. Support for LSC-generated tones and announcements (e.g., announcements generated by the LSC and its Media Server, and not by the EI itself).

7. Compliance with ANSI/TIA-810-B requirements for Send Loudness Rating and Receive Loudness Rating (RLR).

Figure 5.3.2.21-3, Architecture for Proprietary EIs in UCR 2008, shows the RTS Architecture for supporting vendor-proprietary EIs in a UCR 2008 network (using vendor-proprietary LSC–EI signaling). Figure 5.3.2.21-4, Architecture for Proprietary and Generic AS-SIP EIs in UCR 2008, Change 1, shows the RTS Architecture for supporting AS-SIP EIs in a UCR 2008, Change 1 network (using multivendor-interoperable AS-SIP LSC-EI signaling). The UCR 2008, Change 1 network still supports vendor-proprietary EIs using vendor-proprietary LSC-EI signaling. As a result, both proprietary EIs using proprietary signaling and AS-SIP EIs using AS-SIP signaling are shown in Figure 5.3.2.21-4.

The LSC, AS-SIP EI, and LSC-to-AS-SIP-EI interface requirements here are also applicable to RTS SSs within RTS MFSSs. RTS SSs support internal LSCs, and these internal LSCs support Voice, Secure Voice, and Video EIs. These SS-internal LSCs should also support AS-SIP Voice EIs, AS-SIP Secure Voice EIs, and AS-SIP Video EIs, per the requirements here.

Figure 5.3.2.21-3. Architecture for Proprietary EIs in UCR 2008

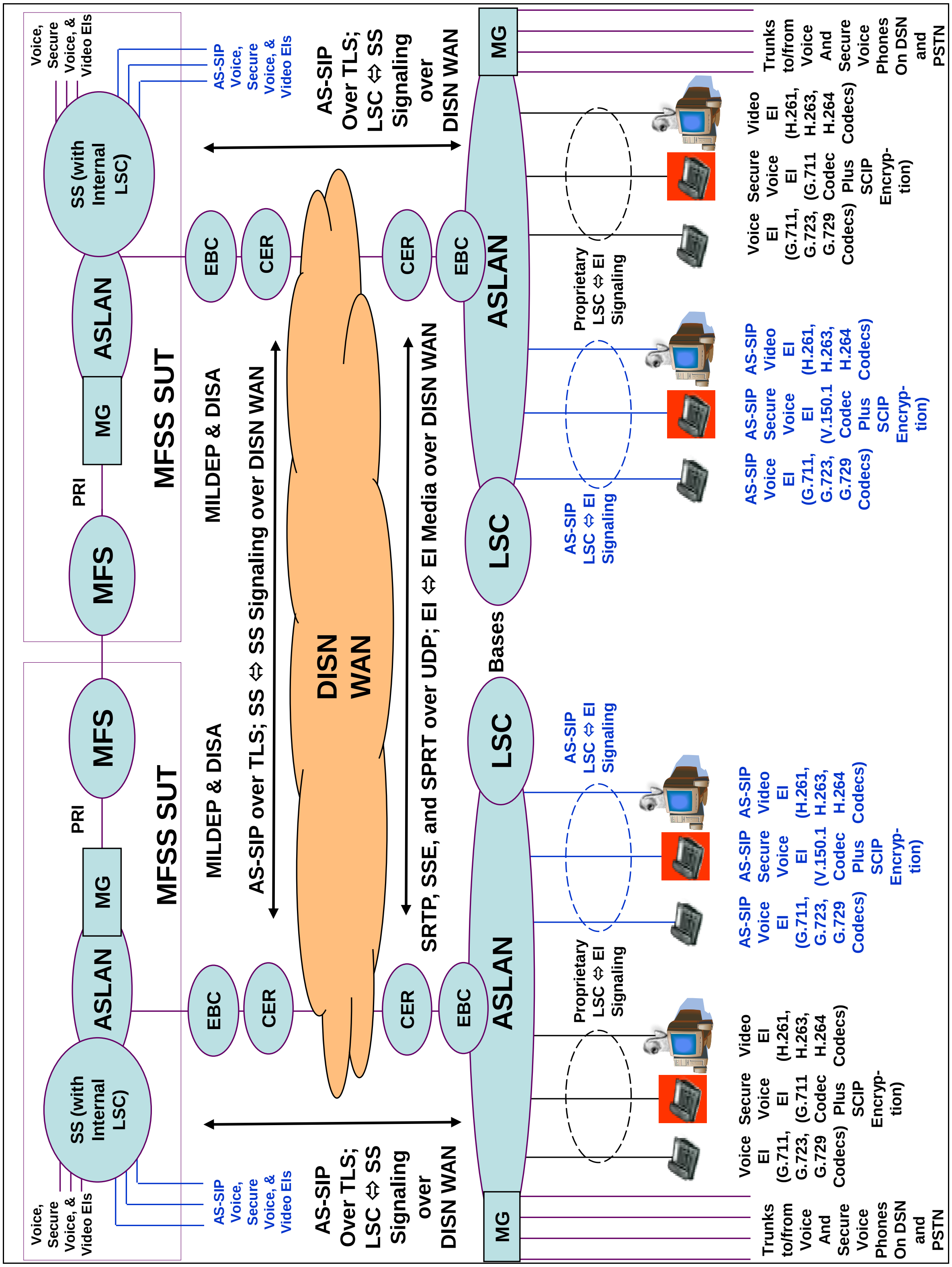

Voice, Secure Voice, & Video EIs
AS-SIP Voice, Secure Voice, & Video EIs
SS (with Internal LSC)
ASLAN
MG
PRI
MFS
MFSS SUT
EBC
CER
AS-SIP Over TLS; SS ⇔ SS Signaling over DISN WAN
MILDEP & DISA
AS-SIP over TLS; SS ⇔ SS Signaling over DISN WAN
DISN WAN
SRTP, SSE, and SPRT over UDP; EI ⇔ EI Media over DISN WAN
Bases
LSC
ASLAN
MG
AS-SIP LSC ⇔ EI Signaling
Proprietary LSC ⇔ EI Signaling
Voice EI (G.711, G.723, G.729 Codecs)
Secure Voice EI (G.711 Codec Plus SCIP Encryp-tion)
Video EI (H.261, H.263, H.264 Codecs)
AS-SIP Voice EI (G.711, G.723, G.729 Codecs)
AS-SIP Secure Voice EI (V.150.1 Codec Plus SCIP Encryp-tion)
AS-SIP Video EI (H.261, H.263, H.264 Codecs)
Trunks to/from Voice And Secure Voice Phones On DSN and PSTN

Figure 5.3.2.21-4. Architecture for Proprietary and AS-SIP EIs in UCR 2008, Change 1

5.3.2.22.2 Requirements for Supporting AS-SIP EIs

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

[Required: LSC, 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 existing requirements in UCR 2008 for EIs (Voice and Video, with Secure Voice EIs following the existing requirements for Voice EIs), except for those requirements that involve vendor-proprietary LSC-to-EI signaling. The existing requirements for EIs in UCR 2008 include, but are not limited to, the following capabilities:

1. Display of the Calling Number and Precedence Level on incoming sessions.

2. Use of DSCPs in signaling and media streams.

3. Support for Audio (G.711, G.722.1, G.723.1, G.729, G.729A) codecs on Voice and Secure Voice EIs.

4. Support for Audio (G.711, G.722, G.722.1, G.723.1, G.729, G.729A) codecs and Video (H.261, H.263, H.263 2000, H.264) codecs on Video EIs.

5. Support for 10/100-T Mbps Ethernet interfaces to the ASLAN.

6. Support for locally generated tones and announcements (e.g., tones generated by the EI and not by the LSC or its Media Server).

7. Support for LSC-generated tones and announcements (e.g., announcements generated by the LSC and its Media Server, and not by the EI itself).

8. Compliance with ANSI/TIA-810-B requirements for Send Loudness Rating (SLR) and RLR.

[Required: LSC, SS, AS-SIP Voice EI, AS-SIP Secure Voice EI, AS-SIP Video EI] The LSCs 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 should authenticate itself with its serving LSC using AS-SIP and TLS signaling, and each LSC should authenticate itself with the AS-SIP EIs that it serves using AS-SIP and TLS signaling.

[Required: LSC, SS] The LSC shall allow a single AS-SIP EI to support Voice, Secure Voice, and Video capabilities. In this case, the LSC shall support that EI using the combined requirements for a AS-SIP Voice EI, a AS-SIP Secure Voice EI, and a AS-SIP Video EI, as given below. The LSC shall also allow a single AS-SIP EI to support the following subset of these three capabilities:

- Voice and Secure Voice
- Voice and Video

[Conditional: AS-SIP Voice EI, AS-SIP Secure Voice EI, AS-SIP Video EI] A single AS-SIP EI may support Voice, Secure Voice, and Video capabilities. In this case, the EI shall support those capabilities in accordance with 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 5.3.2.22.2.1, Requirements for AS-SIP Voice EIs; Section 5.3.2.22.2.2, Requirements for AS-SIP Secure Voice EIs; and UCR 2008, Section 5.3.2.22.2.3, Requirements for AS-SIP Video EIs.

[Conditional: AS-SIP Voice EI, AS-SIP Secure Voice EI] A single AS-SIP EI may support both Voice and Secure Voice capabilities. In this case, the EI shall support those capabilities in accordance with the combined requirements for an AS-SIP Voice EI and an AS-SIP Secure Voice EI, as given in Section 5.3.2.22.2.1, Requirements for AS-SIP Voice EIs, and Section 5.3.2.22.2.2, Requirements for AS-SIP Secure Voice EIs.

[Conditional: AS-SIP Voice EI, AS-SIP Video EI] A single AS-SIP EI may support both Voice and Video capabilities. In this case, the EI shall support those capabilities in accordance with the combined requirements for an AS-SIP Voice EI and an AS-SIP Video EI, as given in Section 5.3.2.22.2.1, Requirements for AS-SIP Voice EIs, and Section 5.3.2.22.2.3, Requirements for AS-SIP Video EIs.

[Required: AS-SIP Secure Voice EI] An AS-SIP Secure Voice EI shall also support the capabilities of an AS-SIP Voice EI in accordance with the AS-SIP Voice EI requirements given in Section 5.3.2.22.2.1, 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 only supports Audio media using the “NoAudio” payload type, then the AS-SIP Secure Voice EI is not required to support the G.7XX codecs.)

5.3.2.22.2.1 Requirements for AS-SIP Voice EIs

[Required: LSC, SS] The LSCs shall support AS-SIP Voice EIs that use AS-SIP for EI ⇔ LSC signaling. The LSCs shall support these AS-SIP Voice EIs using the AS-SIP LSC-to-AS-SIP-EI interface defined in Section 5.3.2.22.3.1, Multiple Call Appearances, and in Section 5.3.4, AS-SIP Requirements.

[Required: AS-SIP Voice EI] The AS-SIP Voice EIs shall support AS-SIP for EI ⇔ LSC signaling. These AS-SIP Voice EIs shall support the AS-SIP LSC-to-AS-SIP-EI interface defined in Section 5.3.2.22.3.1, Multiple Call Appearances, and in Section 5.3.4, AS-SIP Requirements.

[Required: LSC, SS, AS-SIP Voice EI] The LSCs and AS-SIP Voice EIs shall support the following supplementary services for voice calls on AS-SIP Voice EIs, consistent with Section 5.3.2.2.2.1, Voice Features and Capabilities.

- Precedence Call Waiting [Required]
- Call Forwarding [Required]
- Call Transfer [Required]
- Call Hold [Required]
- Preset Conferencing [Conditional]
- Three-Way Calling [Required]
- Hotline Service [Conditional]
- Calling Party and Called Party ID (number only) [Required]
- Call Pickup (Conditional for Voice EIs [both Proprietary and AS-SIP])

The LSCs and AS-SIP Voice EIs shall support these supplementary services using AS-SIP signaling.

[Required: LSC, SS, AS-SIP Voice EI] The LSCs 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 LSC 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 Call Waiting, and additional calls that are being originated by the EI using Call

Transfer or Three-Way Calling. The LSC 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.

[Required: LSC, 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 5.3.2.22.3.1, Multiple Call Appearances). But one of these call appearances may not be used, because the LSC is only configured to support one voice call appearance for one DSN number on this EI.

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

1. When the LSC is configured to support two call appearances on an AS-SIP Voice EI, the LSC shall use a voice call limit of “Two” for that EI.

2. When the LSC is configured to support one call appearance on an AS-SIP Voice EI (even though the EI may support two call appearances), the LSC shall use a voice call limit of “One” for that EI.

5.3.2.22.2.2 Requirements for AS-SIP Secure Voice EIs

[Required: LSC, SS] The LSCs shall support AS-SIP Secure Voice EIs that use AS-SIP for EI ⇔ LSC signaling. The LSCs shall support these AS-SIP Secure Voice EIs using the AS-SIP LSC-to-AS-SIP-EI interface defined in Section 5.3.2.22.3.1, Multiple Call Appearances, and in Section 5.3.4, AS-SIP Requirements.

[Required: AS-SIP Secure Voice EI] AS-SIP Secure Voice EIs shall support AS-SIP for EI ⇔ LSC signaling. These AS-SIP Secure Voice EIs shall support the AS-SIP LSC-to-AS-SIP-EI interface defined in Section 5.3.2.22.3.1, Multiple Call Appearances, and in Section 5.3.4, AS-SIP Requirements.

[Required: LSC, SS] The LSCs and SSs shall support the following supplementary services for voice calls on AS-SIP Secure Voice EIs, consistent with Section 5.3.2.2.2.1, Voice Features and Capabilities, as extended by UCR 2008, Change 1:

- Precedence Call Waiting [Required]

- Call Forwarding [Required]

- Call Transfer [Required]

- Call Hold [Required]
- Preset Conferencing [Conditional]
- Three-Way Calling [Required]
- Hotline Service [Conditional]
- Calling Party and Called Party ID (number only) [Required]
- Call Pickup (Conditional for Voice EIs [both Proprietary and AS-SIP]).

The LSCs shall support these supplementary services using AS-SIP signaling.

NOTE: LSCs and SSs, which are in the session signaling path but not in the session media path, cannot make any distinctions between voice calls ("clear voice" calls) and secure voice calls at an AS-SIP secure voice EI. This limitation occurs because a secure voice call always starts off as a voice call first, and then later converts from a voice call to a secure voice call after an E2E exchange of V.150.1 SSE messages in the media path (and not in the signaling path). As a result, if an LSC provides a supplementary service to an AS-SIP EI for voice calls, the LSC also provides that supplementary service to the AS-SIP EI for secure voice calls, since the LSC on its own cannot distinguish between a voice call at an AS-SIP EI and a secure voice call at that AS-SIP EI.

An AS-SIP Secure Voice EI, however, can distinguish between a voice call (a call in "clear-voice" mode) and a secure voice call. So the AS-SIP Secure Voice EI can prevent the use of a supplementary service on secure voice calls (like Call Hold, Call Transfer, or Three-Way Calling), where the use of that service can "break" the media path between the calling and called EIs (SCIP end points) and cause the secure voice call to fail. But the Secure Voice EI can also allow the use of a supplementary service on secure voice calls by requiring the end user to return the secure voice call to a voice call (a "clear-voice" call) so that the supplementary service can be used. This is the approach supported at the AS-SIP secure voice EI in the following requirements.

[Required: AS-SIP Secure Voice EI] In UCR 2008, Change 1, an AS-SIP Secure Voice EI is not required to support any supplementary services for secure voice calls (calls using SCIP/modem relay media).

[Required: AS-SIP Secure Voice EI] In UCR 2008, Change 1, 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).

[Required: AS-SIP Secure Voice EI] In UCR 2008, Change 1, 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.

[Required: AS-SIP Secure Voice EI] In UCR 2008, Change 1, 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.

[Required: AS-SIP Secure Voice EI] In UCR 2008, Change 1, 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.

[Required: AS-SIP Secure Voice EI] In UCR 2008, Change 1, 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.

[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, as an extension of the requirement to support these services for voice calls in Section 5.3.2.2.2.1, Voice Features and Capabilities:

- Precedence Call Waiting [Required]
- Call Forwarding [Required]
- Call Transfer [Required]
- Call Hold [Required]
- Preset Conferencing [Conditional]
- Three-Way Calling [Required]
- Hotline Service [Conditional]
- Calling Party and Called Party ID (number only) [Required]
- Call Pickup [Conditional for Voice EIs (both Proprietary and AS-SIP)].

The AS-SIP Secure Voice EI shall support these supplementary services using AS-SIP signaling.

[Required: AS-SIP Secure Voice EI] When an AS-SIP Secure Voice EI has a secure voice call active, the LSC sends that EI a Precedence Call Waiting or Routine Call Waiting 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 LSC.

[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 LSC.

[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 LSC.

[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 Three-Way Calling 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 Three-Way Calling 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 LSC.

[Required: AS-SIP Secure Voice EI] When an AS-SIP Secure Voice EI has a secure voice call active, and the LSC sends that EI a Precedence Call Waiting or Routine Call Waiting indication and provides Calling Party ID and Precedence Level information within the Call Waiting 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 Call Waiting 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 Call Forwarding Don't Answer feature or deflected by the Precedence Call Diversion feature.)

[Required: LSC, SS, AS-SIP Secure Voice EI] The LSC and the AS-SIP Secure Voice EI shall support a mechanism to limit the total number of voice and secure voice calls at that EI at any given time. (For example, it is possible for an EI to have a voice call (Audio media) on hold and a secure voice call (Modem Relay media) active at the same time.)

The LSC shall keep track of the total number of active voice and secure voice calls at the EI at all times. (The LSC does not need to separately track the total number of voice calls and the total number of secure voice calls at the EI, since this would require the LSC to know which calls are voice calls using Audio media, and which calls are secure voice calls using modem relay media.) The LSC shall compare this total number of voice and secure voice calls to the configured voice call limit for that EI, and shall block further voice call requests to and from the AS-SIP EI once this call limit is reached.

[Required: LSC, SS, AS-SIP Secure Voice EI] For AS-SIP Secure Voice EIs (which can also operate as AS-SIP Voice EIs), the voice/secure voice call limit depends on the number of voice call appearances supported on the EI. Like AS-SIP Voice EIs, AS-SIP Secure Voice EIs are required to support two voice call appearances for one DSN number in this document (per Section 5.3.2.22.3.1, Multiple Call Appearances). But one of these call appearances may not be used because the LSC is only configured to support one voice call appearance for one DSN number on this EI.

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

1. When the LSC is configured to support two call appearances on an AS-SIP Secure Voice EI, the LSC shall use a voice/secure voice call limit of “Two” for that EI.

2. When the LSC is configured to support one call appearance on an AS-SIP Secure Voice EI (even though the EI may support two call appearances), the LSC shall use a voice/secure voice call limit of “One” for that EI.

5.3.2.22.2.3 Requirements for AS-SIP Video EIs

[Required: LSC, SS] LSCs shall support AS-SIP Video EIs that use AS-SIP for EI ⇔ LSC signaling. The LSCs shall support these AS-SIP Video EIs using the AS-SIP LSC-to-AS-SIP-EI interface defined in Section 5.3.2.22.3.1, Multiple Call Appearances, and in Section 5.3.4, AS-SIP Requirements.

[Required: AS-SIP Voice EI] The AS-SIP Video EIs shall support AS-SIP for EI ⇔ LSC signaling. These AS-SIP Video EIs shall support the AS-SIP LSC-to-AS-SIP-EI interface defined in Section 5.3.2.22.3.1, Multiple Call Appearances, and in Section 5.3.4, AS-SIP Requirements, of UCR 2008, Change 1.

[Objective: LSC, SS, AS-SIP Voice EI] It is an objective that LSCs, SSs, and AS-SIP Video EIs support the following supplementary services for video calls, as an extension of the requirement to support these services for voice calls in Section 5.3.2.2.2.1, Voice Features and Capabilities:

- Precedence Call Waiting [Required for voice calls]
- Call Forwarding [Required for voice calls]
- Call Transfer [Required for voice calls]
- Call Hold [Required for voice calls]
- Preset Conferencing [Objective for voice calls]
- Three-Way Calling [Required for voice calls]
- Hotline Service [Required for voice calls]
- Calling Party and Called Party ID (number only) [Required for voice calls]
- Call Pickup (Conditional for voice calls)

When this objective is supported, the LSCs, SSs, and AS-SIP Video EIs shall support these supplementary services using AS-SIP signaling.

[Required: LSC, SS, AS-SIP Video EI] The LSCs 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 LSC shall keep track of the total number of video calls at the AS-SIP Video EI at all times. The LSC 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.

For AS-SIP Video EIs in UCR 2008, Change 1, the configured call limit for that EI shall be "one video call." This is all that is required of AS-SIP Video EIs in UCR 2008, Change 1.

[Required: LSC, SS, AS-SIP Video EI] The LSC and the AS-SIP Video EI shall support a mechanism to identify the amount of video call bandwidth (counted as Video Session Units) in use at that EI at any given time.

The LSC and the AS-SIP Video EI shall keep track of the total amount of video call bandwidth (in VSU) in use at the AS-SIP Video EI at all times. (A 500-Kbps video call shall use one VSU of bandwidth, a 1-Mbps video call shall use two VSUs of bandwidth, a 2.5-Mbps video call shall use five VSU of bandwidth, and a 4.0-Mbps video call shall use eight VSUs of bandwidth.)

[Required: LSC, SS, AS-SIP Video EI] The LSC and the AS-SIP Video EI shall also 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 LSC-to-AS-SIP-EI interface to signal the bandwidth change.

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

5.3.2.22.3 Multiple call appearance Requirements for AS-SIP EIs

5.3.2.22.3.1 Multiple call appearances

Section 5.3.4, AS-SIP Requirements, contains requirements on "Multiple Appearances" in Sections 5.3.4.10.3.2.2.1a through 5.3.4.10.3.2.2.3. The first of these requirements is as follows:

> "IP end instruments MUST be limited to two (2) appearances per DN and limited to, at most, two (2) DNs."

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 only required to support 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 LSCs that serve the AS-SIP EIs, and to the LSC-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.

[Required: LSC, SS, AS-SIP Voice EI, AS-SIP Secure Voice EI] On the LSC-to-AS-SIP-EI interface, the LSC and the AS-SIP EI shall allow multiple call appearances of the same DN (10-digit DSN number) to be assigned to a single AS-SIP EI. The LSC and the AS-SIP EI shall allow at least two appearances of the same DN to be assigned to the AS-SIP EI. This requirement does not apply to AS-SIP Video EIs.

[Required: LSC, SS, AS-SIP Voice EI, AS-SIP Secure Voice EI] On the LSC-to-AS-SIP-EI interface, the LSC and the 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.

[Required: LSC, SS, AS-SIP Video EI] On the LSC-to-AS-SIP-EI interface, the LSC and the AS-SIP EI shall support one DN for video calls, and 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.

[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).

[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.

[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.

[Required: AS-SIP Video EI] An AS-SIP Video EI shall 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.

[Required: LSC, SS, AS-SIP Voice EI, AS-SIP Secure Voice EI] On the LSC-to-AS-SIP-EI interface, the LSC and the AS-SIP EI shall support the dedication of an individual call appearance to that single EI (instead of sharing of that individual call appearance across multiple EIs). For each call appearance that appears on an AS-SIP EI, the LSC shall have the ability to mark and treat that call appearance as an "Unshared call appearance," as part of the LSC's profile for that EI.

[Required: LSC, SS, AS-SIP Voice EI, AS-SIP Secure Voice EI] On the LSC-to-AS-SIP-EI interface, the LSC shall allow the AS-SIP EI to select the voice call appearance to be used on outgoing calls from that EI (i.e., sessions originated with an EI-to-LSC INVITE message). The LSC shall determine the Calling Number to be used on that outgoing call request based on the DN associated with the EI-selected call appearance.

The AS-SIP EI and LSC shall also allow multiple media types to be requested (as part of SDP capability declaration) in the same EI-to-LSC INVITE message. For example, INVITE messages from a voice call appearance on an AS-SIP Secure Voice EI can contain both an Audio media declaration (with G.711, G.722.1, G.723, and G.729 codecs indicated), and a V.150.1 modem relay media declaration (with SSE and SPRT protocols indicated).

[Required: LSC, SS, AS-SIP Voice EI, AS-SIP Secure Voice EI] On the LSC-to-AS-SIP-EI interface, the LSC shall select the call appearance and media types (e.g., Audio and modem relay) to be used on incoming calls to that EI (i.e., sessions offered with an LSC-to-EI INVITE message). The LSC shall determine the call appearance based on the Called Number for that incoming call request; the called number for the incoming call request shall match the DN associated with the LSC-selected call appearance. The LSC and AS-SIP EI shall also allow multiple media types to be requested (as part of SDP capability declaration) in the same LSC-to-EI INVITE message.

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

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

[Required: AS-SIP Secure Voice EI] The AS-SIP Secure Voice EI shall only allow 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 only allow this secure voice call to be in an "active" state, and not in a "held" state, or a "call in progress" state.

[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 only allow this additional voice call to be in 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 Call Waiting 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.

[Required: LSC, SS, AS-SIP Voice EI, AS-SIP Secure Voice EI] On the LSC-to-AS-SIP-EI interface, the LSC and 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). The LSC and AS-SIP EI shall support transitions from Voice media to Secure Voice media, and transitions from Secure Voice media to Voice media.

5.3.2.22.3.2 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 LSC-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.

These LSC, AS-SIP Voice EI, and AS-SIP Secure Voice EI requirements are based on the corresponding requirements for handling incoming precedence calls on the DSN-switch-to-ISDN-BRI interface, for an ISDN BRI station set that supports multiple appearances of a single DN. These requirements are found in UCR 2008, Section 5.2.2.6.3, Single B Channel, Multiple Appearances, Single Directory Number.

[Required: LSC, SS, AS-SIP Voice EI, AS-SIP Secure Voice EI] When offering an incoming precedence call to a multiple-call-appearance AS-SIP EI, the LSC shall direct the EI to the following:

1. Play a precedence ringing tone for that call.

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

3. Provide a visual precedence level display to the end user.

The EI shall play the precedence ringing tone, offer the call on the indicated call appearance, and provide the precedence level display to the end user as directed by the LSC.

[Required: LSC, SS, AS-SIP Voice EI, AS-SIP Secure Voice EI] The LSC and the AS-SIP EI shall then give the called user the option of either of the following:

1. Placing the currently active call (on the currently active call appearance) on hold and picking up the incoming precedence call on the new call appearance.

2. Ignoring the incoming precedence call on the new call appearance. "Ignoring," as used here, means that the called user allows the call to be forwarded by the Call Forwarding Don't Answer feature, or deflected by the Precedence Call Diversion feature.

[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 callback 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.

[Required: LSC, SS, AS-SIP Voice EI, AS-SIP Secure Voice EI] The LSC and 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 LSC and 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. This process of offering a new precedence call, placing an existing call on hold, and answering the precedence call shall remain the same until the AS-SIP EI is saturated (i.e., all of its call appearances are in use).

[Required: LSC, SS, 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 LSC and 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.

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

[Required: LSC, SS, AS-SIP Voice EI, AS-SIP Secure Voice EI] The LSC and 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.

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

As a result, the called user should 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.

[Required: LSC, SS, AS-SIP Voice EI, AS-SIP Secure Voice EI] The LSC and 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 Call Forward Don't Answer is assigned), or letting it divert to an attendant (e.g., if Precedence Call Diversion is assigned).

[Required: LSC, SS, 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 LSC and 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).

[Required: LSC, SS, AS-SIP Voice EI, AS-SIP Secure Voice EI] When the local party on the active call appearance goes "on hook," the LSC and 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 where the active call has been cleared.

[Required: LSC, SS, AS-SIP Voice EI, AS-SIP Secure Voice EI] The LSC and 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 Call Forward Don't Answer is assigned), or letting it divert to an attendant (if Precedence Call Diversion is assigned).

[Required: LSC, SS, AS-SIP Voice EI, AS-SIP Secure Voice EI] In both of the previous cases (held call preempted and active call preempted), the LSC and 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.

[Required: LSC, SS, AS-SIP Voice EI, AS-SIP Secure Voice EI] In both previous cases above where the end user ignores the precedence call, and lets it either forward to an alternate party (via Call Forward Don't Answer) or divert to an attendant (via Precedence Call Diversion), the LSC and the AS-SIP EI shall follow the requirements in UCR 2008, Section 5.3.2.2.2.1.1, Call Forwarding, that define the interaction between VVoIP precedence calls and Call Forwarding.

5.3.2.22.4 AS-SIP Video EI Features

[Conditional: AS-SIP Video EI] If the AS-SIP Video EI also supports FECC based on

- 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

- Section 5.3.4.9.7.3, General H.224 Control Channel for Far End Camera Control Messages,

of UCR 2008, Change 1.

[Conditional: AS-SIP Video EI] If the AS-SIP Video EI also supports BFCP based on

- RFC 4582 and
- RFC 4583

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

- Section 5.3.4.9.7.4, SDP Attributes for Binary Floor Control Protocol Streams,

of UCR 2008, Change 1.

[Conditional: AS-SIP Video EI] If the AS-SIP Video EI also supports Video Channel Flow Control [VCFC] based on

- RFC 4585

then the EI shall support all the AS-SIP and SDP protocol requirements for VCFC in

- Section 5.3.4.9.7.5, Video Channel Flow Control,

of UCR 2008, Change 1.

This UCR section requires support for 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

[Conditional: AS-SIP Video EI] If the AS-SIP Video EI also supports Video Channel Fast Update Requests [VCFUR] based on

- RFC 5104

then the EI shall support all the AS-SIP and SDP protocol requirements for VCFUR in

- Section 5.3.4.9.7.6, Video Channel Fast Update Requests,

of UCR 2008, Change 1.

The Full Intra Request (FIR) payload-specific feedback message is the method adopted in this UCR section for implementing VCFUR.

5.3.2.23 Requirements for Supporting Commercial Cost Avoidance

This section provides an initial set of requirements for a Commercial Cost Avoidance application at RTS LSCs, MFSSs, and WAN SSs using an RTS Routing Database. These requirements apply to calls that are dialed to commercial numbers (PSTN E.164 numbers) by IP end users who are served by RTS LSCs and RTS EIs. These requirements assume that an RTS Routing Database is deployed in the DISN that contains records, which list both the commercial PSTN number and the corresponding DSN number for a select set of RTS and DSN end users. These initial requirements may be expanded in later releases of the UCR to include more Commercial Cost Avoidance and Routing Database functionality.

With the planned implementation of the RTS Routing Database and its associated NRT collection of DSN and PSTN numbers from voice and video EI assigned to RTS LSCs, a new DISN application called Commercial Cost Avoidance can be enabled if the LSCs can perform basic overflow routing.

[Required: LSC] Use of this Commercial Cost Avoidance functionality shall be an optional application that can be configured (i.e., enabled and disabled) on each RTS LSC. Initially, this application will have a very small utility due to the low number of RTS telephones deployed. But as RTS expands, this application will be more and more beneficial to the Government due to commercial call cost avoidance.

[Required: LSC] The LSC shall be able to query the DISN RTS Routing Database on "99 dialed PSTN number" call requests from LSC end users. When the database responds to this query with a DSN number that matches the dialed PSTN number, the LSC shall route the call request over the appropriate IP (AS-SIP) or TDM (e.g., T1.619A PRI) path, using the DSN number returned by the database. When the database responds with a "number not found" indication, the LSC shall route the call request to the local TDM PSTN trunk group (PRI or CAS) on the LSC's MG, using the originally dialed commercial number.

[Required: RTS Routing Database] The RTS Routing Database shall be able to accept Commercial Cost Avoidance queries from the LSC, where this query contains the "PSTN called number" from the "99 dialed PSTN number" call request from the LSC end user. The RTS Routing Database shall be able to accept these queries for both CONUS "PSTN called numbers" (where the called number is from the 10-digit NANP) and OCONUS "PSTN called numbers" (where the called number is from outside of the 10-digit NANP).

[Required: RTS Routing Database] The RTS Routing Database 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 PSTN numbers and OCONUS PSTN numbers, as described in the previous requirement.

[Required: RTS Routing Database] When the RTS Routing Database determines that the PSTN called number (CONUS or OCONUS) received from the LSC in the Commercial Cost Avoidance query matches a 10-digit DSN number stored in the database, the database shall include that 10-digit DSN number in the query response that it sends back to the LSC.

[Required: RTS Routing Database] When the RTS Routing Database determines that the PSTN called number (CONUS or OCONUS) received from the LSC in the Commercial Cost Avoidance query does not match any 10-digit DSN number stored in the Database, the Database shall return a "Number not found" indication in the query response that it sends back to the LSC.

[Required: LSC, RTS Routing Database] The query-response interface between the LSC and the RTS Routing Database shall be LDAP Version 3 (v3) over TLS over IP. This LDAPv3 interface shall be compliant with RFC 4510.

On this interface, the CCA query shall be sent in the LDAPv3 Search Request message, and the CCA response shall be sent in the LDAPv3 Search Result Entry and Search Result Done messages.

The LDAPv3 Search Request message shall contain a field in ASCII format identifying the full international – format called PSTN number (Country Code + Nationally Significant Number), and a field containing the UC domain of the LSC (i.e., uc.mil).

When the database returns a DSN number that matches the called PSTN number, the LDAPv3 Search Result Entry message shall contain fields in ASCII format identifying

- the full international – format called PSTN number,
- the UC domain of the LSC (i.e., uc.mil), and
- the 10-digit DSN number that matches the PSTN called number.

In this case, the LDAPv3 Search Result Done message shall contain a field indicating "Success."

When the database does not find a DSN number that matches the called PSTN number, the Database shall not return an LDAPv3 Search Result Entry message to the LSC, but shall instead return an LDAPv3 Search Result Done message to the LSC.

In this case, the LDAPv3 Search Result Done message shall contain fields indicating "Success" and "0 results."

[Required: LSC, RTS Routing Database] The encoding of the LDAPv3 messages and data schema used on the DB query interface between the LSC and the RTS Routing Database shall follow the BER of ASN.1, consistent with Section 5.1, Protocol Encoding, of RFC 4511.
[Required: LSC, RTS Routing Database] The DB query interface between the LSC and the RTS Routing Database shall be secured using TLS, consistent with the requirements for securing AS-SIP messages using TLS in UCR 2008, Change 1, Section 5.4, Information Assurance Requirements. This security shall provide mutual authentication between the LSC and the RTS Routing Database, message confidentiality for the DB query and DB response, and message integrity for the DB query and DB response.

[Required: LSC, RTS Routing Database] The DB query interface between the LSC and the RTS Routing Database shall traverse the data firewalls (and not the RTS EBC firewalls) at both the LSC and RTS Routing Database sites.

[Required: LSC, RTS Routing Database] The DB query interface between the LSC and the RTS Routing Database shall traverse the CE Routers at both the LSC and RTS Routing Database sites, using the UCR 2008, Change 1, DSCP for OA&M traffic, and the associated CE Router queues.

[Required: LSC] The DB query interface between the LSC and the RTS Routing Database shall terminate on the Ethernet interface used for VVoIP signaling and bearer traffic at the LSC, as described in UCR 2008, Change 1, Section 5.4, Information Assurance Requirements.

[Required: LSC] After transmitting a Commercial Cost Avoidance query to the Database, the LSC shall start a "Commercial Cost Avoidance Query Response" timer awaiting a Database response. If the timer expires and no response is received, the LSC shall route the call request to the local TDM PSTN trunk group (PRI or CAS) using the originally dialed commercial number.

[Required: LSC] On Commercial Cost Avoidance call requests that are re-routed to DSN numbers by the database, the LSC shall respond to MFSS or WAN SS AS-SIP signaling indicating that the call was rejected (i.e., an AS-SIP 4xx, 5xx, or 6xx response to an AS-SIP INVITE message), by overflowing these calls from the AS-SIP trunk group to the local TDM PSTN trunk group (PRI or CAS) using the originally dialed commercial number.

[Required: MFSS, WAN SS] On Commercial Cost Avoidance call requests that are re-routed to DSN numbers by the database, the MFSS or WAN SS shall accept AS-SIP call requests from the LSC where the DSN number is identified as the called number. The MFSS or WAN SS shall also be capable of returning AS-SIP signaling to the calling LSC that indicates "404 Not Found," "480 Temporarily Unavailable," or "500 Server Internal Error." The MFSS or WAN SS shall be capable of generating this AS-SIP signaling on its own, and shall be capable of relaying that AS-SIP signaling when it is received from a remote MFSS, remote WAN SS, or remote LSC.

[Required: LSC] For each RTS end user served by an LSC, the LSC shall be able to upload that user's DSN phone number, PSTN phone number, and a unique LSC CCA-ID, Primary MFSS/WAN SS CCA-ID, and Backup MFSS/WAN SS CCA-ID to the RTS Routing Database.
[Required: LSC, RTS Routing Database] The DB update interface between the LSC and the RTS Routing Database shall also be LDAPv3 over TLS over IP. This LDAPv3 interface shall be compliant with RFC 4510.

On this interface, when the LSC is adding numbers to the DB,

- the DB update shall be sent from the LSC to the DB in the LDAPv3 Add Request message, and
- the DB response shall be sent from the DB to the LSC in the LDAPv3 Add Response message.

On this interface, when the LSC is deleting numbers from the DB,

- the DB update shall be sent from the LSC to the DB in the LDAPv3 Delete Request message, and

- the DB response shall be sent from the DB to the LSC in the LDAPv3 Delete Response message.

The LDAPv3 Add Request and Delete Request messages shall both contain fields in ASCII format identifying

- the full 10-digit DSN number of the RTS end user,
- the UC domain of the LSC (i.e., uc.mil),
- the full international – format PSTN number of the RTS end user,
- the CCA-ID of the LSC serving that RTS end user,
- the CCA-ID of the Primary MFSS/WAN SS serving that LSC, and
- the CCA-ID of the Backup MFSS/WAN SS serving that LSC.

The LDAPv3 Add Response and Delete Response messages shall both contain a field indicating "Success".

[Required: LSC, RTS Routing Database] The encoding of the LDAPv3 messages and data schema used on the DB update interface between the LSC and the RTS Routing Database shall follow the BER of ASN.1, consistent with RFC 4511, Section 5.1, Protocol Encoding.

[Required: LSC, RTS Routing Database] The DB update interface between the LSC and the RTS Routing Database shall be secured using TLS, consistent with the requirements for securing AS-SIP messages using TLS in UCR 2008, Change 1, Section 5.4, Information Assurance Requirements. This security shall provide mutual authentication between the LSC and the RTS Routing Database, message confidentiality for the DB update and DB response, and message integrity for the DB update and DB response.

[Required: LSC, RTS Routing Database] The DB update interface between the LSC and the RTS Routing Database shall traverse the data firewalls (and not the RTS EBC firewalls) at both the LSC and RTS Routing Database sites.

[Required: LSC, RTS Routing Database] The DB update interface between the LSC and the RTS Routing Database shall traverse the CE Routers at both the LSC and RTS Routing Database sites, using the UCR 2008 Change 1 DSCP for OA&M traffic, and the associated CE Router queues.

[Required: LSC] The DB update interface between the LSC and the RTS Routing Database shall terminate on the Ethernet interface used for VVoIP signaling and bearer traffic at the LSC, as described in UCR 2008, Change 1, Section 5.4, Information Assurance Requirements.

[Conditional: LSC] Initially, the RTS Routing DB may be deployed at an RTS MFSS site or an RTS WAN SS site. In this case, the LSC may implement a local RTS Routing DB that is a "mirror copy" of the remote RTS Routing DB deployed at the MFSS or WAN SS site. The RTS can use this "local mirror" RTS Routing DB for call setup performance efficiencies.

5.3.2.24 Requirements for Supporting AS-SIP-Based Ethernet Interfaces for Voicemail, Unified Messaging Systems, and Automated Receiving Devices

The following Conditional Requirements are being added in UCR 2008, Change 1, to add LSC, MFSS, and WAN SS support for AS-SIP-Based Ethernet Interfaces for voicemail systems, Unified Messaging systems, and ARDs. The condition here is that the LSC, MFSS, and WAN SS support an AS-SIP-based Ethernet interface for interconnection with a standalone voicemail system, Unified Messaging system, or ARD. This interface is in addition to any vendor-proprietary interface that the LSC, MFSS, or WAN SS may already support for interconnection with a vendor-proprietary voicemail system, Unified Messaging system, or ARD. Automated Receiving Devices are defined in UCR 2008, Section 5.2.12.3.5.5.

[Conditional: LSC, MFSS, WAN SS] The LSC, MFSS, and WAN 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."

[Conditional: LSC, MFSS, WAN SS] The LSC, MFSS, and WAN SS shall support all mandatory requirements in IETF Internet Draft draft-levy-sip-diversion-08.txt, Diversion Indication in SIP. Per this Internet Draft:

> "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)."

[Objective: LSC, MFSS, WAN SS] It is an objective that the LSC, MFSS, and WAN SS shall also support all mandatory requirements in IETF Internet Draft draft-levy-sip-diversion-09.txt, Diversion Indication in SIP. (draft-levy-sip-diversion-09.txt is dated May 1. 2009; draft-levy-sip-diversion-08.txt is dated August 25, 2004.)

[Conditional: LSC, MFSS, WAN SS] The LSC, MFSS, and WAN 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."

[Conditional: LSC, MFSS, WAN SS] The LSC, MFSS, and WAN 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."

5.3.2.25 RTS Precedence Call Diversion

These RTS requirements are based on the DSN requirements for Precedence Call Diversion (PCD) in UCR 2008, Section 5.2.2.3. The following RTS limitations apply:

1. Support for Precedence Call Diversion from one RTS EI to another RTS EI on the same LSC (or internal LSC within an MFSS or WAN SS) is required.

2. Support for Precedence Call Diversion from an RTS EI on one LSC to an RTS EI on another LSC is required.

3. Support for Precedence Call Diversion from an RTS EI on an LSC to a DSN EI (on an EO, SMEO, PBX1, or PBX 2) is not required.

4. Support for Precedence Call Diversion from a DSN EI (on an EO, SMEO, PBX1, or PBX 2) to an RTS EI on an LSC is not required.

[Required: LSC, MFSS – Conditional: WAN SS] The AS-SIP signaling appliance shall divert ALL unanswered RTS VoIP calls above the ROUTINE precedence level to a designated RTS 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. This PCD time period shall be configurable to be less than the Call Forwarding time period for unanswered calls that are forwarded to voicemail and ACD systems.

[Required: LSC, MFSS – Conditional: WAN SS] Unanswered RTS VoIP calls above the ROUTINE precedence level shall not be forwarded to voicemail, and shall not be forwarded to ACD systems. Instead, they should divert to the PCD DN when the PCD time period expires.

[Required: LSC, MFSS – Conditional: WAN SS] Unanswered RTS VoIP calls at the ROUTINE precedence level shall still be forwarded to voicemail or to ACD systems (when Call Forwarding Don't Answer is assigned to the called RTS DN), even though PCD is enabled and configured for the AS-SIP signaling appliance.

[Required: LSC, MFSS – Conditional: WAN SS] Calls above the ROUTINE precedence level that are destined to (directly dialed to) DNs assigned to voicemail or ACD systems shall only 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).

[Required: LSC, MFSS – Conditional: WAN SS] ROUTINE precedence level calls that are destined to (directly dialed to) DNs assigned to voicemail or ACD systems shall be allowed. The AS signaling appliance shall support a per-appliance configuration option that, when activated, also diverts these ROUTINE calls 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 (e.g., until the separate Call Forwarding Don't Answer feature for that system's DN takes over), and shall not be diverted by PCD.

Precedence Call Diversion may divert calls to the DN of an Attendant Console (or group of attendant consoles). End users can also place precedence calls directly to this attendant console (or group of attendant consoles) by dialing its number from their EIs. The following requirements cover the handling of these precedence calls in these cases. Each attendant console is an RTS EI served by an RTS LSC in the subsequent requirements.

[Required: LSC, MFSS – Conditional: WAN SS] Incoming precedence calls to the attendant's listed DN, and incoming calls that are diverted to this attendant DN, shall be placed in a queue for the attendant console (or group of attendant consoles). A distinctive visual signal indicating the precedence level of the call (including ROUTINE, when a ROUTINE call is placed or diverted to the attendant's DN) shall be sent to the attendant console (or group of attendant consoles) when this call is queued.

[Required: LSC, MFSS – Conditional: WAN SS] When a group of attendant consoles on the same LSC is used, and calls are either placed or diverted to the attendant console DN, call distribution across the Console Group shall be used to reduce excessive caller waiting times. Each attendant console in the group shall operate from a common queue (or common set of queues) associated with the Console DN.

[Required: LSC, MFSS – Conditional: WAN SS] Incoming calls (placed and diverted) to the console DN shall be queued for attendant service by call precedence and time of arrival. The highest precedence call with the longest holding time in the queue shall be offered to an attendant first.

[Required: LSC, MFSS – Conditional: WAN SS] A recorded message of explanation (e.g., ATQA) shall be applied automatically to all the waiting calls in the Attendant Console queue (refer to Table 5.3.4-9, Announcements).

NOTE: In the set of announcements in Section 5.3.4, AS-SIP Requirements, Table 5.3.4-9 (i.e., BPA, Unauthorized Precedence Announcement (UPA), BNEA, ATQA), ATQA is now a 2010 requirement.

5.3.2.26 RTS Attendant Station Features

These RTS requirements are based on the DSN requirements for Attendant Station Features in UCR 2008, Section 5.2.1.2. The following RTS limitations apply:

1. In these requirements, the RTS Attendant Station (attendant console) is an RTS EI that serves other RTS EIs on the same LSC.

2. Support for an RTS Attendant Station that serves other RTS EIs on other LSCs, or serves DSN EIs on DSN switches, is not required.

3. Support for the "Class of Service Override" and "Busy Override and Busy Verification" features, in cases where the served EI and the Attendant Station EI are on the same LSC, is required.

4. Support for the "Class of Service Override" and "Busy Override and Busy Verification" features, in cases where the served EI and the Attendant Station EI are different LSCs (or one is on a DSN switch and the other is on an LSC), is not required. This is due to limitations in AS-SIP and T1.619A PRI signaling that prevent these features from being provided on an LSC-to-LSC or LSC-to-EO basis.

5. In these requirements, the RTS Attendant Station can be either a proprietary RTS EI or an AS-SIP RTS EI. AS-SIP EI requirements for attendant stations are not included in Change 1, but may be included in the next release of the UCR.

Attendant features in this section apply to RTS Attendant Consoles that are provided as part of the local LSC, MFSS, or WAN SS SUT, or provided by an external CPE attendant console, as implemented by the MILDEP acquisition agent.

5.3.2.26.1 Precedence and Preemption

[Required: LSC, MFSS – Conditional: WAN SS] The RTS Attendant Console shall interoperate with PBAS/ASAC as described in

- Section 5.3.2.7.2.1, PBAS/ASAC Requirements
- Section 5.3.2.2.2.3, ASAC – Open Loop
- Section 5.3.4.10, Precedence and Preemption

The console shall be able to initiate all levels of RTS precedence calls (i.e., ROUTINE through FLASH-OVERRIDE).

5.3.2.26.2 Call Display

[Required: LSC, MFSS – Conditional: WAN SS] The RTS Attendant Console shall provide a visual display of each precedence level and the calling number, for incoming direct dialed calls to the attendant, and diverted calls to the attendant (e.g., calls that reach the attendant through PCD).

The AS-SIP trunks and T1.619A PRI trunks support delivery of precedence level and calling number information on incoming calls to RTS LSCs. This means that the precedence level and the calling number should be available to the attendant console, for incoming calls that originate from outside of the LSC.

[Conditional: LSC, MFSS, WAN SS] If the LSC, MFSS, or WAN SS supports assignment of a CoS to an individual EI, then the RTS Attendant Console shall also provide a visual display of the calling EI's CoS, for incoming direct dialed calls to the attendant, and diverted calls to the attendant.

The AS-SIP trunks and T1.619A PRI trunks do not support delivery of CoS information on incoming calls to RTS LSCs. This means that CoS information will not be available to the attendant console for incoming calls that originate from outside of the LSC. The COS information may be available to the attendant console for calls that originate within the LSC.

5.3.2.26.3 Class of Service Override

[Conditional: LSC, MFSS, WAN SS] If the LSC, MFSS, or WAN SS supports assignment of a CoS to an individual EI, then this appliance and the attendant console shall give the attendant the ability to override any incoming call's calling party CoS (based on calling area or precedence) on a call-by-call basis.

The appliance and the attendant console shall also give the attendant the ability to override any diverting call's calling party class of service (based on calling area or precedence) on a call-by-call basis.

5.3.2.26.4 Busy Override and Busy Verification

[Required: LSC, MFSS – Conditional: WAN SS] The appliance and the attendant console shall give the attendant the ability to verify and override a busy line condition. In commercial VoIP networks, attendant verification of a busy line is called Busy Line Verification (BLV), and attendant override of a busy line is called Emergency Interrupt. In the RTS network, support for these BLV and Emergency Interrupt capabilities is

- Required when the "busy line" is an RTS EI served by the local RTS appliance.

- Conditional when the "busy line" is an RTS EI served by a remote RTS appliance.
  - The condition here is that the Attendant's appliance, the remote appliance, and any intermediate appliances all have to support the SIP requirements for BLV and Emergency Interrupt signaling in RFC 3503. In RFC 3501, the "P-DCS-OSPS: BLV" header indicates an attendant's request for BLV, and the "P-DCS-OSPS: EI" header indicates an attendant's request for Emergency Interrupt.

- Not required when the "busy line" is a DSN EI served by a DSN switch.

[Required: LSC, MFSS, Conditional – WAN SS] If the attendant uses BLV on a called line, and that called line (called EI) is busy, the appliance and the attendant console shall give an audible and visual "called line busy" indication back to the attendant.

The appliance and attendant console shall also allow the attendant to request the Emergency Interrupt feature in this case.

[Required: LSC, MFSS, Conditional – WAN SS] The appliance and the attendant console shall prevent an attendant from activating BLV or Emergency Interrupt to called lines and called numbers that are located in the commercial network (the PSTN).

[Required: LSC, MFSS – Conditional: WAN SS] The appliance and the attendant console shall give the attendant the ability to use Emergency Interrupt to interrupt an existing call on a busy line, and inform the busy user of a new incoming call. The appliance and the Attendant console shall provide an override tone to the busy user before the attendant entering the conversation, and they shall repeat the tone periodically for as long as the attendant is connected to the busy user.

[Required: LSC, MFSS, Conditional – WAN SS] The appliance shall give selected destination EIs the ability to be exempt from Emergency Interrupt and attendant break-in. In particular, it shall be possible for the appliance to preclude the BLV and Emergency Interrupt services from being applied to selected destination EIs (e.g., EIs that provide secure voice service).

5.3.2.26.5 Night Service

[Required: LSC, MFSS, Conditional – WAN SS] The appliance and the attendant console shall have the ability to route all calls that are normally directed to the console to a separate night service deflection number. The night service deflection number shall be a fixed (preconfigured) or manually-selected DN.

5.3.2.26.6 Automatic Recall of Attendant

[Required: LSC, MFSS – Conditional: WAN SS] When an attendant redirects an incoming call to a destination station, and that station is either busy or does not answer the call within a preset time, the appliance and the attendant console shall ensure that calling party on the redirected call is recalled automatically to the console.

[Required: LSC, MFSS – Conditional: WAN SS] In this case, the appliance shall ensure that that the “recalled” call is returned to the console that originally processed the call. If that console is busy, the appliance shall ensure that the “recalled” calls is placed into the queue for that console. But if that console is out of service, then the appliance shall ensure that the “recalled” call is routed to another console on that appliance, if another console is available.

5.3.2.26.7 Calls in Queue to the Attendant

[Required: LSC, MFSS – Conditional: WAN SS] The appliance and the attendant console shall have the ability to place calls (both directed to the attendant and diverted to the attendant) into a waiting queue. The appliance and the attendant console shall ensure that calls placed in queue to the attendant are retrieved by the attendant in order of their precedence level (i.e., FLASH-OVERRIDE first, ROUTINE last) and the longest holding time within that precedence level.

[Required: LSC, MFSS – Conditional: WAN SS] The appliance and the attendant console shall ensure that calls in the attendant queue are not lost when a console is placed out of service or has its calls forwarded to a night service deflection number. When the console is placed out of service or forwarded to night service while calls are in queue, the appliance and the console shall be capable of one of the following solutions to ensure that calls are not lost:

1. All the existing calls in the queue shall be forwarded first to a separate DN for the centralized attendant (i.e., a different attendant at a different attendant console), and then on to the night service DN (if the centralized attendant activated night service deflection).

2. All subsequent calls placed to the attendant console shall be forwarded first to the separate DN for the centralized attendant, and then on to the night service DN (if the centralized attendant activated night service deflection). For the existing calls in the queue, the attendant remains at the console and answers all these remaining calls (even though the attendant placed the console out of service or forwarded the console to night service deflection), thereby preventing any of the calls from being lost.

5.3.2.27 Directory Services (“White Pages”)

The CVVoIP will have a directory services capability for searching White pages that allow subscribers to look up specific and applicable user information assigned to other CVVoIP subscribers. This was considered an FY 2012 Objective requirement and was initially included for consideration by LSC/SS product development teams. The directory system will be of the same design and hardware as for SBU VVoIP, but for security reasons, this will be a separate implementation. At the end of FY 2010, a centralized, multivendor supported, standards-based, directory schema based on Microsoft Active Directory will be implemented. Figure 5.3.2.27-1, Centralized Directory (White Pages) Service, illustrates the white pages directory arrangement.

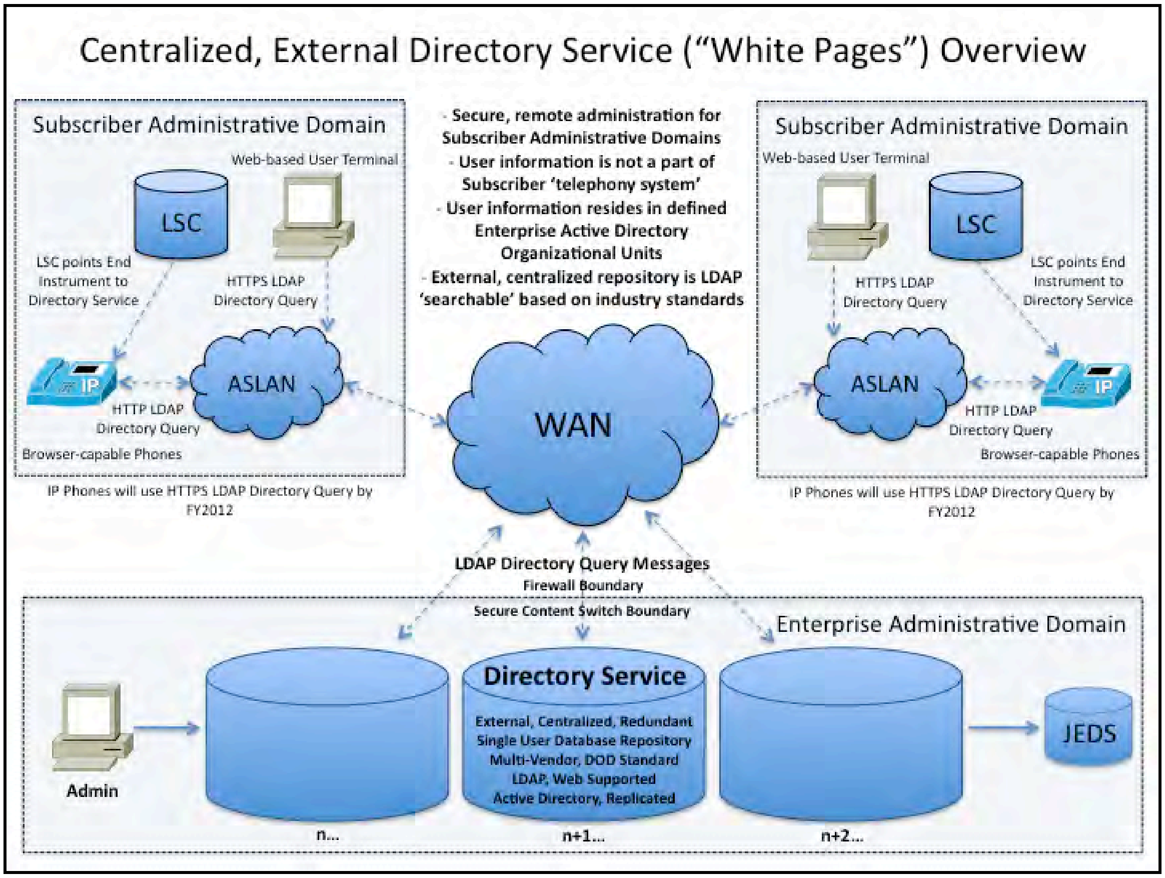

Centralized, External Directory Service ("White Pages") Overview
Subscriber Administrative Domain
Web-based User Terminal
LSC
LSC points End Instrument to Directory Service
HTTPS LDAP Directory Query
IP
ASLAN
HTTP LDAP Directory Query
Browser-capable Phones
IP Phones will use HTTPS LDAP Directory Query by FY2012
- Secure, remote administration for Subscriber Administrative Domains
- User information is not a part of Subscriber 'telephony system'
- User information resides in defined Enterprise Active Directory Organizational Units
- External, centralized repository is LDAP 'searchable' based on industry standards
WAN
Subscriber Administrative Domain
Web-based User Terminal
LSC
HTTPS LDAP Directory Query
LSC points End Instrument to Directory Service
ASLAN
IP
HTTP LDAP Directory Query
Browser-capable Phones
IP Phones will use HTTPS LDAP Directory Query by FY2012
LDAP Directory Query Messages
Firewall Boundary
Secure Content Switch Boundary
Enterprise Administrative Domain
Admin
Directory Service
External, Centralized, Redundant Single User Database Repository Multi-Vendor, DOD Standard LDAP, Web Supported Active Directory, Replicated
JEDS
n...
n+1...
n+2...

Figure 5.3.2.27-1. Centralized Directory (White Pages) Service

The following general requirements have been defined for the centralized directory (white pages) service:

1. Use of External and Centralized "Corporate" Directory.

   a. Location and Architecture Design. The global Directories Services architecture will be consolidated and external to all other attached subscriber "telephony systems." The architecture will be distributed in design to support redundancy and survivability as illustrated in Figure 5.3.2.27-1. All telephony user information will reside within the centralized Directory Services' Active Directory database and will not be part of any independent LSC/SS.

   b. Maintenance, Administrative, and Management Responsibility. Overall responsibility to maintain the global Directory Services' user's database structure will reside with DISA NS4 and the GNSC. Maintenance responsibility will be a DISA NS4 role, with management of individual Active Directory organizational units being delegated to each individual LSC/SS telephony system administrator. This decentralized administrative responsibility within the Active Directory schema will ensure a constant and updated database of user information.

c. Synchronization with the Local (LSC/SS) and DRSN Directories. The local LSC/SS user database for each Active Directory organizational unit will be automatically synchronized within the larger Directory Services' Active Directory server architecture as soon as the LSC/SS administrator provisions the user information within the system. Individual LSC/SS administrators are 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 will be the responsibility of DISA NS4 and will be statically updated as DRSN systems are modified and user information is updated from the field. As a minimum, this is expected to be accomplished at least once a year.

d. Redundancy, Survivability, and Recovery. Redundancy and survivability, as well as disaster recovery, are designed into the Directory Service architecture. DISA NS4 is the responsible agency for design, maintenance, and backup of the system.

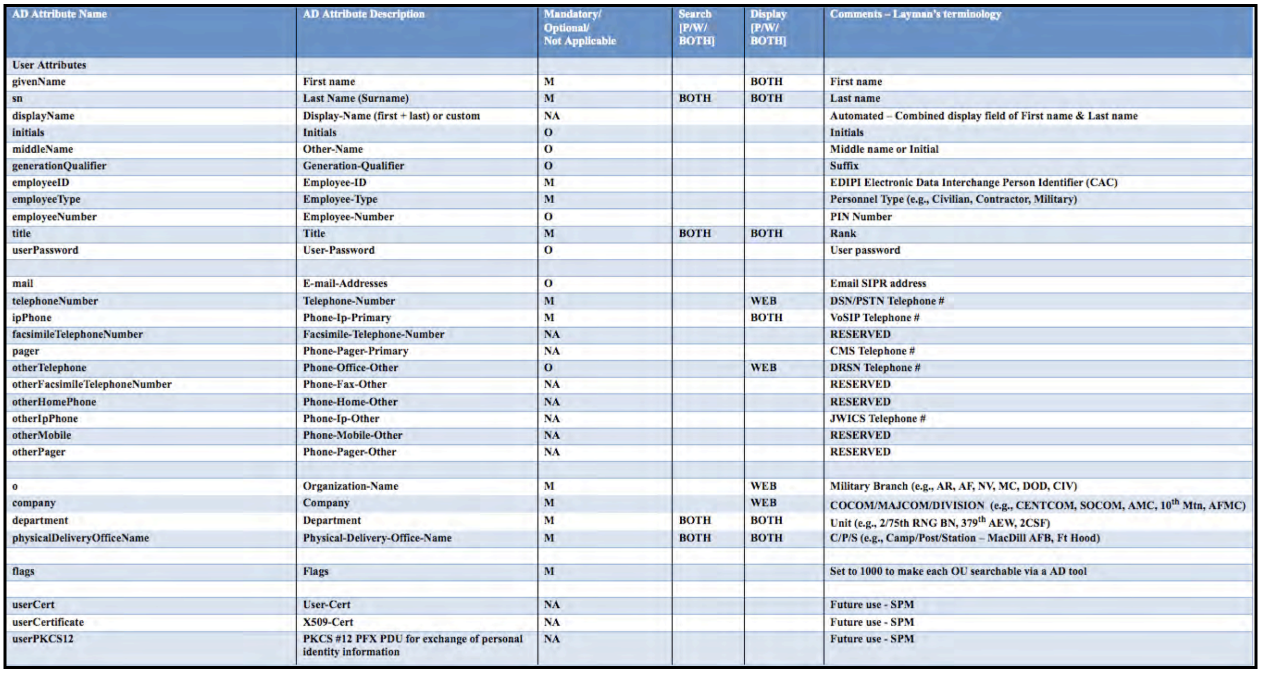
2. Definition of Multivendor Standards Items.

a. Active Directory Defined Attributes (Common Set of Fields). Figure 5.3.2.27-2, Directory Service Attribute Information, provides attribute details.

b. Length and ACSII Characters of Each Attribute Field. ASCII characters supported by Active Directory will be limited to characters that are supported by both LSC/SS enclaves and the DRSN system. These are necessary to ensure proper display of white pages' results. Alphanumeric characters that are supported are: (0123…, abcd…, ABCD), periods (.), dashes (-), and commas (,).

Length of fields is set within Active Directory and is the basis of what is supported.

c. "Ownership," administration, and management responsibility of each organizational unit and its fields.



AD Attribute Name	AD Attribute Description	Mandatory/ Optional/ Not Applicable	Search [P/W/ BOTH]	Display [P/W/ BOTH]	Comments – Layman's terminology
User Attributes					
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 & 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 #
otherTelephone	Phone-Office-Other	O		WEB	DRSN Telephone #
otherFacsimileTelephoneNumber	Phone-Fax-Other	NA			RESERVED
otherHomePhone	Phone-Home-Other	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 via a AD tool
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

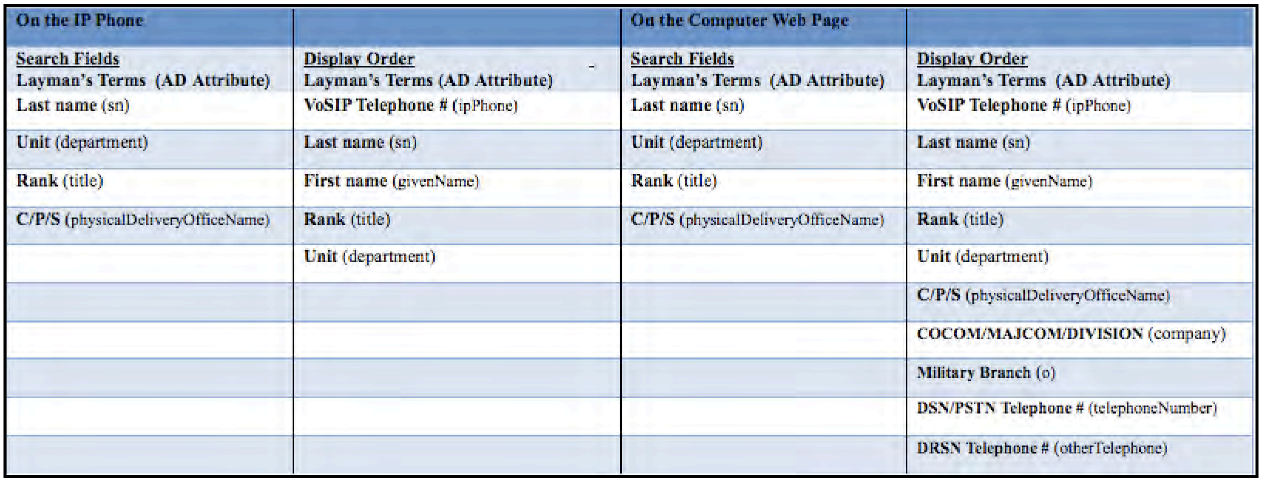
Figure 5.3.2.27-2. Directory Service Attribute Information

Each individual LSC/SS administrator will "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 will be added, modified, and/or deleted to the assigned Directory Service Active Directory organizational unit within the domain. Each LSC/SS administrator will use the designed provisioning tool DISA NS4 has developed that simplifies the task and ensures continuity of required user database information.

3. Search Criteria and Display Presentation for EIs (Computers and IP Phones). Figure 5.3.2.27-3, Directory Service Search and Display Criteria, provides the details.

   a. LDAP Criteria and Browser (Display) Functionality. Industry standard LDAP connection protocols (port 389) are used and supported.

      Standardized browser support for computer white pages functionality (parsing and display of search results) is restricted to secure web protocols (TLS/HTTPS) only. This is part of the Directory Services architecture capability and ensures the privacy and security of user information to authorized viewers.



On the IP Phone		On the Computer Web Page	
Search Fields Layman's Terms (AD Attribute) Last name (sn)	Display Order Layman's Terms (AD Attribute) VoSIP Telephone # (ipPhone)	Search Fields Layman's Terms (AD Attribute) Last name (sn)	Display Order Layman's Terms (AD Attribute) VoSIP Telephone # (ipPhone)
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 # (telephoneNumber)
			DRSN Telephone # (otherTelephone)

Figure 5.3.2.27-3. Directory Service Search and Display Criteria

Standardized browser support for IP phone white pages functionality (parsing and display of search results) is mandatory so web-based (HTML/XHTM) user information can be displayed. Until FY 2012, display of unsecure web protocols is supported (HTTP). After FY 2012, only secure web protocols (TLS/HTTPS) will be supported.

4. Definition of EI Display Fields.

a. Browser Requirements. End Instruments (e.g., IP Phones) will 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 and 8.X, are recommended.

b. Character Fields (Attributes). See Figure 5.3.2.27-3 for details.

c. Length of Attribute Fields.

(1) Web Browsers. The length of the displayed fields on the web interface of a computer are matched and validated with the limitations/policies imposed by the underlying directory server schema definition. Search results are presented in multiple lines with more display information available because of the size of the screening area. On each line, the web browser will 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 can be configured to be truncated to preset values on a per-attribute basis. This is accomplished using the Directory Service web-based administrative interface. If attributes with additional characters are stored in the underlying directory

server, the web-based user interface will truncate the displayed content to the limits imposed by the Directory Service application configuration parameters. All these parameters have been set to optimal lengths given the size of the screening area computers offer.

(2) End Instruments. Search results are presented in multiple lines. On each line, the phone will 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, the phone user interface will 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 5.3.2.27-3, Directory Service Search and Display Criteria, for details.

e. Soft/Hard Key Functions (such as a "directory access button"). The LSC/SS manufacturers are required to provide a single action, "directory access" function through either software and/or hardware on all supported, JITC-certified IP Phones. Through these methods, the action has to be a programmable, web-based function key that can have a URL. This will allow users the capability to use one button to start all actions when using the Directory Service.

THIS PAGE LEFT INTENTIONALLY BLANK