TABLE OF CONTENTS

SECTION **PAGE**

Section 2 Session Control Products 2-1
2.1 Network Engineering Attributes 2-1
2.1.1 Quality of Service Features 2-2
2.1.2 Assured Services Features and Capabilities 2-4
2.1.2.1 Attributes Within the Edge Segment 2-5
2.1.2.2 Attributes Within the DISN WAN (Access/Distribution and Core)........ 2-5
2.1.2.3 E2E Protocol Planes 2-6
2.1.2.4 Assured Services Subsystem 2-6
2.1.3 Voice and Video Signaling Design 2-9
2.1.4 Distributed UC Services Model 2-11
2.1.5 Session Control Failover Feature 2-12
2.2 Enterprise UC Services Design 2-14
2.2.1 Enterprise UC Vision 2-14
2.2.2 Enterprise System Design 2-15
2.2.3 The Enterprise Continuity of Operations (COOP) Capabilities 2-16
2.2.3.1 Environment Type 1 2-16
2.2.3.2 Environment Type 2 2-17
2.2.3.3 Environment Type 3 2-18
2.2.4 Messaging (IM/Chat/Presence) Integration 2-19
2.2.5 Enterprise Directory Services (EDS) 2-20
2.3 Mobility and Service Portability 2-25
2.4 ASAC Operation Overview 2-26
2.4.1 ASAC Budgets and Counts 2-27
2.4.1.1 Voice Budgets and Counts 2-27
2.4.1.2 Video Budgets and Counts 2-27
2.4.2 ASAC Session Control Overview 2-28
2.4.2.1 Outbound (Originating-Outgoing) Voice Sessions 2-28
2.4.2.2 Inbound (Incoming-Terminating) Voice Sessions 2-28
2.4.2.3 Directionalization 2-29
2.4.2.4 Video Session Processing 2-29
2.5 Precedence-Based Assured Services 2-30
2.6 Voice Features and Capabilities 2-31
2.6.1 Call Forwarding 2-31
2.6.2 Precedence Call Waiting 2-32

2.6.3 Call Transfer 2-33
2.6.4 Call Hold 2-33
2.6.5 Three-Way Calling 2-34
2.6.6 Hotline Service 2-34
2.6.7 Calling Number Delivery 2-34
2.6.8 Call Pick-Up 2-35
2.6.9 Precedence Call Diversion 2-35
2.6.10 Public Safety Voice Features 2-36
2.6.10.1 Basic Emergency Service (911) 2-36
2.6.10.2 Tracing of Terminating Calls 2-36
2.6.10.3 Outgoing Call Tracing 2-36
2.6.10.4 Tracing of a Call in Progress 2-37
2.6.10.5 Tandem Call Trace 2-37
2.7 End Instruments 2-37
2.7.1 Voice over IP Sampling Standard 2-38
2.7.2 Operational Framework for AS-SIP EIs 2-39
2.7.2.1 AS-SIP Secure Voice EI Supplementary Services 2-40
2.7.3 V.150.1 Modem Relay Secure Phone 2-41
2.7.3.1 Architecture for Supporting SCIP/V.150.1 Modem Relay 2-41
2.7.3.2 SCIP/V.150.1 Gateway 2-44
2.7.3.3 SCIP/V.150.1 End Instrument 2-45
2.8 Session Controller 2-46
2.9 AS-SIP Gateways 2-49
2.9.1 AS-SIP TDM Gateway 2-49
2.9.1.1 Overview 2-49
2.9.1.2 AS-SIP TDM Gateway Functional Reference Model 2-50
2.9.2 AS-SIP IP Gateway 2-52
2.9.2.1 Overview 2-52
2.9.2.2 AS-SIP IP Gateway Functional Reference Model, Assumptions, Functions and Features 2-53
2.9.3 AS-SIP – H.323 Gateway 2-55
2.9.3.1 Overview 2-55
2.9.3.2 AS-SIP – H.323 Gateway Functional Reference Model 2-57
2.9.3.3 Summary of AS-SIP – H.323 Gateway Functions and Features 2-58
2.9.3.4 AS-SIP – H.323 Gateway CCA Function Overview 2-59
2.10 Network-Level Softswitch 2-60
2.10.1 SS Functional Reference Model, Assumptions and Signaling Interfaces 2-61
2.10.1.1 Assumptions – SS 2-61

2.10.1.2 Signaling Interfaces – SS 2-63
2.11 Call Connection Agent 2-64
2.11.1 Introduction 2-64
2.11.2 Functional Overview of the CCA 2-65
2.11.2.1 CCA IWF Component 2-67
2.11.2.2 CCA MGC Component 2-67
2.11.3 CCA Interaction With Network Appliances and Functions 2-67
2.11.3.1 CCA Interactions With Transport Interface Functions 2-67
2.11.3.2 2CCA Interactions With the SBC 2-68
2.11.3.3 CCA Support for Admission Control 2-69
2.11.3.4 CCA Support for User Features and Services 2-69
2.11.3.5 CCA Support for Information Assurance 2-70
2.11.3.6 CCA Interactions With Session Controller Location Service 2-70
2.11.3.7 CCA Interactions With Softswitch Location Service 2-71
2.11.3.8 CCA Interactions With End Instrument(s) 2-71
2.11.3.9 CCA Interactions With Service Control Functions 2-71
2.12 Media Gateway 2-72
2.12.1 Introduction 2-72
2.12.2 Overview of the MG and MGC Functions 2-74
2.12.2.1 Primary Trunk Functions and Interfaces 2-75
2.12.2.2 Primary Access Functions and Interfaces 2-75
2.12.2.3 MGC Functions 2-76
2.12.3 Role of the MG in Appliances 2-77
2.12.3.1 Role of the MG in the SC 2-77
2.12.3.2 Role of the MG in the SS 2-79
2.12.4 MG Interaction With NES and Functions 2-80
2.12.4.1 MG Support for ASAC 2-80
2.12.4.2 MG and Information Assurance Functions 2-81
2.12.4.3 MG Interaction With Service Control Functions 2-82
2.12.4.4 Interactions With IP Transport Interface Functions 2-82
2.12.4.5 MG-SBC Interaction 2-83
2.12.4.6 MG Support for Appliance Management Functions 2-84
2.12.4.7 Interactions With VoIP EIs 2-84
2.12.5 MG and Echo Cancellation 2-84
2.12.5.1 Echo Control Design 2-84
2.12.6 MG and Synchronization 2-86
2.12.7 MGC-MG CCA Functions 2-86
2.12.8 Remote Media Gateway Requirements 2-86

2.13 Session Border Controller 2-88
2.14 Worldwide Numbering and Dialing Plan 2-88
2.14.1 Domain Directory 2-92
2.15 Management of Network Appliances 2-94
2.15.1 Voice and Video Network Management Domain 2-95
2.15.2 General Management Approach 2-95
2.15.3 Traffic Flow Control Overview 2-97
2.15.3.1 Destination Code Controls 2-98
2.15.3.2 Call Budget Control 2-98
2.16 Dynamic ASAC 2-98
2.16.1.1 Dynamic ASAC Calculation Examples 2-103

LIST OF FIGURES

FIGURE **PAGE**

Figure 2.1-1. Overview of UC Network Attributes 2-2
Figure 2.1-2. Queuing Design Overview 2-3
Figure 2.1-3. Attributes of AS-SIP 2-6
Figure 2.1-4. Assured Services Subsystem Functional Diagram 2-7
Figure 2.1-5. SBU Voice and Video Services Signaling Design 2-9
Figure 2.1-6. End-to-End Two-Level SBU AS-SIP Network Signaling Design 2-11
Figure 2.1-7. Distributed UC Services Model 2-12
Figure 2.2-1. Enterprise UC Services Architecture 2-15
Figure 2.2-2. Environment Type 1 2-17
Figure 2.2-3. Environment Type 2 2-18
Figure 2.2-4. Environment Type 3 2-19
Figure 2.2-5. Multivendor Interoperability Normalized on XMPP 2-20
Figure 2.2-6. Basic Architecture for Providing EDS in the Enterprise UC Network 2-23
Figure 2.3-1. Mobile Warfighter’s Communication Dilemma 2-25
Figure 2.6-1. Call Forwarding Logic Diagram 2-32
Figure 2.6-2. Call Hold Scenarios 2-33
Figure 2.7-1. Framework for Proprietary and AS-SIP EIs 2-40
Figure 2.7-2. Framework for SCIP Phones Using VoIP 2-43
Figure 2.7-3. Framework for SCIP Phones Using Modem Relay 2-44
Figure 2.8-1. Functional Reference Model – SC 2-47
Figure 2.9-1. AS-SIP TDM Gateway Topologies 2-50
Figure 2.9-2. Functional Reference Model – AS-SIP TDM Gateway 2-51
Figure 2.9-3. AS-SIP IP Gateway Topology 2-53
Figure 2.9-4. Functional Reference Model – AS-SIP IP Gateway 2-54
Figure 2.9-5. AS-SIP – H.323 Gateway Topology 2-57
Figure 2.9-6. Functional Reference Model – AS-SIP – H.323 Gateway 2-58
Figure 2.9-7. CCA Relationships 2-60
Figure 2.10-1. Functional Reference Model – SS 2-61
Figure 2.11-1. CCA Relationships With Functional Components 2-66
Figure 2.12-1. MGC – MG Layered Interface 2-74
Figure 2.12-2. MG Trunk Function 2-75
Figure 2.12-3. MG Primary Access Functions and Interfaces 2-76
Figure 2.12-4. Example IP Network Echo Control Design 2-85
Figure 2.12-5. Remote MG Architecture Diagram 2-87

Figure 2.15-1. Network Appliance Management Model 2-94
Figure 2.15-2. Relationship of UC Managements 2-95
Figure 2.16-1. AS-SIP Triggers for AVSC 2-101
Figure 2.16-2. Notional System Architecture for Examples 1, 2, and 4 2-103
Figure 2.16-3. Notional System Environment for Example 3 (Voice MUX with HAIPE Tunnel) 2-104

LIST OF TABLES

TABLE **PAGE**

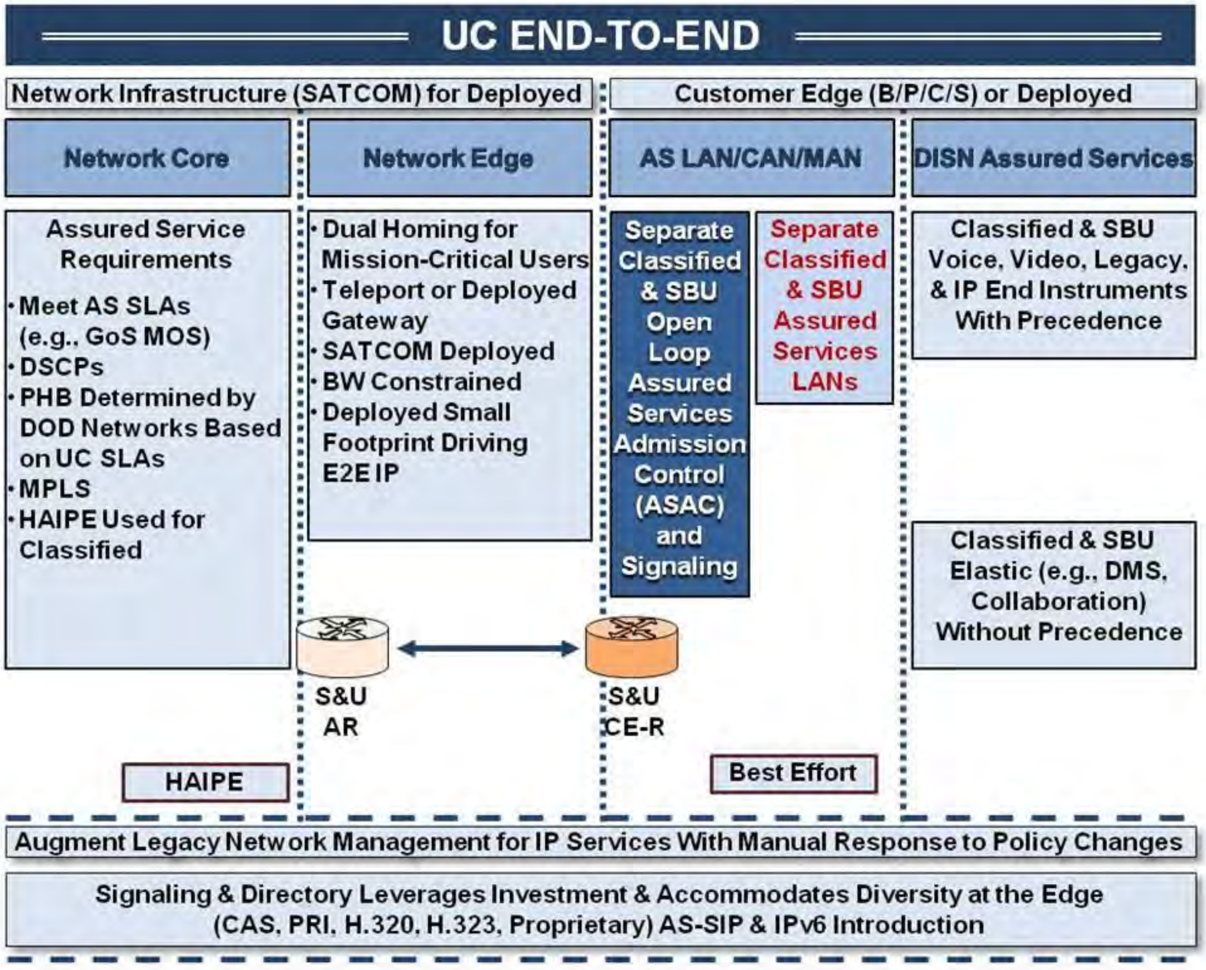
Table 2.8-1. Summary of SC Functions 2-48
Table 2.8-2. SC Support for VoIP and Video Signaling Interfaces 2-49
Table 2.9-1. AS-SIP TDM Gateway Support for VoIP and Video Signaling Interfaces .. 2-51
Table 2.9-2. Summary of AS-SIP IP Gateway Functions 2-55
Table 2.9-3. Summary of AS-SIP – H.323 Gateway Functions 2-58
Table 2.10-1. SS Support for VoIP and Video Signaling Interfaces 2-63
Table 2.12-1. SC MG Support for VoIP Signaling Interfaces 2-78
Table 2.12-2. SS MG Support for VoIP Signaling Interfaces 2-79
Table 2.12-3. Protocol Stack 2-88
Table 2.14-1. DSN User Dialing Format 2-88
Table 2.14-2. Examples of Internal DSN Numbers and Their Corresponding Global E.164 PSTN Telephone Numbers 2-90
Table 2.14-3. Mapping of DSN tel Numbers to SIP URIs 2-92
Table 2.14-4. White Pages Directory Data Elements 2-94
Table 2.16-1. EISC Estimation Parameters 2-99
Table 2.16-2. Example 1: Current Session Status (No HAIPE Case) 2-105
Table 2.16-3. Example 2: AVSC Calculation Assuming the G.711 Session Is New (HAIPE Case) 2-105
Table 2.16-4. Example 3: Use of Voice MUX With a HAIPE Tunnel 2-106
Table 2.16-5. Example 4: Use of Header Compression With a HAIPE Tunnel 2-107

SECTION 2
SESSION CONTROL PRODUCTS

2.1 NETWORK ENGINEERING ATTRIBUTES

The logical location of the major Unified Capabilities (UC) network attributes within the UC End-to-End (E2E) design is shown in Figure 2.1-1, Overview of UC Network Attributes. The location of attributes in terms of the Customer Edge (Base/Post/Camp/Station [B/P/C/S]), the Network Edge (Access) and the Network Core are depicted.

The functions contained in the boxes of Figure 2.1-1 constitute the scope of the Assured Services functions while the placement of the boxes indicates where in the overall design (Wide Area Network [WAN] to Edge) the functions logically reside. Voice, video, and data sessions are converged in the Defense Information Systems Network (DISN) WAN and the Assured Services (AS) Local Area Network (LAN) (ASLAN), while currently only voice and video sessions are supported by Assured Services.



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 UC SLAs
- MPLS
- HAIPE Used for Classified

- 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

Classified & SBU Voice, Video, Legacy, & IP End Instruments With Precedence

Classified & SBU Elastic (e.g., DMS, Collaboration) Without Precedence

Augment Legacy Network Management for IP Services With Manual Response to Policy Changes

Signaling & Directory Leverages Investment & Accommodates Diversity at the Edge (CAS, PRI, H.320, H.323, Proprietary) AS-SIP & IPv6 Introduction

LEGEND:

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

Figure 2.1-1. Overview of UC Network Attributes

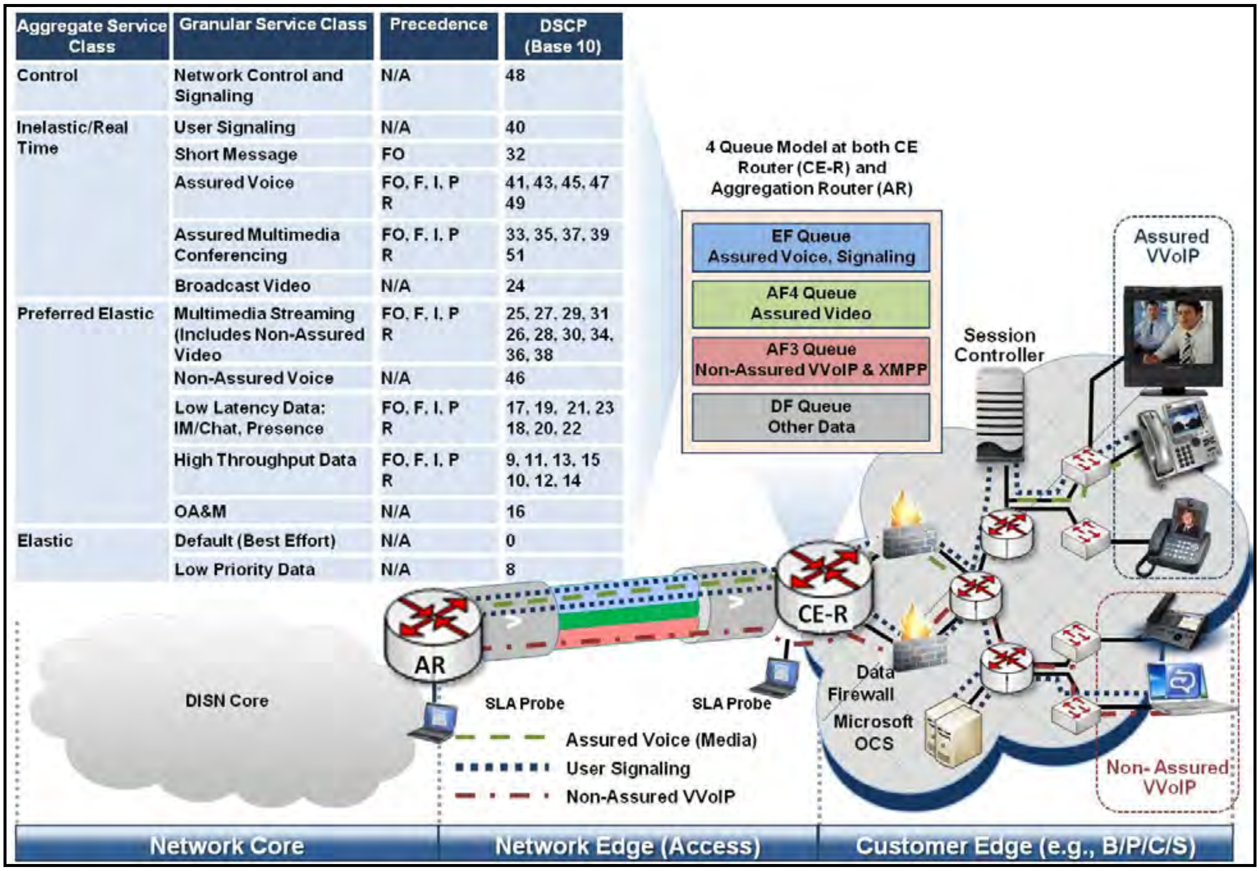
2.1.1 Quality of Service Features

Quality of Service (QoS) features are implemented within the DISN to provide different priority to the DISN UC Service Classes. The various DISN UC Service classes have different network bandwidth needs and use different transmission protocols to send their data. When these different types of data converge, and are sent on a shared link, one transmission can overwhelm another, resulting in a negative effect. The required QoS for each UC Aggregate Service Class is maintained by assigning Differentiated Services Code Points (DSCPs) to each DISN UC Service class and then assign the service classes into different queues.

There are four Aggregated Service Classes which in turn, are refined into 13 Granular Service Classes.

Each of the 13 Granular DISN UC Service Classes is mapped into a 6-queue structure or four-queue structure as described in Unified Capabilities Requirements (UCR) 2013, Section 6, Network Infrastructure End-to-End Performance. An example of the four-queue mapping is illustrated in Figure 2.1-2. Assured Voice, User Signaling, and Network Control Traffic are placed in the Expedited Forwarding (EF) queue. Assured Multimedia Conferencing (i.e., Video) traffic is placed in the Class 4 Assured Forwarding (AF4) queue. Preferred data, non-assured Voice and Video over Internet protocol (IP) (VVoIP); instant messaging (IM), Chat, and Presence; and Operations, Administration, and Maintenance (OA&M) traffic is placed in the Class 3 Assured Forwarding (AF3) queue. All other traffic (data and any other service) are placed in the Best Effort (Default) queue.

> NOTE: User Signaling associated with non-assured Voice and Video over Internet Protocol (VVoIP) is placed in the EF queue. Figure 2.1-2 shows the queue structure, DSCPs, and associated rules for each granular service class.



Aggregate Service Class	Granular Service Class	Precedence	DSCP (Base 10)
Control	Network Control and Signaling	N/A	48
Inelastic/Real Time	User Signaling	N/A	40
	Short Message	FO	32
	Assured Voice	FO, F, I, P R	41, 43, 45, 47 49
	Assured Multimedia Conferencing	FO, F, I, P R	33, 35, 37, 39 51
	Broadcast Video	N/A	24
Preferred Elastic	Multimedia Streaming (Includes Non-Assured Video	FO, F, I, P R	25, 27, 29, 31 26, 28, 30, 34, 36, 38
	Non-Assured Voice	N/A	46
	Low Latency Data: IM/Chat, Presence	FO, F, I, P R	17, 19, 21, 23 18, 20, 22
	High Throughput Data	FO, F, I, P R	9, 11, 13, 15 10, 12, 14
	OA&M	N/A	16
Elastic	Default (Best Effort)	N/A	0
	Low Priority Data	N/A	8

Figure 2.1-2. Queuing Design Overview

To ensure acceptable QoS in IP networks for assured VVoIP, it is necessary to assign the assured VVoIP traffic to different queues than non-assured VVoIP and data sessions on congested connections. Mixing assured VVoIP with non-assured VVoIP in the same aggregate service class (and queue) will result in the uncontrolled non-assured VVoIP degrading the assured VVoIP sessions on congested networks. To delineate the assured VVoIP from the non-assured VVoIP (and other types of packets), Internet protocol (IP) packets are marked with unique DSCPs.

The following discussion explains the differences between assured and non-assured VVoIP, and why they are assigned to two different queues:

Assured VVoIP traffic is subject to Session Admission Control (SAC). SAC policies control the number of sessions that are offered to the network. Session admission control can be provided by Session Controllers (SCs) or Gatekeepers (i.e., H.323 Gatekeepers) and is associated with establishing a budget for the number of simultaneous sessions and with ensuring that the number of active sessions is within that budget. Assured Services Admission Control (ASAC) extends SAC to allow sessions to be preempted when the SAC budget is at capacity and additional higher precedence sessions are offered.

SAC is not applied to non-assured VVoIP. Non-assured VVoIP typically is composed of peer-to-peer sessions that do not transit a centralized SAC appliance, (e.g., SC); therefore, SAC cannot be applied.

In addition to queuing, traffic conditioning is applied to the non-assured VVoIP packets. Enabling traffic conditioning on non-assured VVoIP packets may cause degradation on non-assured VVoIP sessions during periods of high usage, but will ensure that preferred data sessions continue to receive better than best effort performance in accordance with (IAW) the UCR performance objectives.

The bandwidth for each queue must be provided based on a sound traffic-engineering analysis, which includes the site budget settings, the site busy hour traffic load plus a 25 percent surge for voice and video traffic, plus a 10 percent aggregate overhead for signaling, Network Management (NM), and routing traffic.

Non-assured VVoIP users can only interoperate with an assured services VVoIP user via an Assured Services Session Initiation Protocol (AS-SIP) gateway. All non-assured VVoIP users must be traffic engineered and controlled, and must meet information assurance requirements.

2.1.2 Assured Services Features and Capabilities

A key component of the military robust VoIP and Video over IP design is the Assured Services subsystem. The Assured Services subsystem addresses Assured Services by replacing the current Time Division Multiplexing (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 End Instrument (EI)-to-EI basis, while functioning within a converged Department of Defense (DoD) UC network.

2.1.2.1 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 SCs 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 Mean Opinion Score (MOS) method.
3. Call Preemption. Lower precedence sessions will be preempted on the access circuit to accept the SC setup of higher precedence level outgoing or incoming session establishment requests.
4. Voice and Video Traffic Service Classification and Priority Queues. In terms of the Customer Edge (CE) Router (CE-R) queuing structure, voice and video traffic will be assigned to the higher priority queues by Aggregated Service Class as described in Section 2.1.1, Quality of Service Features.

2.1.2.2 Attributes Within the DISN WAN (Access/Distribution and Core)

Under the access part of the DISN WAN, dual homing is required between the CE-R and the Aggregation Router (AR) that serve an ASLAN having FLASH/FLASH OVERRIDE (F/FO) users, IMMEDIATE (I)/PRIORITY (P) users, and ROUTINE (R) users. Dual homing is optional for cases where only ROUTINE users (I/P [ROUTINE] and non-I/P users) are supported. The DISN Core part of the DISN WAN (i.e., from AR to AR) is assumed to be bandwidth rich for whatever AR queue the voice and video traffic is placed in. That is, the core bandwidth for assured voice and video traffic will match or exceed the expected bandwidth required for the voice/video busy-hour traffic in each of the DISN worldwide geographic locations. Since the ASLAN is required to be implemented as non-blocking for voice and video traffic, the access circuit from the Customer Edge Segment to the DISN Core Service Delivery Node (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 Multiprotocol Label Switching (MPLS) fast reroute (FRR) in the Network Core. Naturally, users are provided a lower availability if they choose not to or cannot implement dual homing.

2.1.2.3 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. Figure 2.1-3, Attributes of AS-SIP, illustrates the basic attributes of AS-SIP, which are critical to assured services, multivendor interoperability, and security.

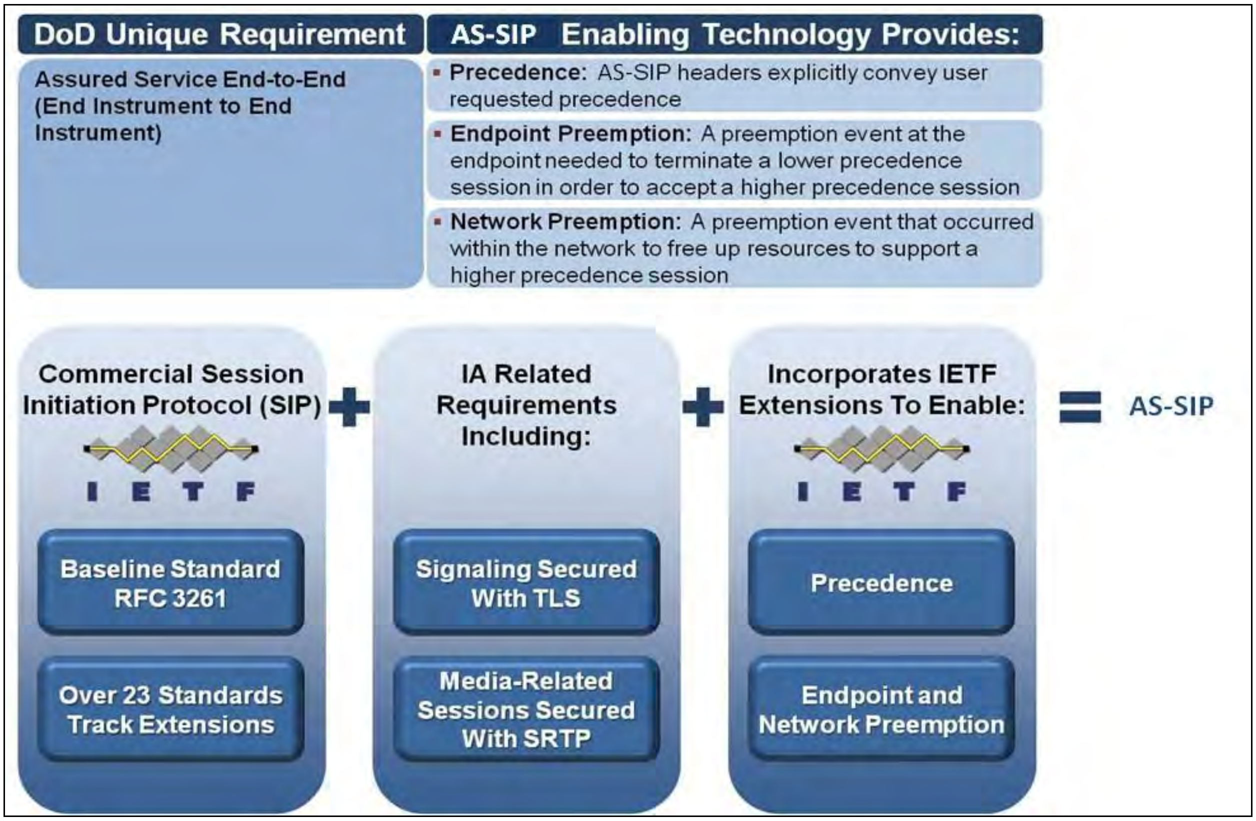

DoD Unique Requirement
AS-SIP Enabling Technology Provides:
Assured Service End-to-End (End Instrument to End Instrument)
Precedence: AS-SIP headers explicitly convey user requested precedence
Endpoint Preemption: A preemption event at the endpoint needed to terminate a lower precedence session in order to accept a higher precedence session
Network Preemption: A preemption event that occurred within the network to free up resources to support a higher precedence session
Commercial Session Initiation Protocol (SIP)
I E T F
Baseline Standard RFC 3261
Over 23 Standards Track Extensions
IA Related Requirements Including:
Signaling Secured With TLS
Media-Related Sessions Secured With SRTP
Incorporates IETF Extensions To Enable:
I E T F
Precedence
Endpoint and Network Preemption
AS-SIP

Figure 2.1-3. Attributes of AS-SIP

The transport plane is associated with the bearer traffic and protocols, such as Secure Real-Time Transport Protocol (SRTP) and Real-Time Transport Control Protocol (RTCP).

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

2.1.2.4 Assured Services Subsystem

The Assured Services subsystem, shown in Figure 2.1-4, Assured Services Subsystem Functional Diagram, the DISN WAN, and the ASLAN make up the total system. These components 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.

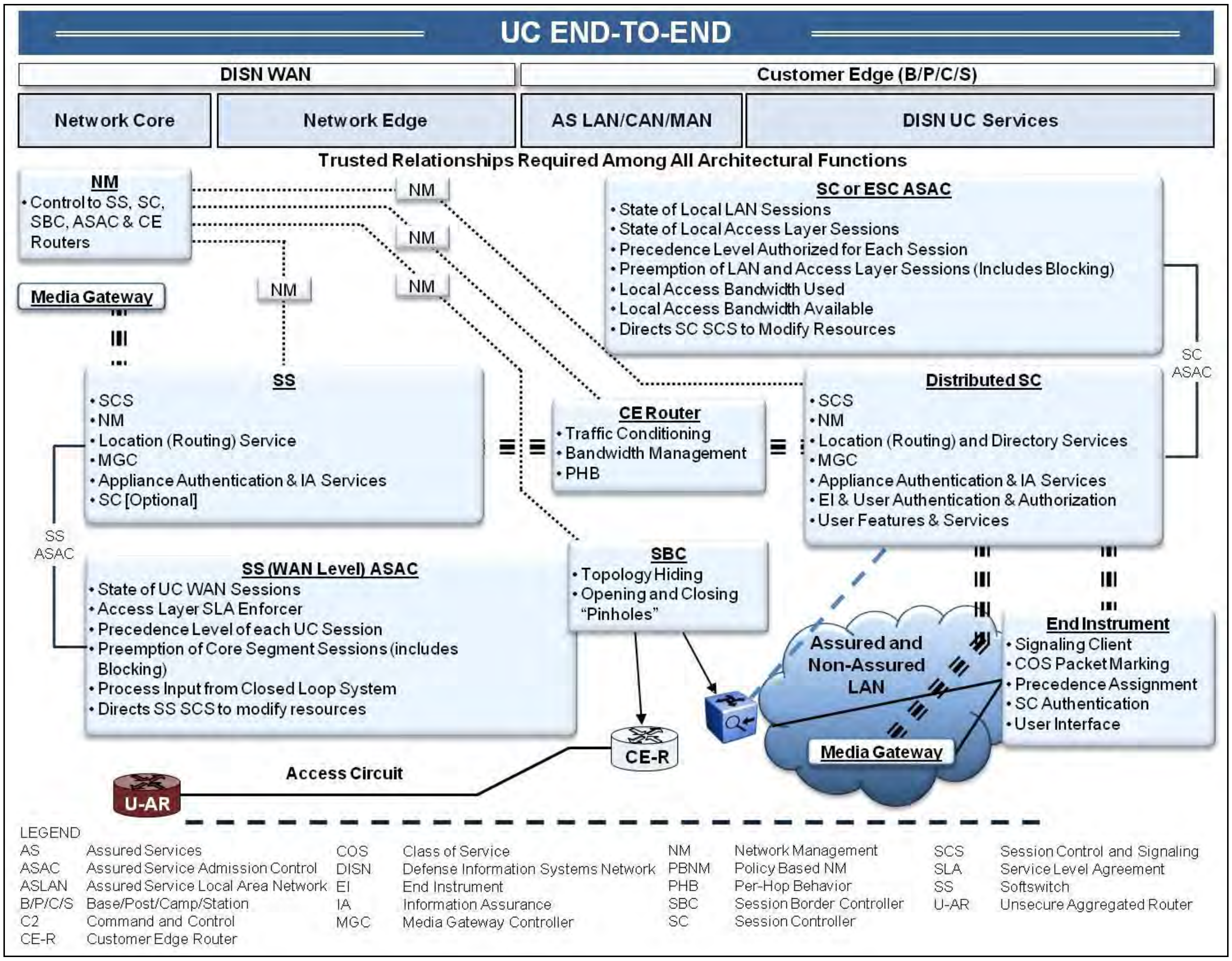

UC END-TO-END
DISN WAN
Customer Edge (B/P/C/S)
Network Core
Network Edge
AS LAN/CAN/MAN
DISN UC Services
Trusted Relationships Required Among All Architectural Functions
NM
• Control to SS, SC, SBC, ASAC & CE Routers
NM
NM
NM
NM
Media Gateway
SC or ESC ASAC
• State of Local LAN Sessions
• State of Local 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 SC SCS to Modify Resources
SC ASAC
SS
• SCS
• NM
• Location (Routing) Service
• MGC
• Appliance Authentication & IA Services
• SC [Optional]
CE Router
• Traffic Conditioning
• Bandwidth Management
• PHB
Distributed SC
• SCS
• NM
• Location (Routing) and Directory Services
• MGC
• Appliance Authentication & IA Services
• EI & User Authentication & Authorization
• User Features & Services
SS ASAC
SS (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)
• Process Input from Closed Loop System
• Directs SS SCS to modify resources
SBC
• Topology Hiding
• Opening and Closing "Pinholes"
Assured and Non-Assured LAN
Media Gateway
End Instrument
• Signaling Client
• COS Packet Marking
• Precedence Assignment
• SC Authentication
• User Interface
CE-R
Access Circuit
U-AR
LEGEND
AS Assured Services
ASAC Assured Service Admission Control
ASLAN Assured Service Local Area Network
B/P/C/S Base/Post/Camp/Station
C2 Command and Control
CE-R Customer Edge Router
COS Class of Service
DISN Defense Information Systems Network
EI End Instrument
IA Information Assurance
MGC Media Gateway Controller
NM Network Management
PBNM Policy Based NM
PHB Per-Hop Behavior
SBC Session Border Controller
SC Session Controller
SCS Session Control and Signaling
SLA Service Level Agreement
SS Softswitch
U-AR Unsecure Aggregated Router

Figure 2.1-4. Assured Services Subsystem Functional Diagram

The functions contained in the Figure 2.1-4 boxes and the SBC 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 2.1-4 and subordinate functions listed within each box are specified in this section. In addition, 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 are specified to the maximum extent possible, and any deviations or enhancements to these are specified in detail within UCR 2013.

The ASAC technique is the key design component ensuring that E2E Service-Level Agreements (SLAs) (grade of service [GOS], voice/video quality, assured service delivery, and session preemption to the EI) are met in the converged DISN. The ASAC technique involves functional aspects of, and interactions among, virtually all network elements (NEs) end-to-end as illustrated in Figure 2.1-4, Assured Services Subsystem Functional Diagram. The ASAC functions identified for the SC are also employed in the Enterprise SC. Deployable VoIP products may connect via compressed satellite circuits to the DISN backbone and operate in a similar manner to Fixed products on the LAN.

In the access circuit and the ASLAN, AS-SIP signaling is used by the SC and SS to establish or preempt voice and video sessions based on precedence and engineered traffic levels on the access circuits (both origination and destination ends). In the bearer plane, the QoS/DSCP manages router Per-Hop Behavior (PHB) based on the type of service class. Both the ASLAN and the backbone are assumed to be traffic engineered to be nonblocking for voice and video traffic. In the DISN Core, the DISN SLAs will support voice and video with assured services provided by QoS/DSCP, traffic engineering, and MPLS. Traffic with no marking will be treated as Best Effort.

The SC manages a budget for sessions determined by the voice and video traffic-engineered bandwidth of the associated access infrastructure. The Resource-Priority header portion of the AS-SIP signaling message conveys the precedence of the desired session establishment to the destination end SC. Both the originating and destination SCs independently manage their session budgets, so that sessions are permitted or established by precedence until the budget limit is reached. Then a new session can be allowed only if a lower precedence session is available to preempt. At the originating end after preemption has taken place, if necessary, the origination request is sent to the destination upon which, after preemption has taken place, if necessary, the request acceptance is returned to the originating SC. If the originating SC is at its budget limit and has no lower precedence session to preempt, then a blocked session indication, in the form of a Blocked Precedence Announcement (BPA), will be sent to the originating EI. If the terminating SC is at its budget limit and has no lower precedence session to preempt, then a Session Request Denied message will be returned to the originating SC, which, in turn, will send a BPA to the EI. For ROUTINE precedence calls reaching the maximum budget limit, “fast busy” (120 impulses per minute [ipm]) will be sent to the originating EI. All AS-SIP users will come under ASAC. Some H.323 video users on a base may choose to use a separate H.323 Gatekeeper and not come under ASAC. Data traffic (non-voice and video) does not have any ASAC and is handled as Best Effort or preferred data, if the data application implements DSCP packet marking.

Session control processing to establish, maintain, and terminate sessions is performed by the Call Connection Agent (CCA) part of the SC and SS. Signaling is performed by the Signaling Gateway (SG) (used for Circuit Switched T1.619a/AS-SIP signaling conversion), the Media Gateway (MG) (for EI IP signaling to Commercial Primary Rate Interface [PRI] signaling), and as part of the AS-SIP signaling appliance part of the SC and SS depending on requirements for a particular session. Local subscriber directories are stored in the SCs and network-level worldwide routing tables and addressing and numbering plans are stored in the SS.

2.1.3 Voice and Video Signaling Design

The voice/video signaling design for SBU voice and video is shown in Figure 2.1-5, SBU Voice/Video Services Signaling Design. Currently, the classified voice and video services employ H.323, and will migrate to AS-SIP signaling in the future. Duration migration, both H.323 and AS-SIP signaling will be employed in classified VVoIP. Classified VVoIP interfaces to the TDM Defense RED Switch Network (DRSN) via a proprietary PRI. For SBU voice and video, on the edge of the DISN IP WAN cloud, an SC on the B/P/C/S signals via AS-SIP to the network-level softswitch part of SS. The Defense Switched Network (DSN) Common Channel Signaling 7 (CCS7) network is being phased out and replaced by PRI trunks. The TDM End Offices (EOs) use PRI for signaling to the TDM switching part of the SS. The SSs use AS-SIP between themselves to set up IP-to-IP EI sessions across the DISN IP WAN.

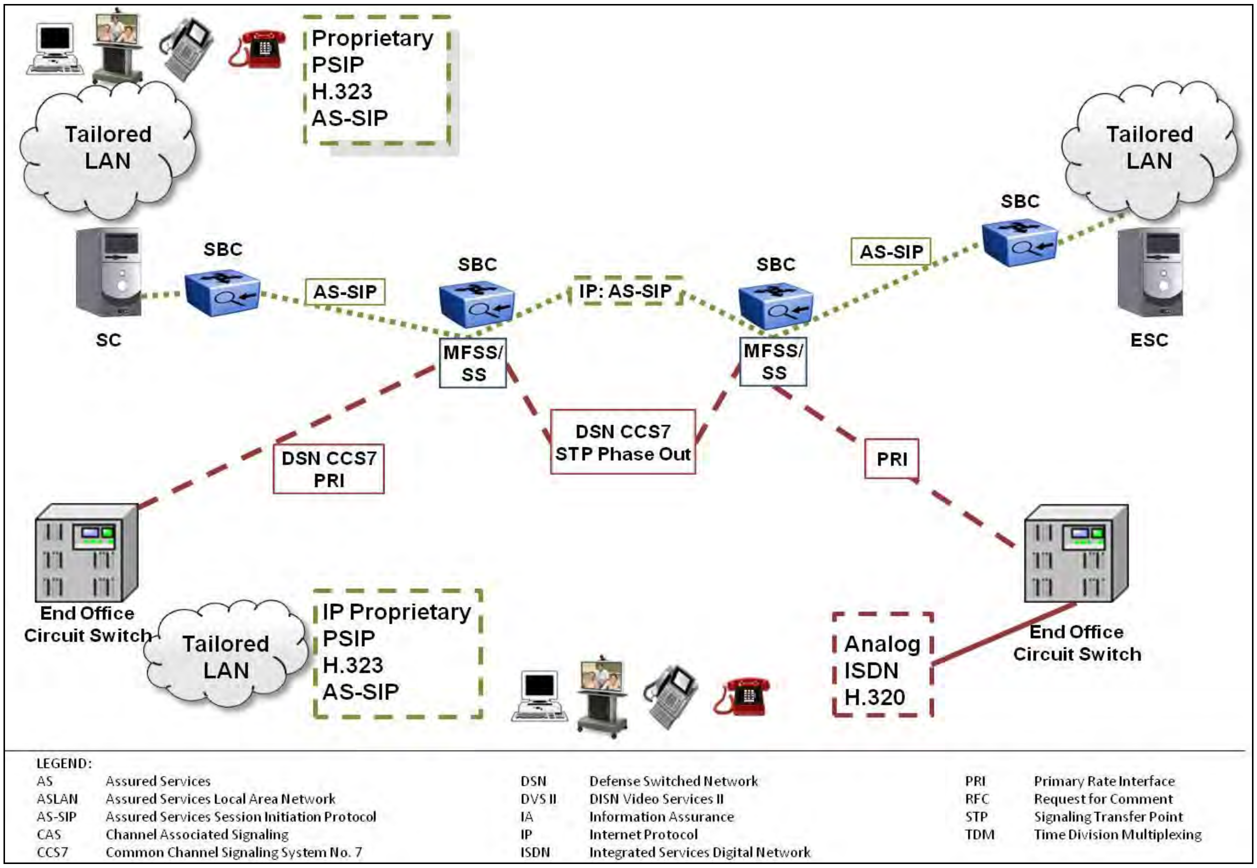

Proprietary
PSIP
H.323
AS-SIP
Tailored LAN
Tailored LAN
SBC
SBC
SBC
SBC
AS-SIP
AS-SIP
IP: AS-SIP
SC
ESC
MFSS/ SS
MFSS/ SS
DSN CCS7 PRI
DSN CCS7 STP Phase Out
PRI
End Office Circuit Switch
End Office Circuit Switch
Tailored LAN
IP Proprietary
PSIP
H.323
AS-SIP
Analog
ISDN
H.320
LEGEND:
AS Assured Services
ASLAN Assured Services Local Area Network
AS-SIP Assured Services Session Initiation Protocol
CAS Channel Associated Signaling
CCS7 Common Channel Signaling System No. 7
DSN Defense Switched Network
DVS II DISN Video Services II
IA Information Assurance
IP Internet Protocol
ISDN Integrated Services Digital Network
PRI Primary Rate Interface
RFC Request for Comment
STP Signaling Transfer Point
TDM Time Division Multiplexing

Figure 2.1-5. SBU Voice and Video Services Signaling Design

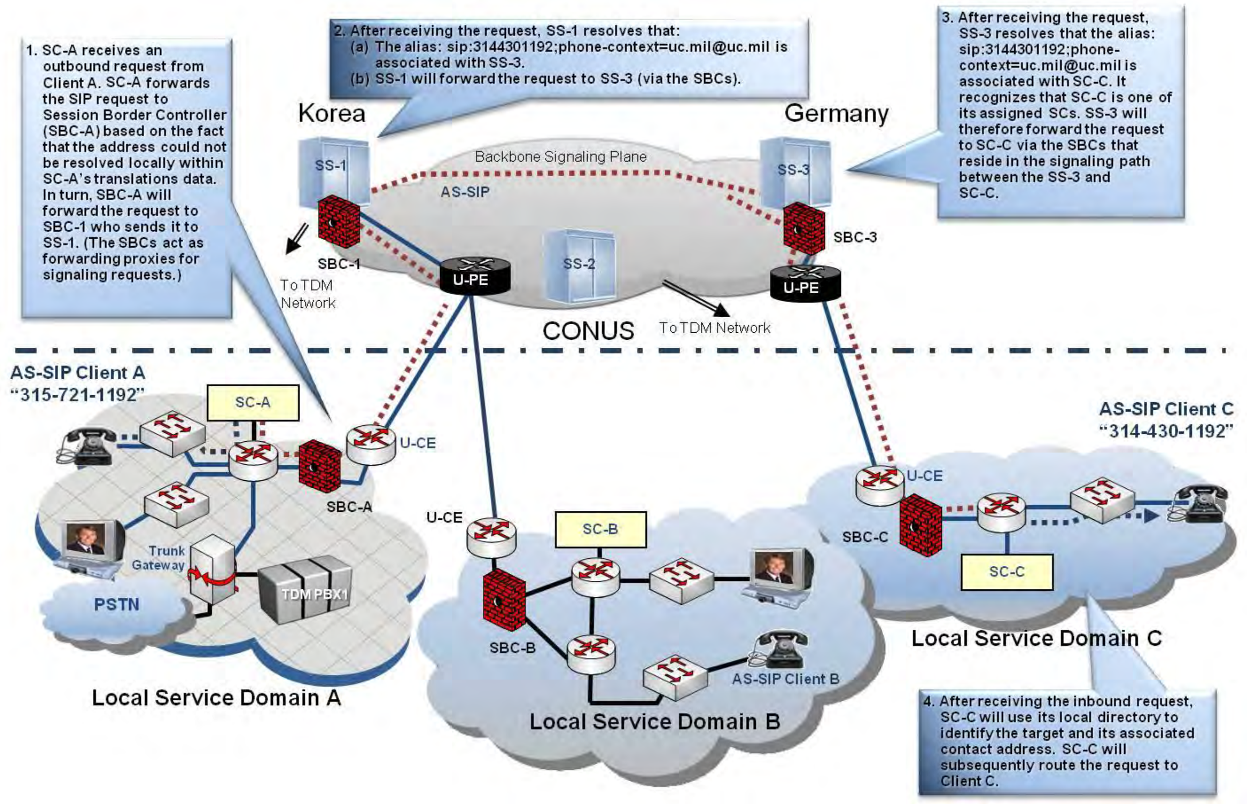
The SSs use PRI to set up TDM-to-TDM EI sessions across the TDM trunking part of the DISN WAN. Both types of signaling (IP or TDM) are required to support a hybrid TDM and IP EI environment as the DISN voice/video system migrates to an all IP EI environment in the post-2016 timeframe.

The key rules and attributes of the signaling design are as follows:

- Two-level signaling hierarchy—SC and SS:
  - SC A to SS A to SS B to SC B when the SCs have different primary SSs.
  - SC A to SS A to SC B when they have the same primary SS.
- The SCs are assigned a primary and backup SS for signaling robustness.
- Signaling from an IP EI to an SC may be proprietary, or AS-SIP.
- The SC-to-SC signaling is not permitted external to the security enclave except for use in cases involving Deployable products operating in a single area of operational responsibility network that is not the DISN.
- The SC can set up:
  - On-base sessions when a connection to an SS is lost.
  - Sessions to Public Switched Telephone Network (PSTN) trunks independent of an SS.
- Signaling:
  - A TDM EO will signal via DSN CCS7 or PRI to SSs.
  - The SSs will signal via PRI to the PSTN and to coalition gateways.

Signaling from the SC must pass through the network SS part of the SS or through a network-level SS so the SS can implement Precedence-Based Assured Services controls and police the proper use of access circuit bandwidth. For bases that have a collocated SS, base-level access to the local PSTN can be provided through the SC portion of the SS. At the network level, the SS will serve as the gateway to external networks, such as Services' Deployable Programs networks, the DRSN, and coalition networks, using appropriate signaling protocols, such as PRI signaling.

The end-to-end, two-level SBU AS-SIP network signaling design is shown in Figure 2.1-6, End-to-End Two-Level SBU AS-SIP Network Signaling Design. This diagram illustrates operations with Local SCs (LSCs). Operations will be similar for Enterprise SCs (ESCs). For classified networks, the two-level signaling uses SSs.



1. SC-A receives an outbound request from Client A. SC-A forwards the SIP request to Session Border Controller (SBC-A) based on the fact that the address could not be resolved locally within SC-A's translations data. In turn, SBC-A will forward the request to SBC-1 who sends it to SS-1. (The SBCs act as forwarding proxies for signaling requests.)

2. After receiving the request, SS-1 resolves that:
   (a) The alias: sip:3144301192;phone-context=uc.mil@uc.mil is associated with SS-3.
   (b) SS-1 will forward the request to SS-3 (via the SBCs).

3. After receiving the request, SS-3 resolves that the alias: sip:3144301192;phone-context=uc.mil@uc.mil is associated with SC-C. It recognizes that SC-C is one of its assigned SCs. SS-3 will therefore forward the request to SC-C via the SBCs that reside in the signaling path between the SS-3 and SC-C.

4. After receiving the inbound request, SC-C will use its local directory to identify the target and its associated contact address. SC-C will subsequently route the request to Client C.

Figure 2.1-6. End-to-End Two-Level SBU AS-SIP Network Signaling Design

2.1.4 Distributed UC Services Model

The SC product can be deployed locally—physically located within the edge segment it serves—or as an enterprise services provider, with centrally located components interacting with components located at edge segments. Figure 2.1-7, Distributed UC Services Model, shows an arrangement of Local SCs and SSs in the DISN assured services voice and video network. See Section 2.2, Enterprise UC Services Design, for a description of the Enterprise UC Services model.

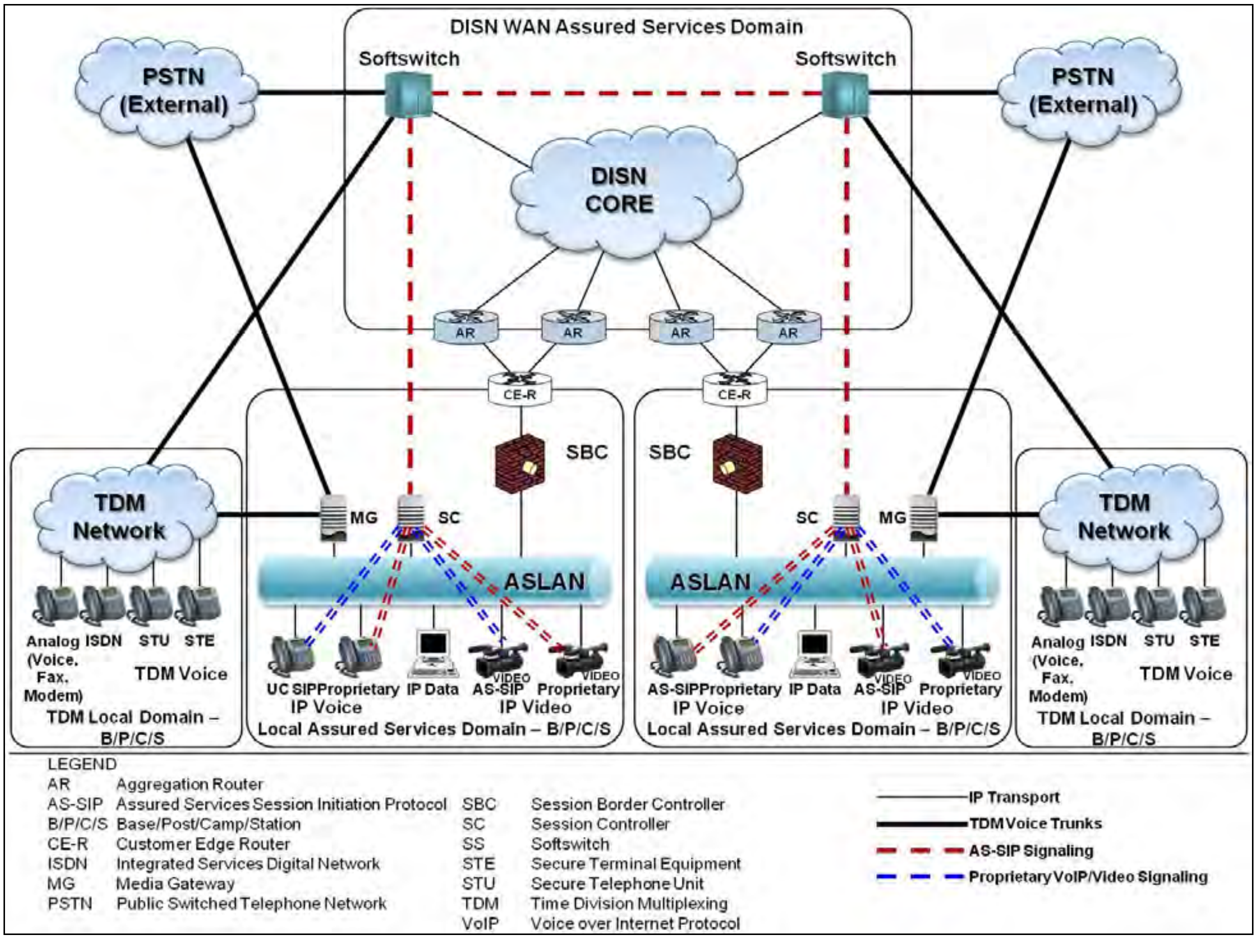

DISN WAN Assured Services Domain
Softswitch
Softswitch
PSTN (External)
PSTN (External)
DISN CORE
AR
AR
AR
AR
CE-R
CE-R
SBC
SBC
TDM Network
TDM Network
MG
SC
SC
MG
ASLAN
ASLAN
Analog (Voice, Fax, Modem)
ISDN
STU
STE
TDM Voice
TDM Local Domain – B/P/C/S
UC SIP
Proprietary
IP Voice
IP Data
AS-SIP
Proprietary
IP Video
VIDEO
VIDEO
Local Assured Services Domain – B/P/C/S
AS-SIP
Proprietary
IP Voice
IP Data
AS-SIP
Proprietary
IP Video
VIDEO
VIDEO
Local Assured Services Domain – B/P/C/S
Analog (Voice, Fax, Modem)
ISDN
STU
STE
TDM Voice
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
CE-R Customer Edge Router
ISDN Integrated Services Digital Network
MG Media Gateway
PSTN Public Switched Telephone Network
SBC Session Border Controller
SC Session Controller
SS Softswitch
STE Secure Terminal Equipment
STU Secure Telephone Unit
TDM Time Division Multiplexing
VoIP Voice over Internet Protocol
IP Transport
TDM Voice Trunks
AS-SIP Signaling
Proprietary VoIP/Video Signaling

Figure 2.1-7. Distributed UC Services Model

The network is a hierarchical network supporting the following:

- Local services and features within an Edge Segment [base/post/camp/station (B/P/C/S)].
- Global services and features across the UC network.
- Services and features to Department of Defense (DoD) allied networks, DoD coalition networks, and the external Public Switched Telephone Network (PSTN).

2.1.5 Session Control Failover Feature

The session control failover feature involves deploying the SSs as active primary/secondary pairs, whereby one SS acts as the Primary SS for one set of SCs (set A) and acts as the Secondary SS for the SCs of its active paired SS (set B SCs). Similarly, its paired SS acts as the Primary SS for the set B SCs and acts as the Secondary SS for the set A SCs. The SCs shall be assigned to a primary and a secondary (i.e., backup) SS during network configuration.

Each SC is configured with the identity of its Primary SS and its Secondary SS. This is input by operations personnel during SC configuration.

Each SS in the network is configured with the identity of its secondary paired SS. This is input by operations personnel during SS configuration.

Each SS in the network is configured with the identity of every active primary/Secondary SS pair. This is input by operations personnel during SS configuration and is modified as new SSs are added to the network.

The SC and SS failover feature make use of SUBSCRIBE and NOTIFY requests associated with the failover event package defined in UCR 2013, Section 2.6, SC and SS Failover.

Each SC creates a subscription with its Primary SS and with its Secondary SS; the Primary SS and the Secondary SS each create subscriptions with every SC served by the Primary SS and served by the Secondary SS. The subscriptions are arranged based upon a failover event scenario. In addition, the Primary SS and the Secondary SS also create subscriptions with each other based on a failover event scenario. These subscriptions enable the SC and the SSs to send and receive the notification messages that trigger failover and failback.

Each SC sends periodic OPTIONS requests to its Primary SS to detect loss of SIP layer access to the Primary SS.

Each SS sends periodic OPTIONS requests to every one of the SCs for which the SS is operating as the Primary SS to detect loss of SIP layer access to an SC. Specifically, these OPTIONS requests are to enable the Primary SS to detect loss of the Transport Layer Security (TLS) path from the Primary SS SBC to the SC SBC. The TLS path from the SC SBC to the Primary SS MAY be operational in which case the SC cannot detect this outage by the periodic OPTIONS requests the SC sends to the Primary SS.

Each SS in the network sends periodic OPTIONS requests to every other SS in the network (with the exception of its paired SS) to detect loss of SIP layer accessibility to any other SS.

Whenever the SC sends a defined configurable number (default equals 2) of successive OPTIONS requests to its Primary SS that result in failure responses, then the SC concludes the Primary SS is inaccessible (this may be due to a transport failure or a failure of the Primary SS). The SC sends a ‘failover’ NOTIFY message to the Secondary SS informing the Secondary SS that the SC is failing over to the Secondary SS. Then the SC begins sending outbound AS-SIP messages intended for destinations outside the enclave to the Secondary SS.

Upon receipt of a ‘failover’ NOTIFY message, the Secondary SS sends OPTIONS request(s) to the Primary SS to determine whether the Primary SS is accessible at the SIP layer to the Secondary SS.

If the OPTIONS request is successful, then the Secondary SS sends a ‘failover’ NOTIFY message to the Primary SS. The Primary SS now sends all its inbound AS-SIP messages intended for the SC to the Secondary SS instead. The Secondary SS sends all new inbound INVITEs intended for the SC and all subsequent AS-SIP messages associated with the new inbound INVITEs to the SC.

2.2 ENTERPRISE UC SERVICES DESIGN

In accordance with the UC Master Plan, the Enterprise UC Services Architecture is a strategy for providing Enterprise UC Services from a centralized location to DoD Component enclaves within a select geographic region. To achieve the full potential of Enterprise UC Services, the architecture integrates UC voice, video, and IM/Chat/Presence capabilities with other DoD Enterprises Services such as Enterprise E-mail, Enterprise collaboration (e.g., Defense Connect Online), Enterprise Directory Services, and Enterprise Voice Internet Service Provider (ISP) services via a Defense Information Systems Agency (DISA) Internet Access Point (IAP).

2.2.1 Enterprise UC Vision

As depicted in Figure 2.2-1, the Enterprise UC Services Architecture consists of both Centralized Enterprise Infrastructure components and Edge Infrastructure components:

- The Centralized Enterprise Infrastructure is composed of the following:
  - ESC.
  - ESC-fronting SBC.
  - Enterprise Hosted UC Services.
  - Enterprise Required Ancillary Equipment (RAE).
- The Edge Infrastructure (at DoD Components' B/P/C/S locations) consist of the following:
  - End Instruments.
  - Media Gateways.
  - Enclave-fronting SBCs.
  - Survivable Call Processing capabilities (for Environments 1 and 2).
  - Local RAE.

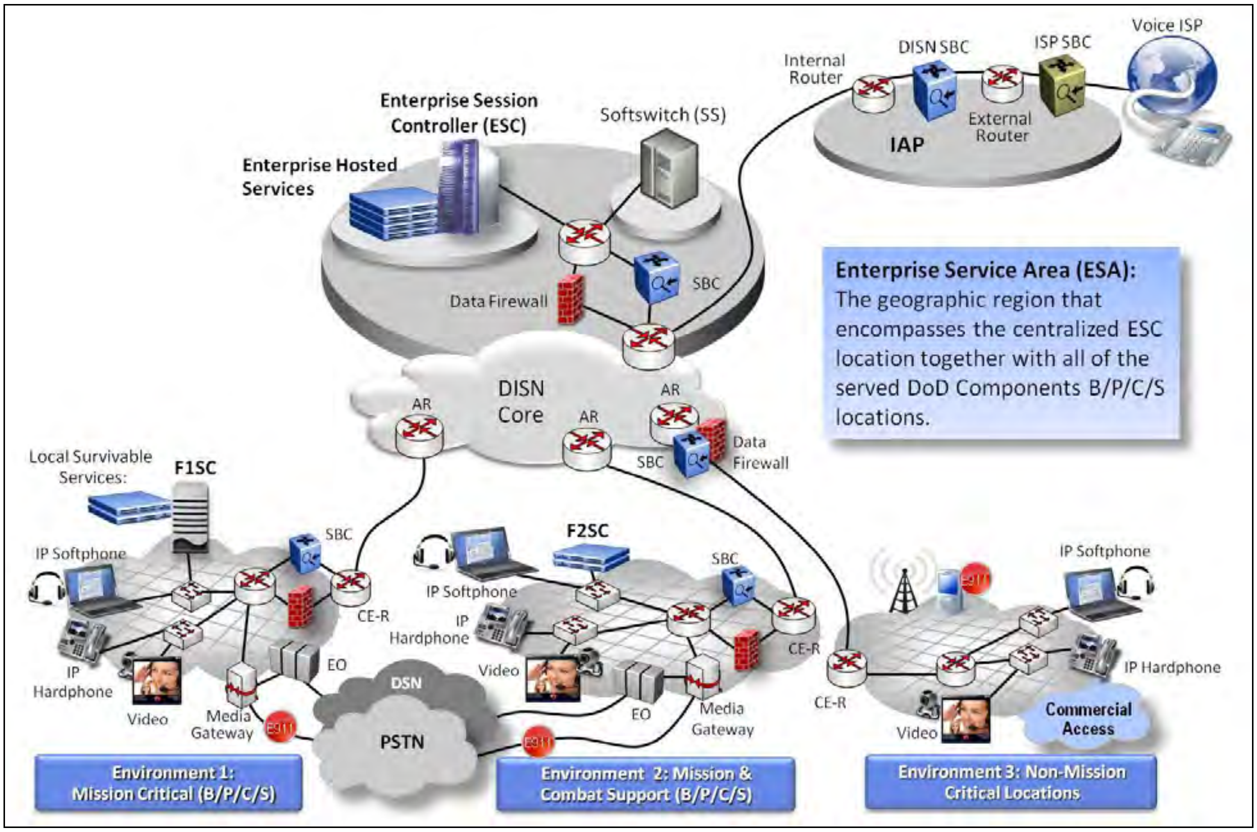

Voice ISP
ISP SBC
DISN SBC
Internal Router
External Router
IAP
Enterprise Session Controller (ESC)
Softswitch (SS)
Enterprise Hosted Services
SBC
Data Firewall
Enterprise Service Area (ESA): The geographic region that encompasses the centralized ESC location together with all of the served DoD Components B/P/C/S locations.
DISN Core
AR
AR
AR
SBC
Data Firewall
Local Survivable Services:
F1SC
IP Softphone
SBC
CE-R
IP Hardphone
Video
Media Gateway
EO
F2SC
IP Softphone
IP Hardphone
SBC
Video
EO
Media Gateway
CE-R
DSN
PSTN
E911
E911
E911
IP Softphone
IP Hardphone
CE-R
Video
Commercial Access
Environment 1: Mission Critical (B/P/C/S)
Environment 2: Mission & Combat Support (B/P/C/S)
Environment 3: Non-Mission Critical Locations

Figure 2.2-1. Enterprise UC Services Architecture

2.2.2 Enterprise System Design

The ESC provides centralized, integrated voice, video and data session management on behalf of served IP end instruments (EIs) that are located at different enclaves (i.e., B/P/C/S locations) within the served geographic region. A full suite of Enterprise Hosted UC Services are collocated with the ESC. The Hosted UC Services include the following:

- Centralized voice and video session management.
- Centralized voice and video conferencing.
- Unified messaging.
- Integrated E911 Call Management.
- Extensible Messaging and Presence Protocol (XMPP) IM/Chat/Presence federation.
- Service portability.
- Integrated Enterprise Directory Services.

The geographic region that encompasses the centralized ESC location together with all of the served DoD Components B/P/C/S locations is referred to as the Enterprise Services Area (ESA). The ESC provides an integrated management framework that enables the centralized configuration, provisioning, administration, management, and monitoring of all Centralized

Enterprise Services Infrastructure components and all Edge Infrastructure components within the ESA. Reliable and redundant systems at all levels of the Enterprise UC Services architecture ensure the high availability needed to meet the requirements of the warfighter and operational user.

2.2.3 The Enterprise Continuity of Operations (COOP) Capabilities

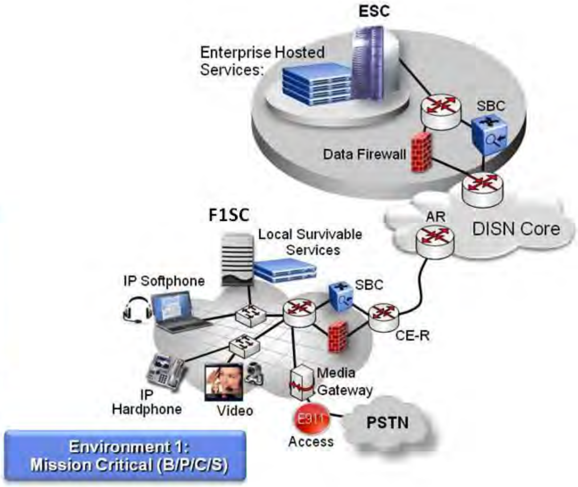
The Enterprise UC Services Architecture includes a Continuity of Operations (COOP) strategy which provides for the survivability of essential UC services during a period of network disruption and/or a loss of access to the serving ESC. The survivable UC services (i.e., COOP) requirement of a given location is based upon the mission being performed at that location. The COOP requirements in turn dictate the technical solution components that must be deployed at each B/P/C/S location within the ESA. The UC Master Plan defines three mission environment types as defined in the following subsections.

2.2.3.1 Environment Type 1

Environment 1 is intended to support site user communities with only a limited degradation in UC service when the site is isolated from the ESC (see Figure 2.2-2). A Failover Type 1 Session Controller (F1SC), local service capabilities, enclave-fronting SBC and local media gateway resources are installed on the base. When access to the ESC is interrupted, an Environment 1 location shall have access to the following locally-provided UC services:

- Intra-base precedence calling capability.
- Audio conferencing (sized per customer requirements).
- Video point-to-point.
- Local IM/Chat/Presence capabilities.
- E911 services.
- PSTN/DSN access via local media gateway (sized per customer requirements).

Mission Environment Type 1
"Mission Critical Environment"
(Examples: Operational Flying Wing or Combat Support Unit)



UC Requirements (During Normal Operating Conditions)

- **Access to all UC Services via ESC and Enterprise Hosted Services :**
  - Precedence calling capability
  - IM/Chat/Presence
  - Voice and video conferencing
  - Video point-to-point
  - Unified Messaging
  - Workspace Collaboration
  - PSTN/DSN/E911 access (sized per customer requirements)

COOP Requirements in Survivable Mode
(When Access to DISN/ESC Is Interrupted)

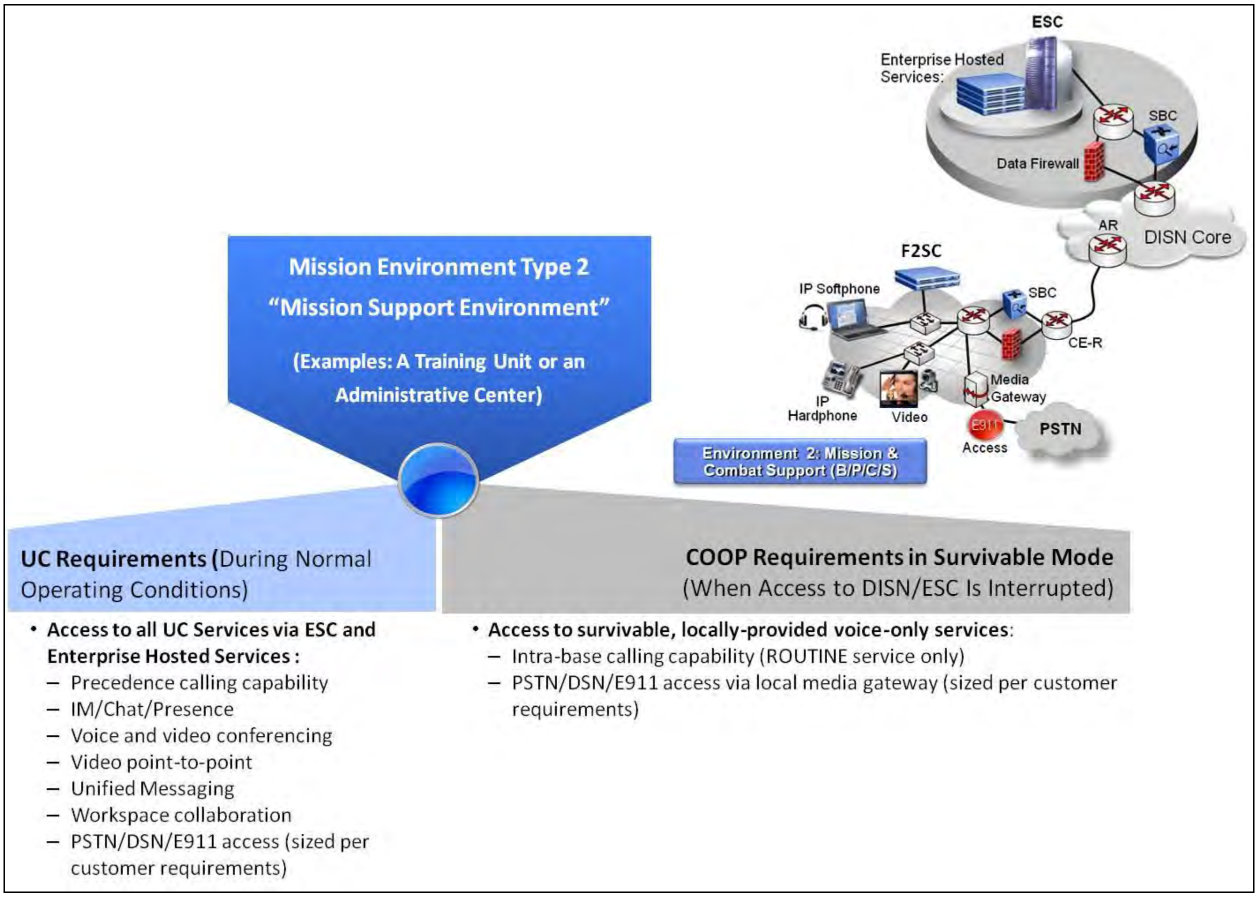
- **Access to a full complement of basic, locally-provided UC services** :
  - Intra-base precedence calling capability
  - Audio conferencing (sized per customer requirements)
  - Video point-to-point
  - Local IM/Chat/Presence
  - E911 services
  - PSTN/DSN access via local media gateway (sized per customer requirements)

Figure 2.2-2. Environment Type 1

2.2.3.2 Environment Type 2

Environment 2 is intended to support user communities with routine voice only capability when the site is isolated from the ESC (see Figure 2.2-3). A Failover Type 2 Session Controller (F2SC), enclave-fronting SBC and local media gateway resources are installed on the base. When access to the ESC is interrupted, an Environment 2 location has access to the following voice services:

- Intra-base calling capability (ROUTINE service only).
- PSTN/DSN/E911 access via local media gateway (sized per customer requirements).



Mission Environment Type 2
"Mission Support Environment"

(Examples: A Training Unit or an Administrative Center)

UC Requirements (During Normal Operating Conditions)

- **Access to all UC Services via ESC and Enterprise Hosted Services :**
  - Precedence calling capability
  - IM/Chat/Presence
  - Voice and video conferencing
  - Video point-to-point
  - Unified Messaging
  - Workspace collaboration
  - PSTN/DSN/E911 access (sized per customer requirements)

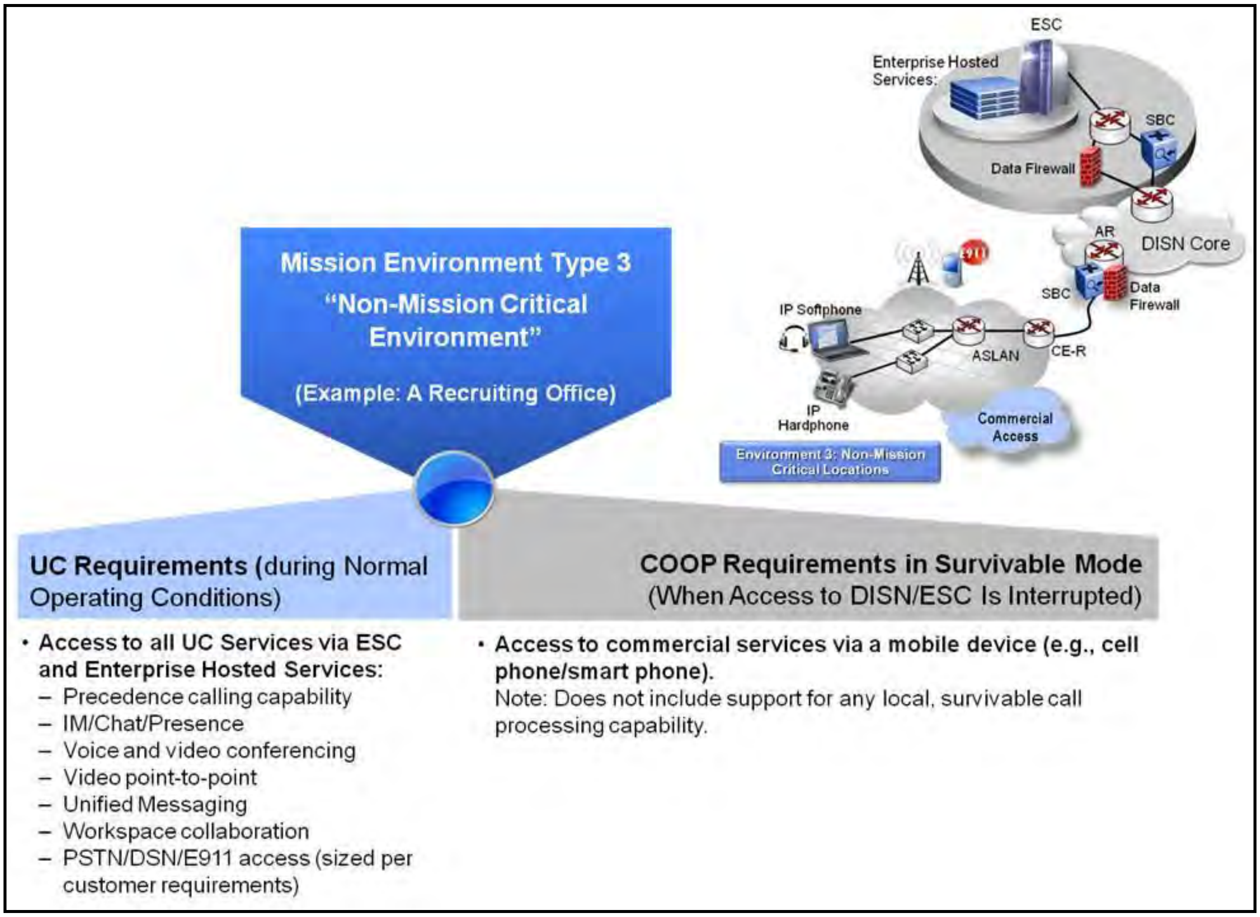
COOP Requirements in Survivable Mode
(When Access to DISN/ESC Is Interrupted)

- **Access to survivable, locally-provided voice-only services**:
  - Intra-base calling capability (ROUTINE service only)
  - PSTN/DSN/E911 access via local media gateway (sized per customer requirements)

Figure 2.2-3. Environment Type 2

2.2.3.3 Environment Type 3

Environment 3 is intended to support user communities that do not require access to locally provided voice services when the site is isolated from the ESC (see Figure 2.2-4). When access to the ESC is interrupted, an Environment 3 location shall rely upon commercial services via a mobile device (e.g., a cell phone/smart phone).



Mission Environment Type 3
"Non-Mission Critical Environment"
(Example: A Recruiting Office)

UC Requirements (during Normal Operating Conditions)

- **Access to all UC Services via ESC and Enterprise Hosted Services:**
  - Precedence calling capability
  - IM/Chat/Presence
  - Voice and video conferencing
  - Video point-to-point
  - Unified Messaging
  - Workspace collaboration
  - PSTN/DSN/E911 access (sized per customer requirements)

COOP Requirements in Survivable Mode
(When Access to DISN/ESC Is Interrupted)

- **Access to commercial services via a mobile device (e.g., cell phone/smart phone).**
  Note: Does not include support for any local, survivable call processing capability.

Figure 2.2-4. Environment Type 3

2.2.4 Messaging (IM/Chat/Presence) Integration

The principal focus of the UC Messaging (IM/Chat/Presence) Integration is to drive the certification and deployment of approved products that enable the near real-time exchange of text-based messages using the Extensible Messaging and Presence Protocol (XMPP). XMPP is an open, standards-based protocol specifically designed to enable the "near real-time" exchange of text-based communications in support of applications such as Instant Messaging (IM), Group Chat, and the exchange of presence information (a status indicator that conveys ability and willingness of another party to communicate). The XMPP protocol is a proven, mature technology that is highly scalable and secure with integrated support for channel encryption and strong authentication.

Another important aspect of the UC Messaging (IM/Chat/Presence) Integration is the support for XMPP-based server-to-server federation (i.e., server-to-server interoperability). As depicted in Figure 2.2.5, Multivendor Interoperability Normalized on XMPP, XMPP server-to-server federation permits users who are hosted on one vendor's messaging platform to seamlessly chat and exchange presence information with users who are hosted on another vendor's platform.

Without server-to-server federation, a user can only exchange messages and see the presence information of other users who are all hosted on the same system.

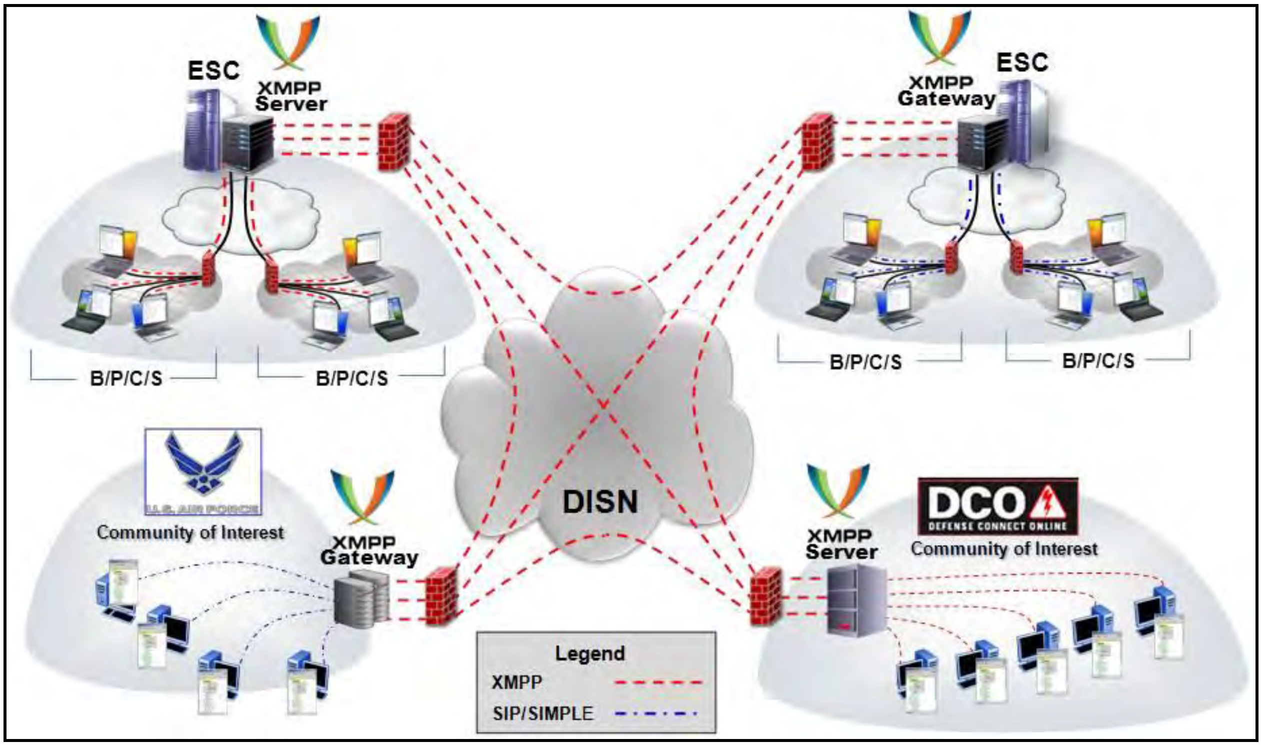


Figure 2.2-5. Multivendor Interoperability Normalized on XMPP

The concept of federating simply refers to a server-to-server link that permits the exchange of Presence information and IM between the two systems.

2.2.5 Enterprise Directory Services (EDS)

This section provides an overview of the initial system concepts for integration of UC services. The voice, video, and data services include multimedia or cross-media collaboration capabilities (including audio collaboration, video collaboration, text-based collaboration, and presence). The focus of the integration is to go beyond local, intra-enclave test events to implement and assess collaboration services and applications on an end-to-end, WAN-level basis. These UC network-wide collaboration services raise the need for new designs to address any potential performance, information assurance, or engineering/configuration issues associated with these different applications traversing the same ASLAN and Network Edge Segments.

This section describes the framework for Enterprise Directory Services (EDS), provided by ESCs and UC Video Conference Bridges for Enterprise UC end users.

The goal of EDS is to provide Enterprise UC end users with access to an Electronic Directory that contains Directory Data (user records) for various DoD end users [users in various DoD Components such as Combatant Commands (COCOMs), Services, and Agencies]. The Directory typically contains one record for each end user, though in some cases the Directory may have more than one record for an individual user. (This can occur in cases in which the user has more than one CAC card and each CAC card represents an individual role that the user performs within his or her DoD Component.) Each Directory record contains a set of attributes that contain information about that particular end user. Examples of attributes that can be found in an individual user's data record are as follows:

- First Name.
- Middle Initials.
- Last Name.
- Organization Name (e.g., Army [AR], Air Force [AF], Navy [NV], Marine Corps [MC], Department of Defense [DoD], Civilian [CIV]).
- Company Name (e.g., COCOM name, Major Command [MAJCOM] name).
- Department Name (e.g., Unit name).
- Display Name.
- E-mail address.
- Business phone number.
- Mobile phone number.
- Fax number.
- Office.
- Job Title.
- Rank.
- DoD SIP URI (e.g., sip:FirstName.MiddleInitials.LastName.civ@uc.mil).

The number of DoD end users whose data is included in the EDS, and therefore the number of data records included in the EDS, is determined by DISA, which is both the EDS provider and the Enterprise UC provider.

An example of an EDS is the Global Address List (GAL) or Global Address Book (GAB) that is currently provided by the Microsoft Outlook (email client), Microsoft Exchange (email server), and Microsoft Active Directory (directory service) products. In an enterprise running these products, end users can look up information on other end users by sending a query to the directory service, and receive a response back from the service containing the records and attributes that match the criteria in the query. The directory queries and responses are performed using the MS Outlook client on the user's PC, the MS Exchange email server in the enterprise data network, and the MS Active Directory server in the enterprise data network.

DISA's current plan is to provide an EDS to Enterprise UC end users using the following:

- EDS client software on an end user's voice or video EI (i.e., a Voice or Video Hard-Phone that also contains an Enterprise Directory query-response capability);
- EDS client software on the end user's PC (i.e., a software application that contains an Enterprise Directory query-response capability); this application can be either integrated with or separate from the Voice Soft-Phone application or Video Soft-Phone application on that end user's PC.

- EDS gateway server software on the ESC serving the end user.
- EDS DoD Enterprise Email Global Address List (DEE GAL) servers in the Enterprise UC network.

The purpose of the EDS gateway server on the ESC is to provide a mediation point between 1) the various EDS clients on end users' EI and PCs served by the ESC and 2) the EDS DEE GAL servers themselves. The ESC concentrates EDS query traffic from the various EIs and PCs and presents a single EDS query/response interface to each EDS DEE GAL server.

The DEE GAL servers in the Enterprise UC network are also linked to IDSS DEE GAL servers in the DISN so that the directory data in the UC DEE GAL servers remains synchronized with the directory data in the IDSS DEE GAL servers. The data in the IDSS DEE GAL servers is considered an authoritative or "Master" version of the EDS data, and the data in the UC DEE GAL servers is a replica or copy of the Master version.

In addition, the EDS DEE GAL servers in the Enterprise UC Network are not UC APL Products. The EDS Framework in this section applies to EDS clients on Voice and Video EIs, EDS clients on Enterprise UC end users' PCs, and the EDS gateway server software on ESCs, but not to the EDS DEE GAL servers themselves.

Figure 2.2-6 shows the basic architecture used to provide EDS in the Enterprise UC network. Additional DISA and DoD Directory Servers upstream of the EDS DEE GAL servers (such as IDMI, EASF, IDSS, and DMDC) are shown for the sake of completeness. These additional servers are outside of the Enterprise UC network and not part of the framework for EDS.

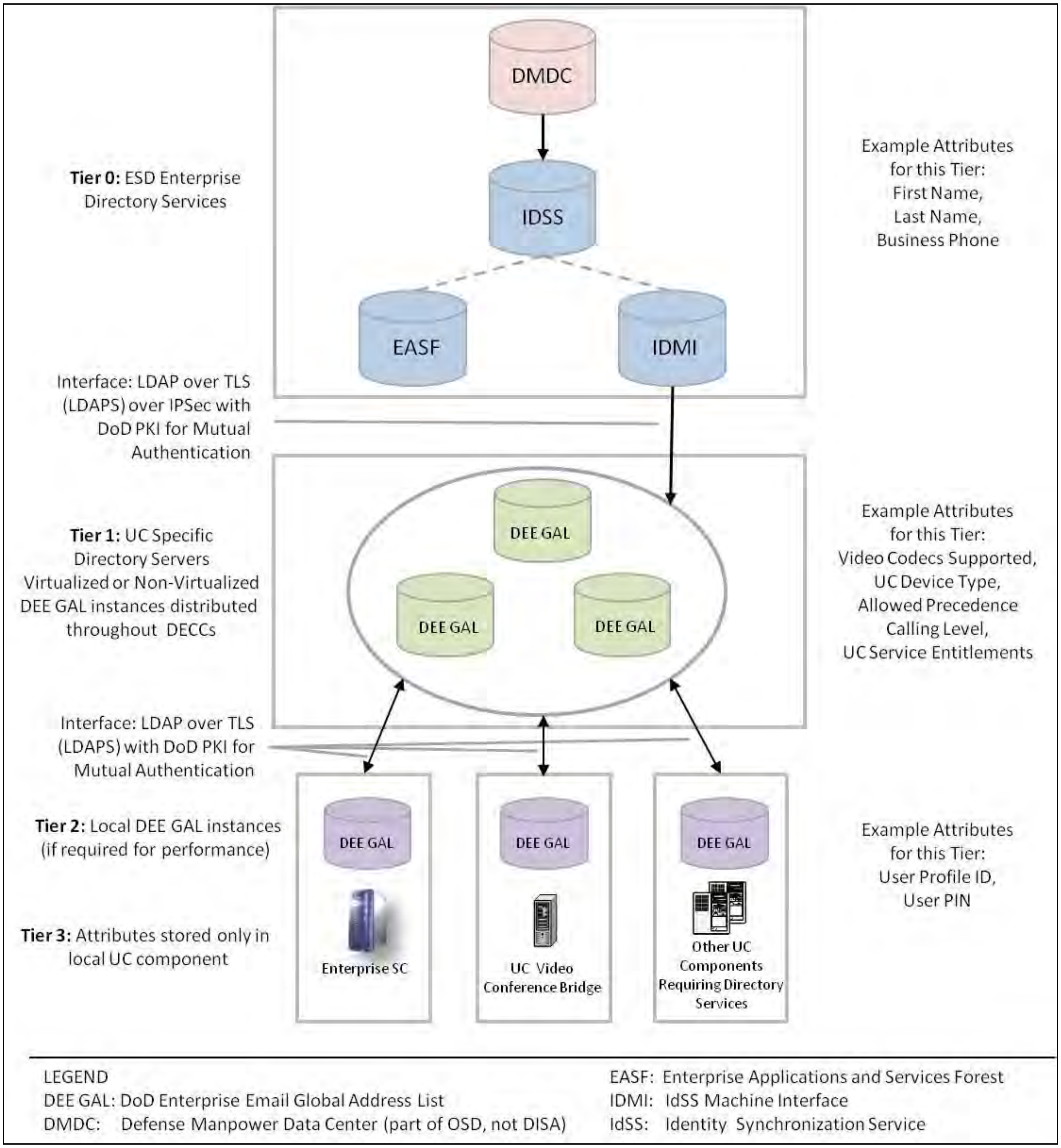

DMDC
IDSS
EASF
IDMI
Tier 0: ESD Enterprise Directory Services
Example Attributes for this Tier: First Name, Last Name, Business Phone
Interface: LDAP over TLS (LDAPS) over IPSec with DoD PKI for Mutual Authentication
DEE GAL
DEE GAL
DEE GAL
Tier 1: UC Specific Directory Servers Virtualized or Non-Virtualized DEE GAL instances distributed throughout DECCs
Example Attributes for this Tier: Video Codecs Supported, UC Device Type, Allowed Precedence Calling Level, UC Service Entitlements
Interface: LDAP over TLS (LDAPS) with DoD PKI for Mutual Authentication
Tier 2: Local DEE GAL instances (if required for performance)
Tier 3: Attributes stored only in local UC component
DEE GAL
Enterprise SC
DEE GAL
UC Video Conference Bridge
DEE GAL
Other UC Components Requiring Directory Services
Example Attributes for this Tier: User Profile ID, User PIN
LEGEND
DEE GAL: DoD Enterprise Email Global Address List
DMDC: Defense Manpower Data Center (part of OSD, not DISA)
EASF: Enterprise Applications and Services Forest
IDMI: IdSS Machine Interface
IdSS: Identity Synchronization Service

Figure 2.2-6. Basic Architecture for Providing EDS in the Enterprise UC Network

This framework uses an architecture that contains the following UC APL Products:

Voice EI with EDS Client, Video EI with EDS Client, ESC with EDS Gateway, and UC Video Conference Bridge with EDS Gateway. The definitions of these four APL Products are as follows:

Voice EI with EDS Client: A Voice EI (Proprietary EI or AS-SIP EI, Hard-phone or PC-based Soft-Phone, per UCR 2013, Sections 2.9.1 and 2.9.6) that contains an EDS Client Application that can be used to make EDS queries via the ESC EDS Gateway. This EDS Client Application also processes EDS query responses from the ESC EDS Gateway and allows the Voice EI user to place a UC VoIP call to another DoD end user by selecting that DoD end user's record from the query responses. The EDS Client Application may also allow the Voice EI user to select the called address (DSN number, commercial wireline number, commercial mobile number, or DoD SIP URI) from the DoD end user's record and use that address to place a VoIP call to the target DoD end user.

Video EI with EDS Client: A Video EI (Proprietary EI or AS-SIP EI, Hard-phone or PC-based Soft-Phone, per per UCR 2013, Sections 2.9.1 and 2.9.6) that contains an EDS Client Application that can be used to make EDS queries via the ESC EDS Gateway. This EDS Client Application also processes EDS query responses from the ESC EDS Gateway and allows the Video EI user to place a UC Video call to another DoD end user by selecting that DoD end user's record from the query responses. The selected DoD end user should also have UC Video capabilities in this case. The EDS Client Application may also allow the Video EI user to select the called address (DSN number or DoD SIP URI) from the DoD end user's record and use that address to place a Video call to the target DoD end user.

ESC with EDS Gateway: An ESC that contains an EDS Gateway that accepts directory queries from EDS Clients on Voice and Video EIs, converts them to LDAP queries, and then sends them on to the UC DEE GAL server that serves that ESC. When this UC DEE GAL server returns LDAP query responses to the ESC, the ESC converts these responses to a protocol (a format) that the EDS Clients can understand and returns these responses to these EDS Clients on the Voice and Video EIs. Note that the ESC and the UC DEE GAL exchange queries and responses using LDAP protocol, but the ESC EDS Gateways and the EDS Clients can exchange queries and responses using another protocol, such as HTTPS / XML / Simple Object Access Protocol (SOAP).

UC Video Conference Bridge with EDS Gateway: A UC Video Conference Bridge that contains an EDS Gateway. The role of the EDS Gateway in the UC Video Conference Bridge is identical to the role of the EDS Gateway in the ESC; that is, the Conference Bridge's EDS Gateway accepts directory queries from EDS Clients on Voice and Video EIs, converts them to LDAP queries, and sends these queries on to the UC DEE GAL server that serves the Conference Bridge. When this UC DEE GAL server returns LDAP query responses to the Bridge, the Bridge converts these responses to a protocol (a format) that the EDS Clients can understand and returns these responses to these EDS Clients on the Voice and Video EIs.

One difference between the ESC's EDS Gateway and the Video Conference Bridge's EDS Gateway is that the Bridge's EDS Gateway only supports EDS Clients on Voice and Video EIs that are located behind the Video Conference Bridge in the Enterprise UC Architecture (EIs ⇔ Voice Conference Bridge ⇔ ESC.)

2.3 MOBILITY AND SERVICE PORTABILITY

Service portability is defined as the end user's ability to obtain subscribed services in a transparent manner regardless of the end user's point of attachment to the network. The key UC objective is to provide service continuity by ensuring mobile warfighters' telephone numbers, e mail addresses, and communication and collaboration tools remain constant as their mission and location change. Figure 2.3-1, Mobile Warfighter's Communication Dilemma, shows the problem service portability is trying to solve.

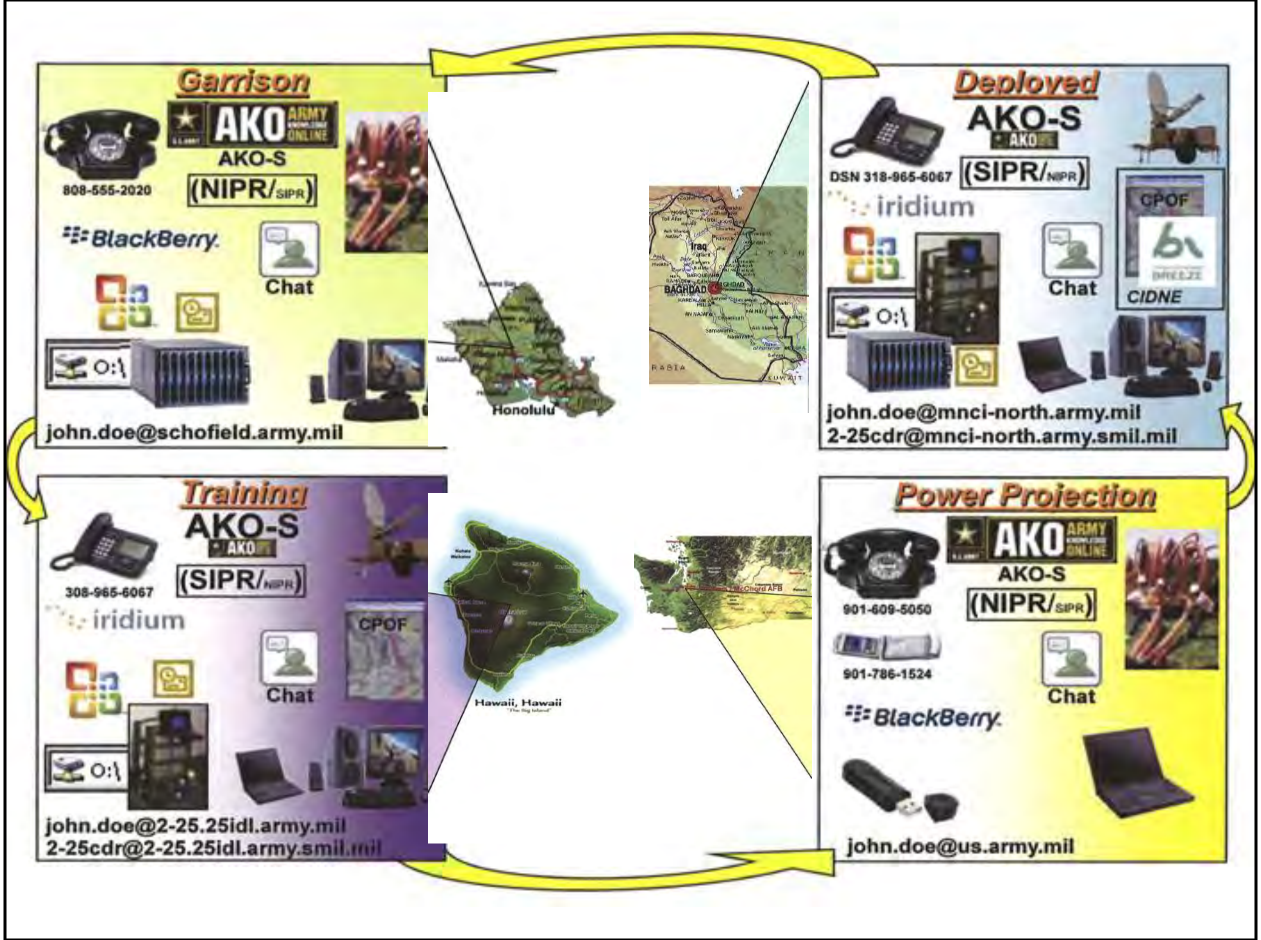


Figure 2.3-1. Mobile Warfighter's Communication Dilemma

To achieve this objective, DISA is working with ESC vendors to provide a UC Mobility feature that would allow Mobile Warfighters to move from one ESC to another and have their assigned phone numbers, IM addresses, and UC services "follow" them as they move. The long-term goal is to provide the same numbers, addresses, and UC services to the Warfighter, independent of the Warfighter's physical location, and independent of the ESC from which he or she is currently being served.

The different ESC vendors provide UC Mobility in their commercial solutions using different methods. The ESC vendors also provide UC services to end users using different EIs (that is, a Hard-Phone, Soft-Phone, or IM/Chat client that works on one vendor's ESC is not currently portable to another vendor's ESC). Because of these differences, DISA needs to work with the ESC vendors to determine the possibility of deploying a multi-vendor-interoperable version of UC Mobility in the worldwide UC network.

In the near term, DISA can use commercial enterprise solutions for User Mobility to serve the Mobile Warfighter. One approach is to use commercial Virtual Private Network (VPN) client software in the user's EI (where the EI is a VVoIP soft client and/or Presence/IM/Chat soft client), and a commercial VPN server in the UC network to provide a secure, encrypted connection ("VPN tunnel") between the user's current physical location and the physical location of the ESC that serves the user. In this approach, the user always obtains service from the same "home" ESC (e.g., the Garrison ESC in the above Figure).

This approach is consistent with the "teleworker" model in commercial enterprises today, where employees who travel or work from home use VPN tunnels over the public Internet to access their office location for corporate email, Web, IM/Chat, and even Voice and Video services. Mobile Warfighters also have the option of using VPN tunnels between their "visited location" and their "home location" in the near term to obtain consistent UC services from their home ESC location until a DISA version of the User Mobility feature is available from the various ESCs in the UC network.

2.4 ASAC OPERATION OVERVIEW

Call Admission Control (CAC) is defined as 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.

CAC is also referred to as Session Admission Control (SAC), because in the network appliances a VoIP call is also a SIP voice session, and a video call is also a SIP video session. SAC is typically limited to managing the pre-populated session budgets for each Assured Service (voice and video).

Assured Services Admission Control (ASAC) 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, and for having calls of a higher precedence level preempt calls of a lower precedence level. Two different levels of ASAC are employed: Session Controller (SC)-Level ASAC and WAN-Level ASAC Policing by the Softswitch (SS).

2.4.1 ASAC Budgets and Counts

2.4.1.1 Voice Budgets and Counts

The SC and its associated SS are configured with an IP Budget (IPB) value, the total budget of VoIP sessions, plus session attempts in the session setup phase, that are allowed on the CE-R to WAN IP access link between the SC and the SS. Optionally, separate budgets for inbound sessions (IPBi) and outbound sessions (IPBo) may also be set.

One voice session budget unit is equivalent to 110 kilobits per second (kbps) of access circuit bandwidth. This bandwidth equivalent is based on International Telecommunications Union – Telecommunication (ITU-T) Recommendation G.711 encoding rate plus IPv6 packet overhead plus ASLAN Ethernet overhead. The G.711 encoding rate is used for the voice session budget unit even though other EI codecs, with lower bandwidth requirements, may be used in the network. Note that IPv6 overhead, not IPv4 overhead, is used in the determination of bandwidth equivalents here.

The terms "inbound" and "outbound" in the context of ASAC are always relative to an SC. An inbound session is one that has been initiated by an EI outside a given SC's domain, whereas an outbound session is one that is initiated by an EI within a given SC's domain. Performing ASAC separately on an inbound and outbound basis is called directionalization, and is optional.

The SC maintains the ASAC session state of each EI in its domain. That is, the SC knows whether the EI is in a busy state (including both the session setup phase and active session phase) and, if busy, the precedence level of the session.

The SC and its associated SS maintains the total number of interbase IP sessions in progress plus the number of session attempts in the session setup phase. This value is the IP Count (IPC). Optionally, separate counts for inbound sessions (IPCi) and outbound sessions (IPCo) may also be maintained.

At the SC, a TDM Session Budget (TDMB) is configured and a TDM Session Count (TDMC) is maintained. The values for these items are in terms of digital signal level 0 (DS0s) on the TDM trunks between the SC and any local EO/Small EO (SMEO)/Private Branch Exchange (PBX) 1/PBX2.

2.4.1.2 Video Budgets and Counts

Since the bandwidth of a video session can vary, video sessions are 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.

Video budget and count values are in VSUs and are similar in concept to voice budgets and counts, except that no TDM-related items are maintained for video:

VDB	the configured video session budget (optional).
VDBi	the configured inbound video session budget (optional).
VDBo	the configured outbound video session budget (optional).
VDC	the count of video sessions, in VSUs.
VDCi	the count of inbound video sessions, in VSUs (optional).
VDCo	the count of outbound video sessions, in VSUs (optional).

2.4.2 ASAC Session Control Overview

2.4.2.1 Outbound (Originating-Outgoing) Voice Sessions

When an outbound session is initiated, the SC checks whether the VoIP count (IPC) is less than the VoIP budget (IPB). If so, the SC forwards the session request to its associated SS for further processing.

If IPC equals IPB, and all existing sessions traversing the SC-to-SS link are at a precedence level equal to or greater than the new session request, the new session is not placed. If the new session attempt is a precedence call (i.e., PRIORITY or higher), the calling party receives a BPA. If the new session attempt in this circumstance is a ROUTINE call, the caller receives an “all trunks busy” indication (also known as “fast busy’).

If IPC equals IPB and at least one existing session is of lower precedence than the new session, the SC preempts one of the lowest precedence sessions and forwards the session INVITE (via the SS) to the sessioned SC for processing.

2.4.2.2 Inbound (Incoming-Terminating) Voice Sessions

When an inbound session INVITE is received by an SC, the SC checks whether the VoIP count (IPC) is less than the VoIP budget (IPB). If so, and the called party is not busy, the SC places the session.

If IPC is less than IPB and the called party is busy with a session that is at a lower precedence level than the one being placed, the SC preempts the existing session and places the new session.

If IPC is less than IPB and the called party 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. If the new session attempt is a precedence call, the calling party receives a BPA. If the new session attempt is a ROUTINE call, the caller receives “fast busy”.

If IPC equals IPB, and the called party is not busy, but all existing sessions traversing the SC-to-SS link are at a precedence level equal to or greater than the new session request, the new session is not placed. The caller receives a BPA, or if it is a ROUTINE call, the caller receives "fast busy".

If IPC equals IPB, and the called party is busy with a session that is of a lower precedence level than the new session, the SC preempts the existing session and forwards the session INVITE to the called party.

If IPC equals IPB, and the called party is busy with a session that is of equal or higher precedence level than the new session, the session is not placed. The caller receives a BPA, or if it is a ROUTINE call, the caller receives "fast busy".

The IPC must be incremented for each inbound and outbound session placed, and decremented for each such session taken down.

NOTE: Intra-enclave calls are subject to preemption rules but are not affected by session budgets or impact session counts.

2.4.2.3 Directionalization

If ASAC directionalization is implemented, directionalized session budgets (IPBo and IPBi) will be set and separate IPCo and IPCi counts will be maintained by the SC in order to ensure that these counts do not exceed their respective budgets. Outbound and inbound ASAC is carried out independently from each other, with each using the respective process described above.

2.4.2.4 Video Session Processing

ASAC processing of video sessions is similar to ASAC processing for VoIP sessions. However, some extensions to the VoIP rules are needed because video sessions consume varying VSU amounts (e.g., one video session could count as 1 VSU against the budget, but another video session could be consuming 8 VSUs):

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.

2.5 PRECEDENCE-BASED ASSURED SERVICES

DoD UC networks support Precedence-Based Assured Services (PBAS) for delivery of UC services. Connections and resources that belong to a call from a UC subscriber are marked with a precedence level and domain identifier and can only be preempted by calls of higher precedence from UC users in the same service domain. Precedence provides for preferred handling of PBAS service requests. PBAS involves assigning and validating priority levels to calls, and prioritized treatment of service requests.

There are five precedence levels; from lowest to highest they are ROUTINE, PRIORITY, IMMEDIATE, FLASH, and FLASH OVERRIDE.

The maximum precedence level of a subscriber is set at the subscription time by the UC network administrator based on the subscriber's validated need. When initiating a session, the subscriber may select a precedence level up to and including the maximum authorized precedence level for that subscriber, on a per call basis.

The network at the subscriber's originating interface ensures that the selected precedence level does not exceed the maximum level assigned to that telephone number. A call will default automatically to the ROUTINE precedence unless a higher precedence is dialed.

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

Four characteristics of preemption follow:

1. Generally, any party whose connection is terminated, whether that resource is reused or not, receives a distinctive preemption notification.
2. Any called party of an active call that is being preempted by a higher precedence call must acknowledge the preemption by going "on-hook," before being connected to the new calling party.
3. When there are no idle resources, preemption of the lowest precedence resources occurs.
4. A call can be preempted any time after the precedence level of the call has been established and before call clearing has begun.

After attempting a precedence call, the calling party receives an audible ringback precedence call tone when the call is offered successfully to the called party.

If the attempted precedence call is not offered to the intended party – because of other calls of equal or higher precedence, or the called party belongs to a network that does not support preemption and there are insufficient resources on that network – the calling party receives a Blocked Precedence Announcement (BPA).

A Busy Not Equipped Announcement (BNEA) is played to the calling party of a precedence call when the called party is busy and classmarked as non-preemptable.

Precedence calls (i.e., PRIORITY and above) that are not responded to by the called party are diverted to an attendant console.

2.6 VOICE FEATURES AND CAPABILITIES

This section describes the following Assured Services voice features and capabilities:

- Call Forwarding.
- Precedence Call Waiting.
- Call Transfer.
- Call Hold.
- Three-Way Calling.
- Hotline Service.
- Calling Number Delivery.
- Call Pick-Up.
- Precedence Call Diversion.

2.6.1 Call Forwarding

Four types of VVoIP Call Forwarding (CF) features are considered for UC:

- Call Forwarding Variable (CFV).
  - When the CFV feature is active for a given user's Directory Number (DN), calls intended for that DN are redirected to a user-specified DN (DSN Number or commercial). A user can activate and deactivate CFV for his DN, and specifies the desired terminating DN during each activation. Users cannot answer calls at a DN for which CFV is active, but can originate calls at that DN.
- Call Forwarding Busy Line (CFBL).
  - When Call Forwarding Busy Line (CFBL) is configured for a given DN, calls intended for that DN are redirected to a configured DN when the former DN is busy.
- Call Forwarding – Don't Answer – All Calls (CFDA).
  - Calls to DNs configured with CFDA that are not answered after a user -specified number of ringing cycles are redirected to a configured DN. NOTE: if the DN to which unanswered calls are forwarded is busy, the original DN continues to ring until the originator of the call abandons it or the call is answered.
- Selective Call Forwarding (SCF).

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

Call forwarding interaction with PBAS is optional. Figure 2.6-1, Call Forwarding Logic Diagram, shows the VVoIP CF treatment logic.

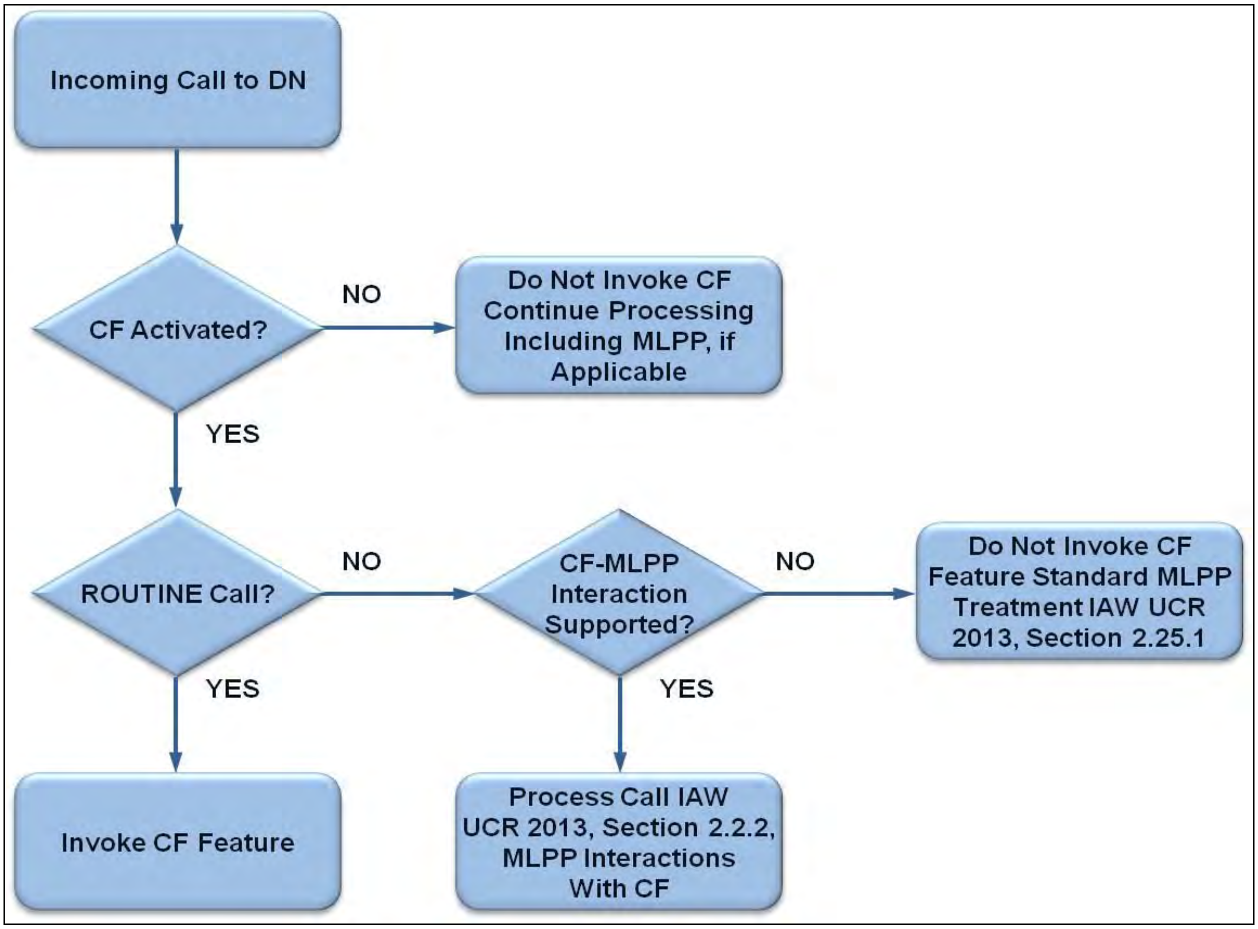

Incoming Call to DN
CF Activated?
NO
Do Not Invoke CF Continue Processing Including MLPP, if Applicable
YES
ROUTINE Call?
NO
CF-MLPP Interaction Supported?
NO
Do Not Invoke CF Feature Standard MLPP Treatment IAW UCR 2013, Section 2.25.1
YES
YES
Invoke CF Feature
Process Call IAW UCR 2013, Section 2.2.2, MLPP Interactions With CF

Figure 2.6-1. Call Forwarding Logic Diagram

2.6.2 Precedence Call Waiting

The UC Precedence Call Waiting feature is for single-call-appearance VoIP phones, Terminal Adapters (TAs), and Integrated Access Devices (IADs) only. It is not a feature for multiple-call-appearance VoIP phones.

When a DN is busy with a call at the same or lower precedence level as an incoming precedence call (i.e., PRIORITY or above), the called party receives the Precedence Call Waiting (CW) tone. The called party can place the current active call on hold, or disconnect the current active call, and answer the incoming precedence call. If the called party does not answer, the incoming precedence call is diverted to attendant (see Precedence Call Diversion below).

2.6.3 Call Transfer

Two types of call transfer are supported:

- A normal call transfer takes place when a user transfers an incoming call to another party.
- An explicit call transfer happens when both calls are originated by the same subscriber.

When a call transfer is made at different precedence levels, the resulting connection is classmarked at the highest precedence level of the two segments of the transfer.

2.6.4 Call Hold

Call Hold is invoked by going "on-hook," then "off-hook." Calls on hold retain the precedence of the originating call. All DNs are subject to normal preemption procedures.

Figure 2.6-2, Call Hold Scenarios, illustrates three typical call hold scenarios. In each scenario, caller #3 is on hold with caller #1, and caller #1 is talking to caller #2.

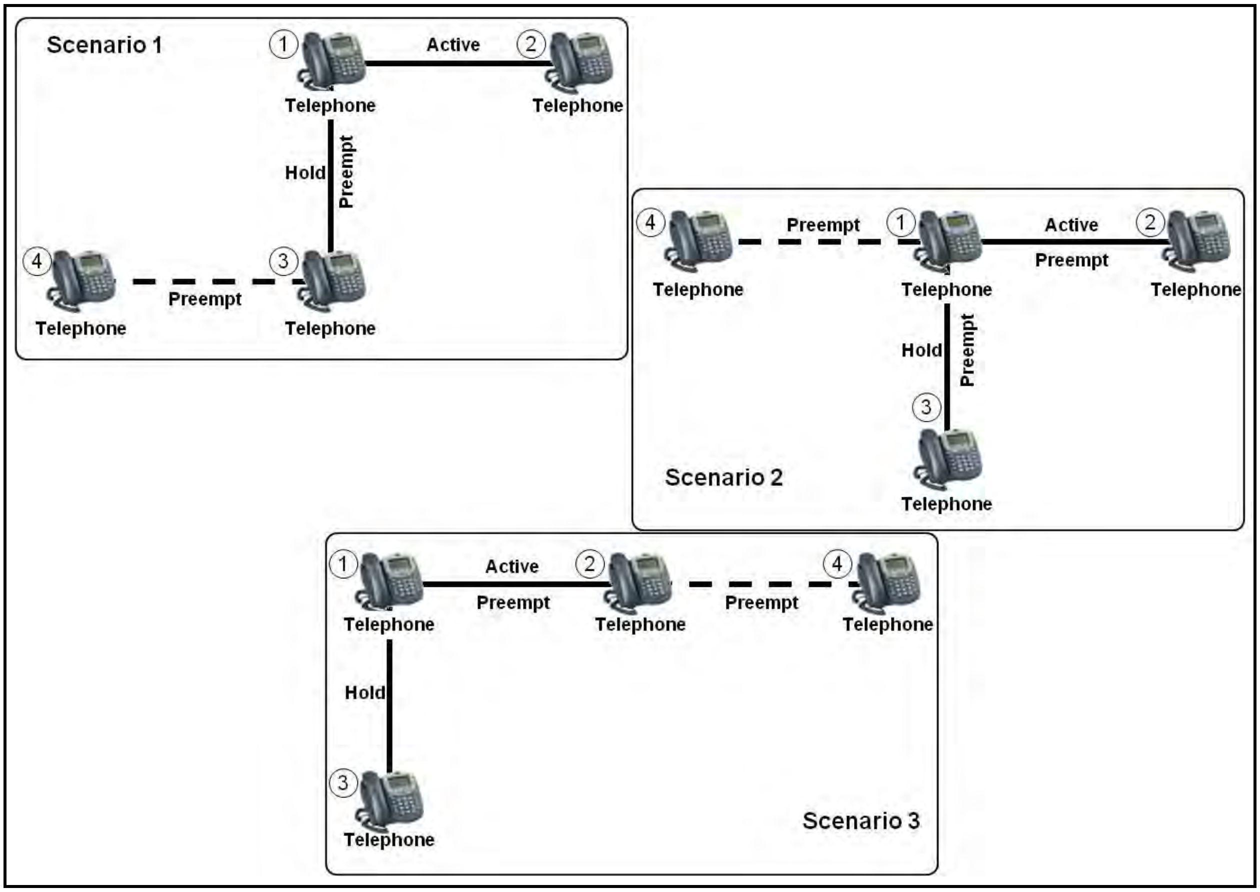


Figure 2.6-2. Call Hold Scenarios

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

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

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

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

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

2.6.5 Three-Way Calling

In Three-Way Calling (TWC), each call has its own precedence level. When a three-way conversation is established, each connection maintains its assigned precedence level. Each connection of a call resulting from a split operation maintains the precedence level that it was assigned upon being added to the three-way conversation. However, originator of the three-way call is classmarked at the highest precedence level of the two segments of the call. Incoming precedence calls to lines participating in TWC that have a higher precedence than the TWC originator invoke preemption (unless the call is marked non-preemptable).

2.6.6 Hotline Service

Hotline Service allows a user to initiate a voice or data call to a predetermined party automatically simply by "going off hook."

2.6.7 Calling Number Delivery

Called parties are provided with the number of the calling party, based on dialing plan used by the calling instrument:

- If the incoming call is from another DSN user, the calling number delivered is the 10-digit DSN number.

- If the incoming call is from a commercial user, the calling number delivered to the called party is in national or international calling number format.

The name, organization and location of the calling party may also be provided, when the called and calling parties are served by the same SC.

2.6.8 Call Pick-Up

Call Pick-Up is an optional feature that allows a user to answer calls directed to other users within a preset pick-up group.

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

- Basic Call Pick-Up.
  - An EI may answer a call that has been offered to another EI in its common call pick up group in a business group. This is accomplished by dialing a pick-up access code while the called EI is being rung. If more than one EI in the group is being rung, the EI that has been ringing longer shall be picked up first.
- Directed Call Pick-Up.
  - Directed call pick-up permits a user to dial a code and destination number and pick up a call that has been answered or is ringing at another telephone, provided the rung telephone permits dial pick-up. If the other EI has answered, a TWC is established.
- Directed Call Pick-Up Without Barge-In.
  - This feature is identical to the Directed Call Pick-Up feature, except that if the destination number being picked up has already answered, the party dialing the pick-up code shall be routed to reorder rather than be permitted to barge in on the established connection to create a TWC.

If a Call Pick-Up feature is provided, it must support precedence and preemption. When a call pick-up group has more than one party in an unanswered condition and the unanswered parties are at different precedence levels, a call pick-up attempt in that group retrieves the highest precedence call first. If multiple calls of equal precedence are ringing simultaneously, a call pick-up attempt in that group retrieves the longest ringing call. If a party in a call pick-up group is busy, and an incoming precedence call is placed to that number, normal PBAS rules apply.

2.6.9 Precedence Call Diversion

Unanswered precedence calls (i.e., PRIORITY and above) are diverted to a designated DN (e.g., attendant console), after a specified period. This diversion takes place before any forwarding to voice mail or Automatic Call Distribution (ACD) systems.

Incoming precedence calls to the attendant’s listed DN, and incoming calls diverted to an attendant, signal the attendant by a distinctive visual signal indicating the precedence level, and are placed in queue. Call distribution is used to reduce excessive waiting times. Each attendant position operates from a common queue or set of queues. Incoming calls are queued for attendant service by precedence and time of arrival. The highest precedence call with the longest holding time is answered first. A recorded message of explanation is played to the parties waiting in queue.

In some cases, the B/P/C/S where the SC or SS is located may not have a continuously manned Attendant Station (or set of Attendant Stations). In these cases, Precedence Call Diversion provides an announcement back to the calling party (the party whose call was diverted), providing them with a DSN number that gives them access to a continuously manned attendant.

- Support for Precedence Call Diversion from one UC EI to another UC EI on the same SC is required.
- Support for Precedence Call Diversion from an UC EI on one SC to an UC EI on another SC is required.
- Support for Precedence Call Diversion from an UC EI on an SC to a DSN EI (on an EO, SMEO, PBX1, or PBX 2) is not required.
- Support for Precedence Call Diversion from a DSN EI (on an EO, SMEO, PBX1, or PBX 2) to an UC EI on an SC is not required.

2.6.10 Public Safety Voice Features

2.6.10.1 Basic Emergency Service (911)

The Basic 911 Emergency Service feature provides a three-digit universal telephone number (e.g., 911) that gives direct access to an emergency service bureau. 911 calls may be routed either to a DoD emergency response center, or to a PSTN 911 PSAP. Calling 911 does not require the use of access codes such as 99. 911 calls are not subject to PBAS/MLPP preemption.

See Section 3.4.1 for a description of E911 Management Systems.

2.6.10.2 Tracing of Terminating Calls

The Tracing of Terminating Calls feature identifies the calling number on intraoffice and interoffice calls terminating to a specified DN. When this feature is activated, the originating DN, the terminating DN, and the time and date are recorded for each call to the specified line.

2.6.10.3 Outgoing Call Tracing

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

2.6.10.4 Tracing of a Call in Progress

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.

2.6.10.5 Tandem Call Trace

The Tandem Call Trace feature identifies the calling party of a call to a specified office DN for calls that involve a SS. A record of the calling party number and terminating DN, and the time and date, is generated for every call to the specified DN.

2.7 END INSTRUMENTS

The following End Instrument (EI) types are considered in UC:

- Proprietary IP voice EIs.
- Proprietary IP video EIs.
- ROUTINE-only EIs.
- AS-SIP voice EIs.
- AS-SIP video EIs.
- AS-SIP Secure voice EIs.
- Secure IP EI (using SCIP/V.150.1 protocol).
- Softphone.

Issues unique to classified EIs are described in Appendix B, Unique Classified Unified Capability.

An EI that uses vendor-proprietary signaling is indicated by PEI in this document and in UCR 2013. Both ITU H.323 and Internet Engineering Task Force (IETF) SIP (i.e., commercial SIP, not DISA-specified AS-SIP) also are considered vendor-proprietary EI to SC protocols. They are treated as vendor-proprietary protocols because one EI vendor's implementation of H.323 or SIP is not guaranteed to interoperate with another SC vendor's implementation of H.323 or SIP.

A ROUTINE-only EI (ROEI) is an EI that meets the PEI requirements in UCR 2013, Section 2, except that it is not required to support PBAS. Any SC that supports ROUTINE-only voice EIs must also support voice EIs that fully support PBAS. An SC is allowed to support ROUTINE-only video EIs without supporting fully PBAS-capable video EIs.

An AS-SIP voice EI is a UC voice phone (Hard-Phone or Soft-Phone) that uses AS-SIP signaling instead of vendor-proprietary signaling.

An AS-SIP video EI is a UC video phone (Hard-Phone or Soft-Phone) that uses AS-SIP signaling instead of vendor-proprietary signaling. A proprietary video EI is a video phone that uses vendor-proprietary signaling. The AS-SIP video EIs and proprietary video EIs are video phones (Hard-Phones or Soft-Phones), and are not MCUs. MCUs are more complex than video phones, and involve point-to-multipoint video conferences instead of point-to-point video calls.

An AS-SIP secure voice EI is a UC secure voice phone (hardphone only) that uses AS-SIP signaling instead of vendor-proprietary signaling. A proprietary secure voice EI is a secure phone that uses vendor-proprietary signaling. 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 end-to-end voice communication is done "in the clear."

A softphone is an end user software application on an approved operating system that enables a general-purpose computer to function as either a PEI or AEI. The softphone is conceptually identical to a traditional IP "hard" telephone and is generally required to provide the voice features and functionality provided by a traditional IP hard telephone.

2.7.1 Voice over IP Sampling Standard

For Fixed-to-Fixed calls, EIs 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 use of different voice sample lengths and voice payload packet sizes is 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.

Using the 24-Kbps version of the G.722.1 codec with a 20-ms voice sample frame length, and two frames per packet, results in a packet-per-second rate of 25 PPS (one packet per every 40 ms). Each packet has 960 bits, or 120 bytes, of payload.

The 32-Kbps G.722.1, with a 20-ms frame length and two frames per packet, also has a 25 PPS rate, but each packet has 1280 bits, or 160 bytes, of payload.

The G.723.1 codec has two bit rates: 5.3- and 6.3-Kbps. Both use a frame size of 30 ms. At one frame per packet, the PPS rate is 33.3. The payload for the low bit rate version is 20 bytes and the payload for the high bit rate version is 24 bytes.

2.7.2 Operational Framework for AS-SIP EIs

This section describes a framework for how voice EIs, secure voice EIs, and video EIs (also known as video codecs) connect to, and interoperate with any VVoIP vendor's SC, using AS-SIP protocol instead of the various vendor-proprietary SC-to-EI protocols.
The basic change needed to support AS-SIP EIs is to add SC-to-AS-SIP-EI interfaces where proprietary SC-to-EI interfaces are currently supported:

- The SC CCA (called just the SC here).
- The Voice EI (for both the hardphone EI and the softphone EI).
- The Secure Voice EI (hardphone EI only).
- The Video EI (for both the hardphone EI and the softphone EI).

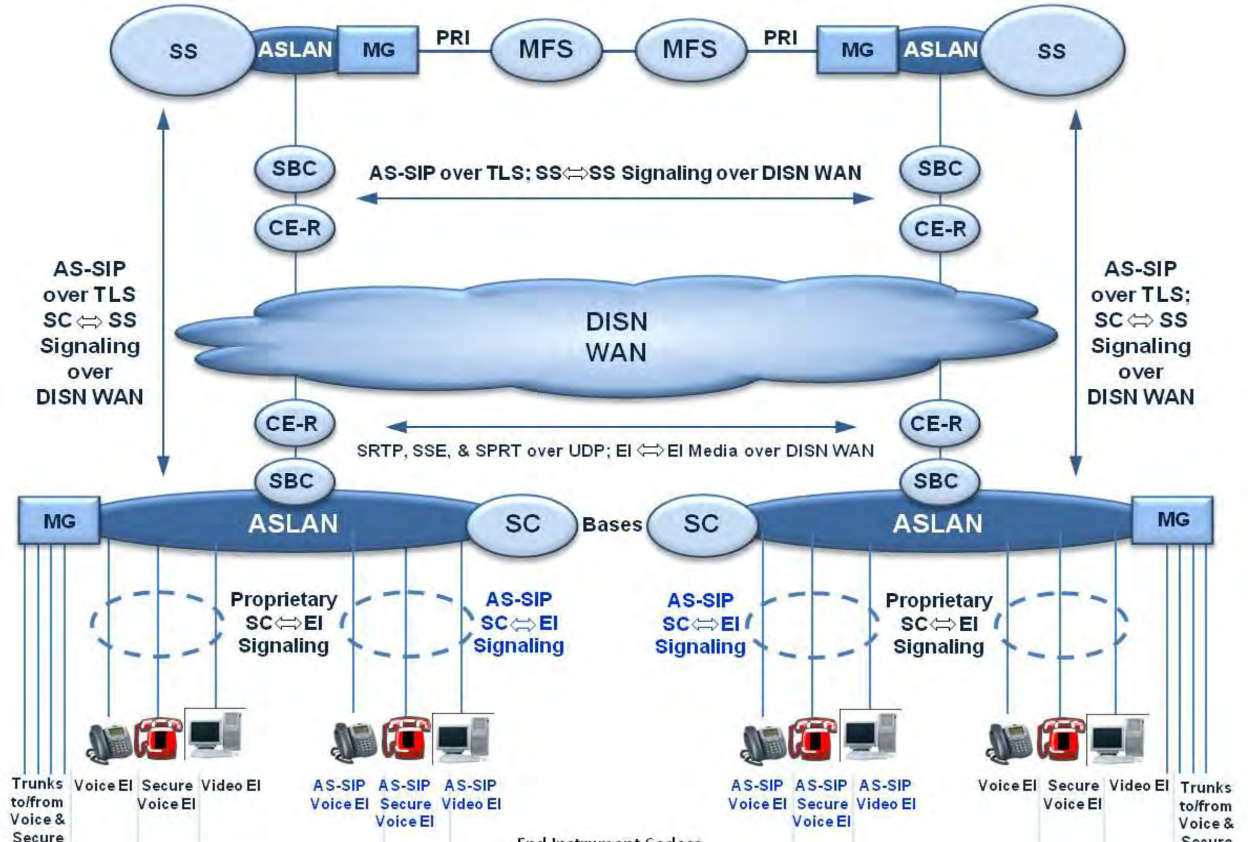
Secure video EIs (e.g., Video EIs that use SCIP to encrypt video media streams) are outside the scope of this section.

AS-SIP EI capabilities do not need to be supported in the following VVoIP NEs:

- The MG-Transport Switching (TS) and MG-MG-LAN Switch (LS).
- TAs.
- IADs.

The signaling interfaces between the SC CCA and the MG-TS, between the SC CCA and the MG-LS, between the SC CCA and the TA, and between the SC CCA and the IAD are vendor-proprietary.

Figure 2.7-1, Framework for Proprietary and Generic AS-SIP EIs, shows the support for AS-SIP EIs in a UC network (using multivendor-interoperable AS-SIP SC-EI signaling). The UC network still supports vendor-proprietary EIs using vendor-proprietary SC-EI signaling. As a result, both proprietary EIs using proprietary signaling and AS-SIP EIs using AS-SIP signaling are shown in Figure 2.7-1.


SS
ASLAN
MG
PRI
MFS
MFS
PRI
MG
ASLAN
SS
SBC
AS-SIP over TLS; SS⇔SS Signaling over DISN WAN
SBC
CE-R
CE-R
AS-SIP over TLS SC⇔SS Signaling over DISN WAN
DISN WAN
AS-SIP over TLS; SC⇔SS Signaling over DISN WAN
CE-R
CE-R
SRTP, SSE, & SPRT over UDP; EI⇔EI Media over DISN WAN
SBC
SBC
MG
ASLAN
SC
Bases
SC
ASLAN
MG
Proprietary SC⇔EI Signaling
AS-SIP SC⇔EI Signaling
AS-SIP SC⇔EI Signaling
Proprietary SC⇔EI Signaling
Trunks to/from Voice & Secure Voice Phones on DSN and PSTN
Voice EI
Secure Voice EI
Video EI
AS-SIP Voice EI
AS-SIP Secure Voice EI
AS-SIP Video EI
AS-SIP Voice EI
AS-SIP Secure Voice EI
AS-SIP Video EI
Voice EI
Secure Voice EI
Video EI
Trunks to/from Voice & Secure Voice Phones on DSN and PSTN

End Instrument Codecs

Voice EI, AS-SIP Voice EI	G.711, G.729/A optional: G.722.1, G.723.1
Video EI, AS-SIP Video EI	H.263-2000, H.264 optional: H.261, H.264 SVC
Secure Voice EI	G.711 with SCIP Encryption
AS-SIP Secure Voice EI	V.150.1 with SCIP Encryption

Figure 2.7-1. Framework for Proprietary and AS-SIP EIs

2.7.2.1 AS-SIP Secure Voice EI Supplementary Services

SCs support the following supplementary services for voice calls on AS-SIP secure voice EIs, consistent with Section 2.6, Assured Services Voice Features and Capabilities, using AS-SIP signaling:

- Precedence Call Waiting.
- Call Forwarding.
- Call Transfer.
- Call Hold.
- Three-Way Calling.
- Calling Number Delivery.
- Call Pickup.

SCs 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 end-to-end exchange of V.150.1 SSE messages in the media path (and not in the signaling path). As a result, if an SC provides a supplementary service to an AS-SIP EI for voice calls, the SC also provides that supplementary service to the AS-SIP EI for secure voice calls (since the SC on its own cannot distinguish between a voice call at an AS-SIP EI and a secure voice call at that AS-SIP EI).

A 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 TWC), 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.

2.7.3 V.150.1 Modem Relay Secure Phone

This section describes the architecture for V.150.1 Modem Relay support by UC MGs of SCIP-based secure phones for all scenarios required by the National Security Agency (NSA).

V.150.1 Secure Phone Support relies on the following:

- SCIP-216 Modem Relay capabilities in UC MGs, TAs, and IADs.
- SCIP-215 Modem Relay capabilities in UC 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.
- Voiceband Data (VBD).
- Modem Relay.

2.7.3.1 Architecture for Supporting SCIP/V.150.1 Modem Relay

Support for SCIP phones and V.150.1 is achieved by adding Modem Relay capabilities to the following UC 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 Integrated Services Digital Network (ISDN) PRI and Channel Associated Signaling (CAS) Trunk Groups.
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 optional in the UCR.
3. Analog Terminal Adapter (ATA). A device on the UC 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 optional in the UCR.
4. Integrated Access Device (IAD). A device on the end user's premise that supports interconnection between the ASLAN and multiple end user analog telephones, analog secure telephones, analog fax machines, and analog modems. This device supports a single Ethernet RJ-45 interface on the ASLAN side, and multiple analog RJ-11 interfaces on the end user side. Support for modem relay in the IAD is optional in the UCR.
5. AS-SIP Components of the SC and SS. The SC and SS CCAs must support new AS-SIP and SDP signaling for modem relay calls. Additional SDP lines for the modem relay media type are added to existing SDP lines for the audio media type in AS-SIP INVITE, UPDATE, 180 (Ringing), 183 (Session Progress), 200 (OK), and Acknowledgement (ACK messages).

Modem relay capabilities do not need to be added to the SBC. The SBCs 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 UC 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 Real Time Protocol (RTP) for media transfer and Secure RTCP for media control) and the secure portion of the call (which uses SPRT and SSE for media transfer and does not use Secure RTCP for media control). 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 SBCs.

When a nonsecure call is established between two IP media endpoints, a Secure RTP media stream is established using one UDP port number and a Secure RTCP media control stream is established using a second UDP port number. The SBC (when the media traverses an SBC) opens a UDP pinhole for the Secure RTP traffic and another UDP pinhole for the Secure RTCP traffic. When the call transitions from nonsecure (clear) voice using SRTP to secure voice using SPRT, the SPRT media stream reuses the UDP port number and SBC pinhole that were previously used by the SRTP media stream. The Secure Real-Time Transport Control Protocol (SRTCP) is turned off during this transition but the UDP port number used for the SRTCP media control stream is maintained by the IP media endpoints and the UDP pinhole for the SRTCP media control stream is maintained by the SBC until the call is terminated. The port number and pinhole are maintained so that if the call transitions back to nonsecure voice, the RTCP port number and RTCP pinhole can be reused. In other words, if the call transitions from secure voice using SPRT back to nonsecure voice using SRTP, the new SRTP media stream reuses the UDP port number and SBC pinhole that were previously used by the original SRTP media stream. There also is a new SRTCP media control stream after this transition and the separate UDP port number for SRTCP is reused by the IP endpoints and the separate pinhole for SRTCP is reused by the SBC. One other architecture change is the addition of Secure IP Phones to the UC Network. Here, these Secure IP Phones are called IP SCIP Phones also.

Figure 2.7-2, Framework for SCIP Phones in Using VoIP, and Figure 2.7-3, Framework for SCIP Phones Using Modem Relay, show the frameworks for supporting analog and IP SCIP Phones in a VoIP network and a Modem Relay network, using modem relay media and either proprietary Phone-to-SC signaling or AS-SIP Phone-to-SC signaling. The Modem Relay network continues to support audio media in MGs, ATAs, IADs, SCs, and SBCs for backward compatibility with VoIP network operation.

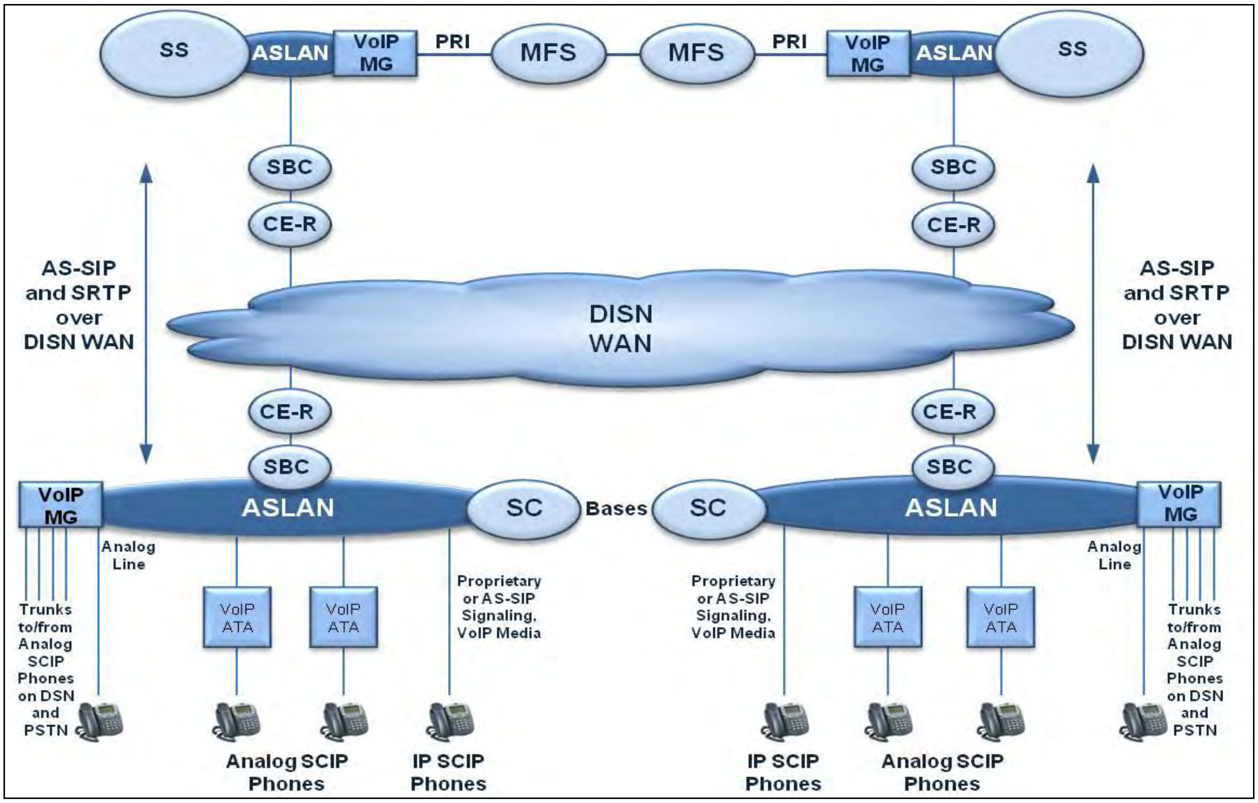

SS
ASLAN
VoIP MG
PRI
MFS
MFS
PRI
VoIP MG
ASLAN
SS
SBC
CE-R
SBC
CE-R
AS-SIP and SRTP over DISN WAN
DISN WAN
AS-SIP and SRTP over DISN WAN
CE-R
SBC
CE-R
SBC
VoIP MG
ASLAN
SC
Bases
SC
ASLAN
VoIP MG
Analog Line
Trunks to/from Analog SCIP Phones on DSN and PSTN
VoIP ATA
VoIP ATA
Proprietary or AS-SIP Signaling, VoIP Media
Proprietary or AS-SIP Signaling, VoIP Media
VoIP ATA
VoIP ATA
Analog Line
Trunks to/from Analog SCIP Phones on DSN and PSTN
Analog SCIP Phones
IP SCIP Phones
IP SCIP Phones
Analog SCIP Phones

Figure 2.7-2. Framework for SCIP Phones Using VoIP

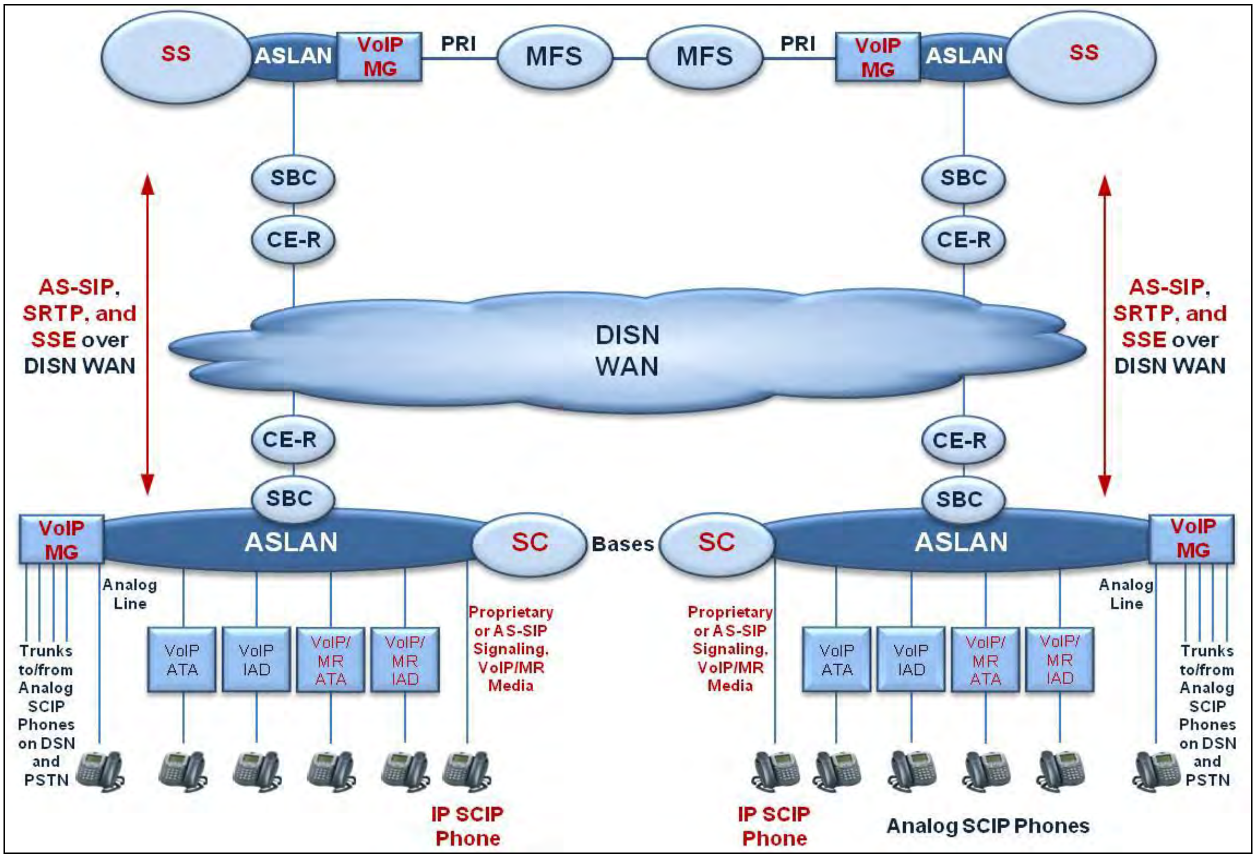

SS
ASLAN
VoIP MG
PRI
MFS
MFS
PRI
VoIP MG
ASLAN
SS
SBC
CE-R
SBC
CE-R
AS-SIP, SRTP, and SSE over DISN WAN
DISN WAN
AS-SIP, SRTP, and SSE over DISN WAN
CE-R
SBC
CE-R
SBC
VoIP MG
ASLAN
SC
Bases
SC
ASLAN
VoIP MG
Analog Line
Proprietary or AS-SIP Signaling, VoIP/MR Media
Proprietary or AS-SIP Signaling, VoIP/MR Media
Analog Line
Trunks to/from Analog SCIP Phones on DSN and PSTN
VoIP ATA
VoIP IAD
VoIP/ MR ATA
VoIP/ MR IAD
VoIP ATA
VoIP IAD
VoIP/ MR ATA
VoIP/ MR IAD
Trunks to/from Analog SCIP Phones on DSN and PSTN
IP SCIP Phone
IP SCIP Phone
Analog SCIP Phones

Figure 2.7-3. Framework for SCIP Phones Using Modem Relay

2.7.3.2 SCIP/V.150.1 Gateway

For UCR purposes, a “SCIP Gateway” is any VoIP Gateway that conforms to SCIP-216, Revision 2.1. 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.

For UCR purposes, a “SCIP/V.150.1 Gateway” is a VoIP Gateway that conforms to SCIP-216 and is served by an SC. Media Gateways, ATAs, and IADs that support SCIP-216 and are served by an SC are examples of SCIP/V.150.1 Gateways.

One key difference between the SCIP Gateway and the SCIP/V.150.1 Gateway is that the SCIP Gateway only supports trunk-side connections to the PSTN and the DSN. The SCIP/V.150.1 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.

SCIP/V.150.1 Gateways are expected to be deployed in both Strategic (Fixed) networks and Tactical (Deployable) networks.

2.7.3.3 SCIP/V.150.1 End Instrument

The UC SCIP/V.150.1 End Instrument (EI), is based on 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 the UCR, 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.

In the UCR, a "SCIP/V.150.1 EI" is a Secure IP Phone that conforms to SCIP-215 and is served by an SC.

A SCIP/V.150.1 EI communicates with the SC using either vendor-proprietary signaling and transport protocols or AS-SIP signaling over TLS.

A SCIP EI might communicate only with a TDM switch on the base (which provides DSN line-side VoIP) using vendor-proprietary signaling and transport protocols.

A SCIP/V.150.1 EI also exchanges media with other EIs, MGs, ATAs, and IADs using SRTP over UDP during the audio part of the call ("talking in the clear"), and using SSE and SPRT over UDP during the modem relay part of the call ("talking secure"). A 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.

SCIP/V.150.1 EIs are expected to be deployed in both Strategic (Fixed) networks and Tactical (Deployable) networks.

It is also possible for two SCIP/V.150.1 EIs to communicate with one another over the UC VVoIP network using the SCIP-214.2 protocol, as defined in the NSA document SCIP 214.2, Secure Communication Interoperability Protocol (SCIP) over Real-Time Transport Protocol (RTP), Revision 1.0, January 2010.

Unlike SCIP-216 and SCIP-215, SCIP-214.2 does not use V.150.1 Modem Relay, SPRT, or SSE to exchange media over a VVoIP network. Instead, the SCIP media stream packets are sent from one EI to another over the VVoIP network, and do not traverse any SCIP/V.150.1 Gateways.

Before the call "goes secure," the media stream packets are exchanged between the two EIs using a VoIP codec (like G.711 or G.729) over Secure RTP. After the call goes secure, the media stream packets are exchanged between the two EIs using SCIP over Secure RTP, instead of using SCIP over SPRT. This means that the "clear voice to secure voice" transition only involves a change from a VoIP codec to the SCIP protocol; Secure RTP is used for media transport both before and after the transition.

In addition, this means that EI transitions from "clear voice" to "secure voice" and back again are transparent to SBCs, because SRTP is used to transport the media packets (and SRTCP is used to transport the media control packets) both in "clear voice" mode and in "secure voice" mode.

The SCIP-214.2 support is optional for SCIP/V.150.1 EIs in the UCR.

SCIP/V.150.1 EIs may use SCIP-214.2 to communicate in both Strategic (Fixed) networks and Tactical (Deployable) networks.

2.8 SESSION CONTROLLER

The Session Controller (SC) is a software-based call processing product that provides voice and video services to IP telephones and media processing devices within a service domain. Additionally, an SC extends signaling and session (call) control services to allow sessions to be established with users 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.

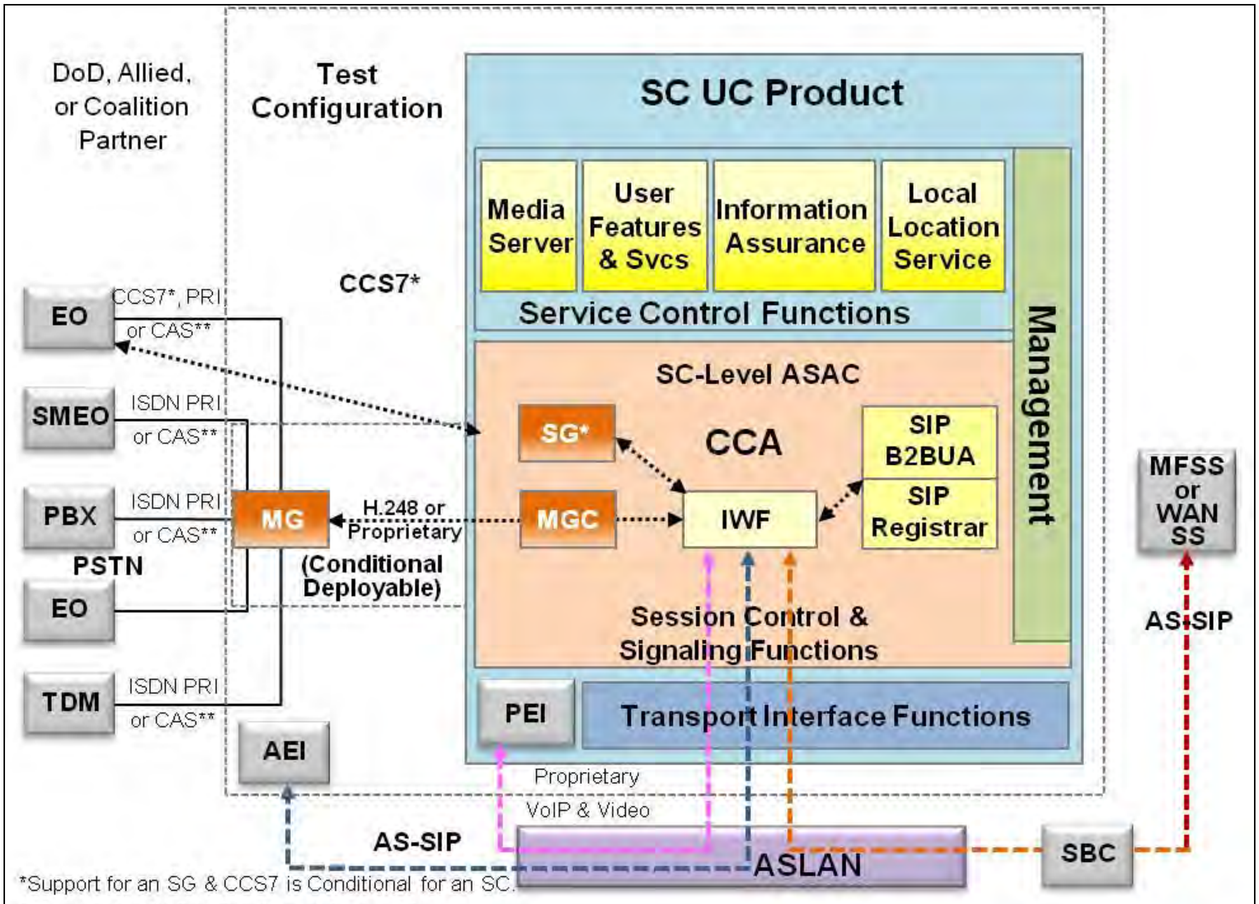
SCs that provide Hosted UC voice and video services to end instruments (EIs) located at different enclaves (i.e., B/P/C/S locations) within a designated geographic region are called ESCs. The region that encompasses the centralized ESC location together with all of the served DoD Components B/P/C/S locations is referred to as the Enterprise Services Area (ESA).

Local SCs are physically located at the B/P/C/S where the EIs they serve are located.

Multiple SCs may be deployed at a single serving area in a coordinated cluster with one SC acting as the Master SC (MSC) and the others – Subtended Session Controllers (SSCs) – subordinate to the MSC. MSC/SSC clusters may be used in both Strategic (Fixed) deployments and within tactical extensions of the DISN.

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

Figure 2.8-1, Functional Reference Model – SC, illustrates the reference model for the Session Controller.



*Support for an SG & CCS7 is Conditional for an SC.

**Support for CAS is Conditional for an SC.

LEGEND:

AEI:	AS-SIP End Instrument	MG	Media Gateway
ASAC:	Assured Services Access Control	MGC	Media Gateway Controller
ASLAN:	Assured Services Local Area Network	PBX:	Private Branch Exchange
AS-SIP:	Assured Services Session Initiation Protocol	PEI:	Proprietary IP Voice End Instrument
B2BUA:	Back-to-Back User Agent	PRI:	Primary Rate Interface
CAS:	Channel Associated Signaling	PSTN:	Public Switched Telephone Network
CSS7	Common Channel Signaling No. 7	SBC:	Session Border Controller
DOD:	Department of Defense	SC:	Session Controller
EO:	End Office	SIP:	Session Initiation Protocol
IP:	Internet Protocol	SS:	Softswitch
ISDN:	Integrated Services Digital Network	VoIP:	Voice over IP
IWF:	Interworking Function	WAN:	Wide Area Network
MFSS:	Multifunction Softswitch		

Figure 2.8-1. Functional Reference Model – SC

The SC 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 Table 2.8-1, Summary of SC Functions, provides a summary of SC functions.

Table 2.8-1. Summary of SC 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 Signaling interworking [optional] H.323, H.248 PRI, MGCP
ASAC	Executes AS functions via control of the PEI and AEI. 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 EMS.
Local Domain Directory	Subscriber information, including telephone number, organization name, code address, and subscriber name.
MGC	Controls the MG when the MG in included in the SC.
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 Voice End Instrument
AS: Assured Services
ASAC: Assured Services Admission Control
AS-SIP: Assured Servies Session Initiation Protocol
B2BUA: Back-to-Back User Agent
CAC: Call Admission Control
CE: Customer Edge
CoS: Class of Service
EI: End Instrument
EMS: Element Management System
IA: Information Assurance
MG: Media Gateway
MGC: Media Gateway Controller
MGCP: Media Gateway Control Protocol
PEI: Proprietary IP Voice End Instrument
RTS: Real Time Services
SBC: Session Border Controller
SC: Session Controller
UFS: User Features and Services

Table 2.8-2, SC Support for VoIP and Video Signaling Interfaces, provides a complete list of the SC signaling interfaces.

Table 2.8-2. SC Support for VoIP and Video Signaling Interfaces

FUNCTIONAL COMPONENT	VOIP AND VIDEO SIGNALING INTERFACES	VOIP AND VIDEO SIGNALING PROTOCOLS
CCA	CCA (SC)-to-CCA (SS)	AS-SIP over IP
CCA	CCA (SC)-to-PEI	Proprietary VoIP Signaling over IP
CCA	CCA (SC) to AEI	AS-SIP over IP
CCA/MGC and MG	CCA (MGC)-to-MG	ITU-T H.248 over IP (Optional - used with ISDN PRI, and CAS trunks)
CCA/MGC and MG	CCA (MGC)-to-MG	ISDN PRI over IP (Optional - North American National ISDN Version, used with ISDN PRI trunks only)
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)

LEGEND

AEI: AS-SIP IP Voice End Instrument
AS-SIP: Assured Services Session Initiation Protocol
CAS: Channel Associated Signaling
CCA: Call Connection Agent
DoD: Department of Defense
IP: Internet Protocol
ISDN: Integrated Services Digital Network
ITU-T: International Telecommunications Union – Telecommunication
MG: Media Gateway
MGC: Media Gateway Controller
PEI: Proprietary IP Voice End Instrument
PRI: Primary Rate Interface
SC: Session Controller
SS: Softswitch
VoIP: Voice over IP

The SC supports a Session Controller Location Server (SCLS) functionality that provides information on call routing and called address translation (where a called address is contained within the called SIP URI in the form of the called number). The CCA uses the routing information maintained by the SCLS to route the following:

- Internal calls from one SC PEI or AEI to another PEI or AEI on the same SC.
- Outgoing calls from an SC PEI or AEI to another SC, an SS, or a TDM network.
- Incoming calls from another SC, an SS, or a TDM network to an SC PEI or AEI.

2.9 AS-SIP GATEWAYS

2.9.1 AS-SIP TDM Gateway

2.9.1.1 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. 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 2.9-1, AS-SIP TDM Gateway Topologies, depicts examples of the two basic topologies that use the AS-SIP TDM Gateway. The first example depicts a B/P/C/S 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 a B/P/C/S with multiple TDM switches that may include a PBX2 as well as MLPP-capable TDM switches. One 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. A PBX2 (or any other non-assured services TDM switch) is not permitted to directly interface with an AS-SIP TDM Gateway.

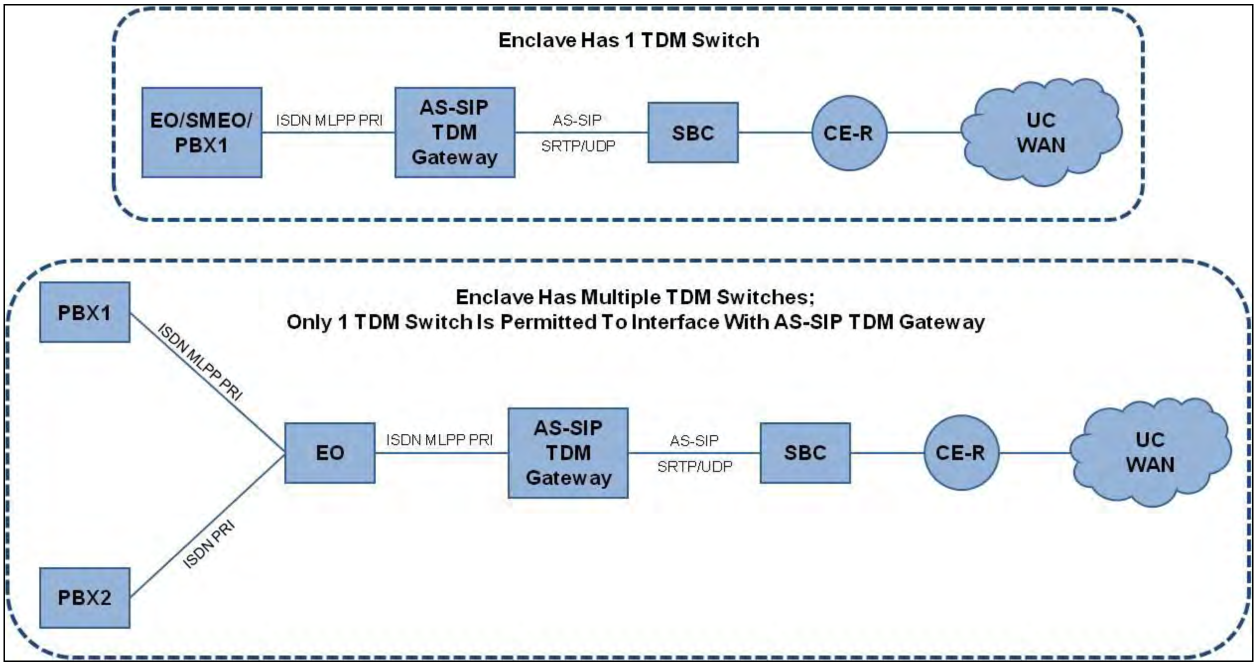


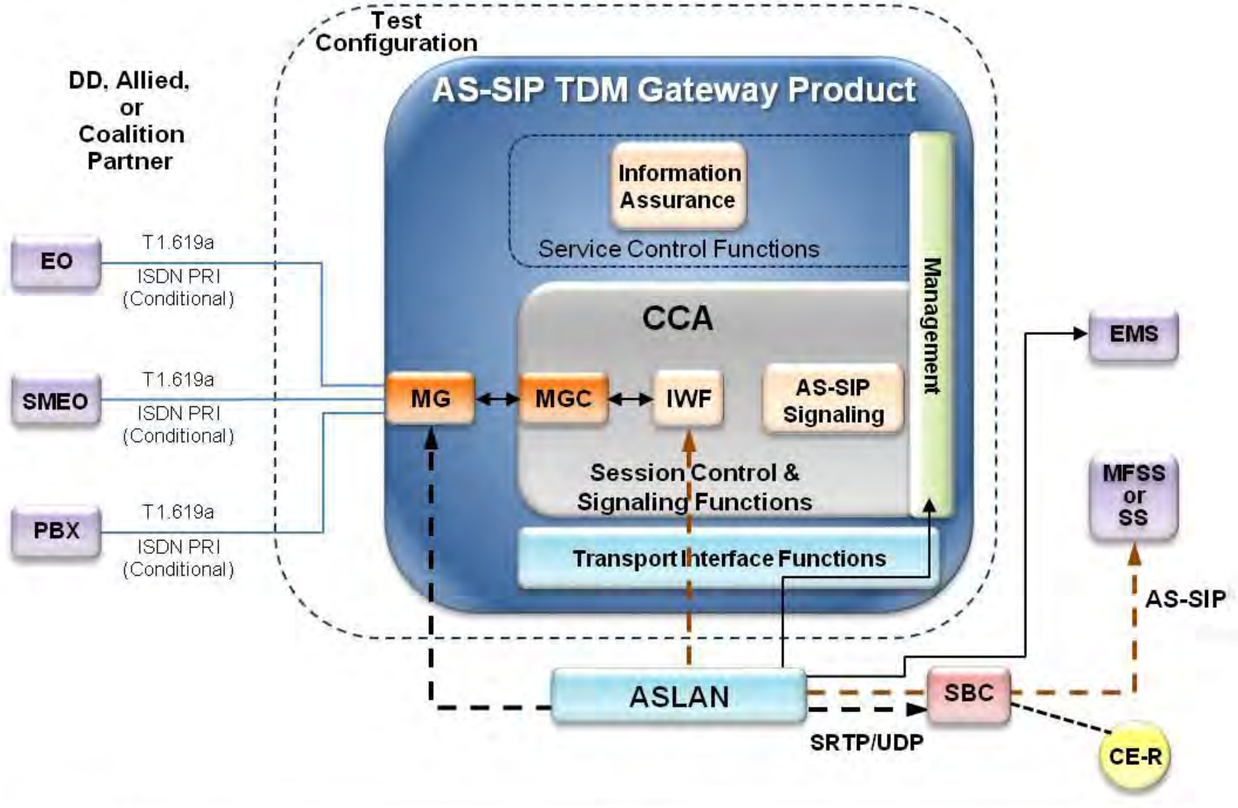
Figure 2.9-1. AS-SIP TDM Gateway Topologies

The AS-SIP TDM Gateway does not support ASAC and relies on the subtended TDM switch to perform that functionality. Appropriate traffic engineering must 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-R and the AR.

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

2.9.1.2 AS-SIP TDM Gateway Functional Reference Model

Figure 2.9-2, 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, Interworking Function (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 (Advanced DSN Integrated Management Support System [ADIMSS]) are provided by external interfaces.



LEGEND:

ASLAN	Assured Services Local Area Network	MGC	Media Gateway Controller
AS-SIP	Assured Services Session Initiation Protocol	PBX	Private Branch Exchange
CCA	Call Connection Agent	PEI	Proprietary IP Voice End Instrument
CE-R	Customer Edge Router	PRI	Primary Rate Interface
DOD	Department of Defense	SBC	Session Border Controller
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
MG	Media Gateway		

Figure 2.9-2. Functional Reference Model – AS-SIP TDM Gateway

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 2.9-1).

Table 2.9-1. AS-SIP TDM Gateway Support for VoIP and Video Signaling Interfaces

FUNCTIONAL COMPONENT	VOIP AND VIDEO SIGNALING INTERFACES	VOIP AND VIDEO SIGNALING PROTOCOLS
CCA	CCA (AS-SIP TDM Gateway) – to – CCA (SS)	AS-SIP over IP

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

LEGEND

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

2.9.2 AS-SIP IP Gateway

2.9.2.1 Overview

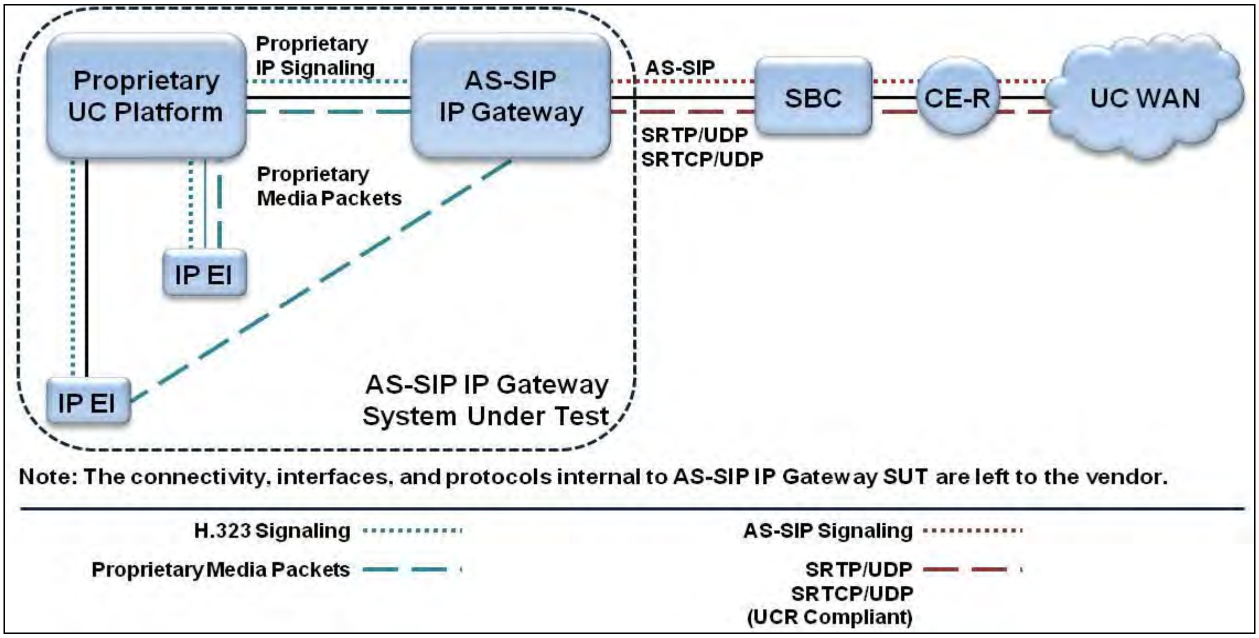
The AS-SIP IP Gateway is a VVoIP interworking appliance, and its purpose is to enable the interconnection and interoperation of proprietary IP-based UC signaling platforms and their associated IP EIs with the DISN UC system to support end-to-end voice and video sessions. The AS-SIP IP Gateway directly interfaces with only one IP-based UC signaling platform. It does not support interworking of TDM-based signaling platforms, and does not serve as a call manager for any TDM or IP EIs.

Unlike the AS-SIP TDM Gateway, the AS-SIP IP Gateway is not an Assured Services appliance.

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

The AS-SIP IP Gateway interfaces to an SBC 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 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.

Figure 2.9-3, AS-SIP IP Gateway Topology, depicts the AS-SIP IP Gateway in relation to the UC WAN where the logical interface is between the AS-SIP IP Gateway and the SBC. The internal signaling and media lines (in blue) represent notional internal connectivity options.



Note: The connectivity, interfaces, and protocols internal to AS-SIP IP Gateway SUT are left to the vendor.

Figure 2.9-3. AS-SIP IP Gateway Topology

2.9.2.2 AS-SIP IP Gateway Functional Reference Model, Assumptions, Functions and Features

Figure 2.9-4 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.

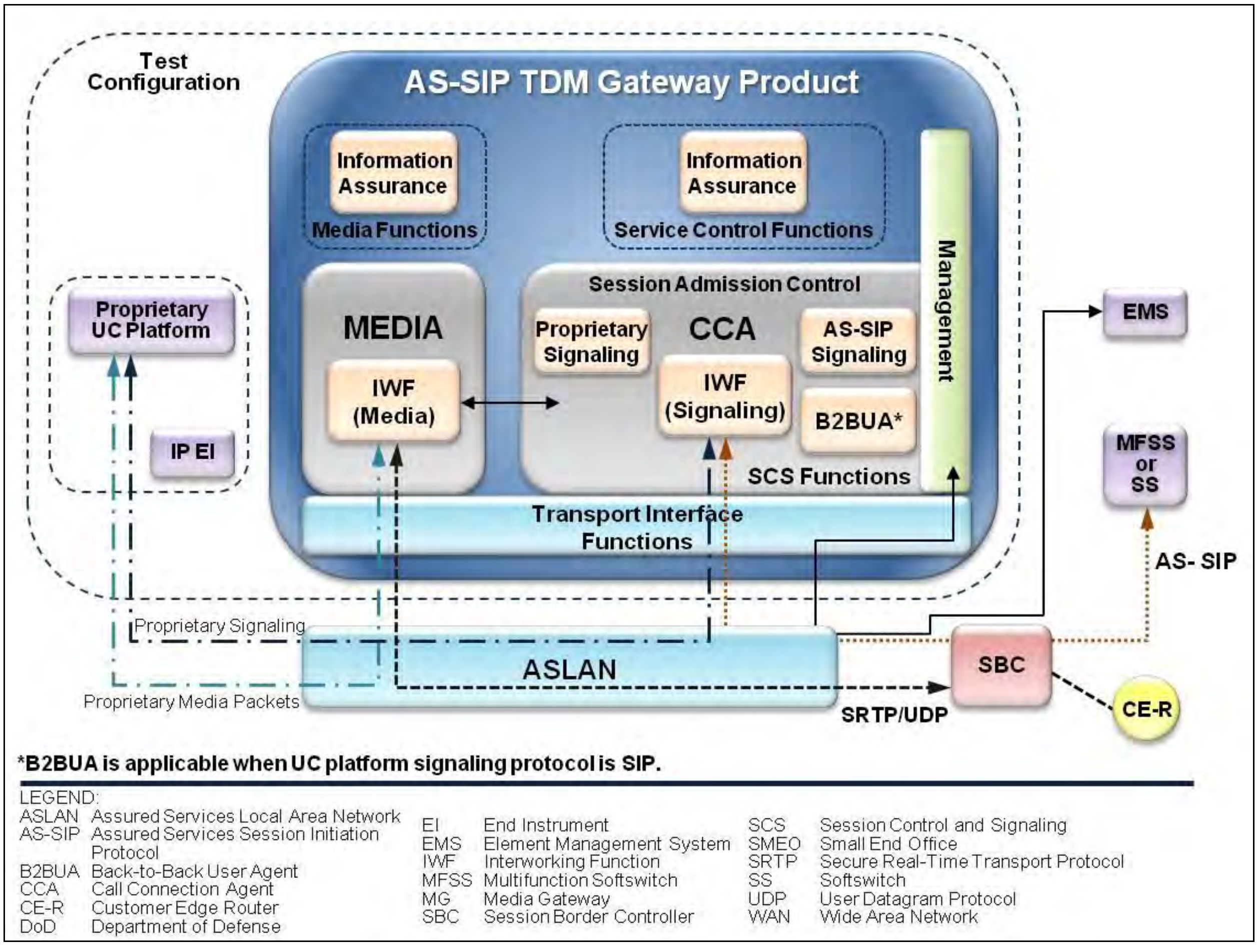

Test Configuration
AS-SIP TDM Gateway Product
Information Assurance
Media Functions
Information Assurance
Service Control Functions
Management
Proprietary UC Platform
IP EI
MEDIA
IWF (Media)
Session Admission Control
Proprietary Signaling
CCA
AS-SIP Signaling
IWF (Signaling)
B2BUA*
SCS Functions
Transport Interface Functions
EMS
MFSS or SS
AS- SIP
Proprietary Signaling
ASLAN
Proprietary Media Packets
SBC
SRTP/UDP
CE-R
*B2BUA is applicable when UC platform signaling protocol is SIP.
LEGEND:
ASLAN Assured Services Local Area Network
AS-SIP Assured Services Session Initiation Protocol
B2BUA Back-to-Back User Agent
CCA Call Connection Agent
CE-R Customer Edge Router
DoD Department of Defense
EI End Instrument
EMS Element Management System
IWF Interworking Function
MFSS Multifunction Softswitch
MG Media Gateway
SBC Session Border Controller
SCS Session Control and Signaling
SMEO Small End Office
SRTP Secure Real-Time Transport Protocol
SS Softswitch
UDP User Datagram Protocol
WAN Wide Area Network

Figure 2.9-4. Functional Reference Model – AS-SIP IP Gateway

2.9.2.2.1 Assumptions

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 Fault, Configuration, Accounting, Performance, and Security (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 SBC are as follows:

a. The SBC controls signaling streams between the AS-SIP IP Gateway and a SS. The AS-SIP IP Gateway accesses the UC WAN via the SBC and an associated AR on the UC WAN.

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

2.9.2.2.2 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 2.9-2, Summary of AS-SIP IP Gateway Functions).

Table 2.9-2. 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 EMS

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

2.9.3 AS-SIP – H.323 Gateway

2.9.3.1 Overview

The AS-SIP – H.323 Gateway is a VVoIP interworking appliance, and its purpose is to enable the interconnection and interoperation of H.323 IP-based UC signaling platforms and their associated IP EIs with the DISN UC system to support end-to-end voice and video sessions.

The Government has adopted Request for Change (RFC) 4123 – Session Initiation Protocol (SIP) – H.323 Interworking Requirements as the document which describes the requirements for the AS-SIP – H.323 Gateway.

NOTE:The AS-SIP – H.323 Gateway is not an Assured Services appliance because H.323 is not an Assured Services protocol, and its placement in this section is for requirements grouping purposes and should not be interpreted as implying that the AS-SIP – H.323 Gateway is an Assured Services appliance.

The AS-SIP – H.323 Gateway is a standalone SUT for testing purposes.

The AS-SIP H.323 Gateway interfaces to the SBC 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 H.323 UC signaling platform. The AS-SIP – H.323 Gateway is responsible for interworking UCR-compliant voice and video media packets with the voice and video media packets supported by the H.323 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 – H.323 Gateway and will not be a part of AS-SIP H.323 Gateway SUT interoperability testing.

From a signaling perspective, the AS-SIP – H.323 Gateway provides a AS-SIP-compliant signaling interface for end-to-end signaling interoperability between the AS-SIP – H.323 Gateway and the AS-SIP signaling appliances of the DISN UC WAN system.

From a media perspective, the AS-SIP – H.323 Gateway provides a UCR-compliant bearer interface for end-to-end interoperability of voice and video media packets between the AS-SIP – H.323 Gateway and SBCs, IP EIs of SCs, MGs, and AS-SIP EIs. The AS-SIP – H.323 Gateway interworks voice and video media packets generated by the IP EIs served by the IP-based UC signaling platform that are intended for a destination outside the H.323 system enclave, to UCR-compliant SRTP/UDP packets having the appropriate DSCP. Similarly, UCR-compliant SRTP/UDP voice and video media packets received from the UC WAN and intended for the IP EIs served by the H.323 UC signaling platform are interworked by the AS-SIP – H.323 Gateway into the H.323 media packets supported by the IP EIs.

Figure 2.9-5, AS-SIP – H.323 Gateway Topology, depicts the AS-SIP – H.323 Gateway in relation to the UC WAN where the logical interface is between the AS-SIP – H.323 Gateway and the SBC. Signaling and media lines in blue represent notional internal connectivity options.

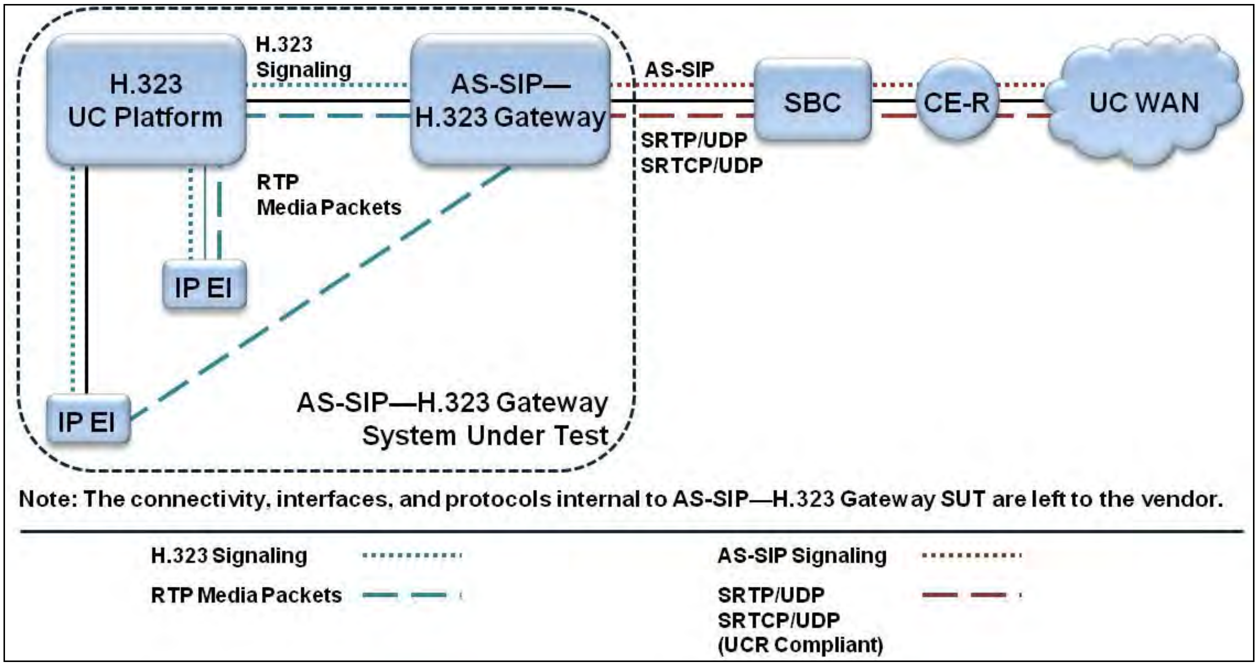


Figure 2.9-5. AS-SIP – H.323 Gateway Topology

The AS-SIP – H.323 Gateway maintains call count thresholds for voice sessions and for video sessions in order to perform Session Admission Control (SAC).

2.9.3.2 AS-SIP – H.323 Gateway Functional Reference Model

Figure 2.9-6, Functional Reference Model – AS-SIP – H.323 Gateway, shows the reference model for the AS-SIP – H.323 Gateway. The AS-SIP – H.323 Gateway consists of several SCS functions performed by the CCA, IWF (for signaling), and IWF (for media). These are connected via H.323 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.

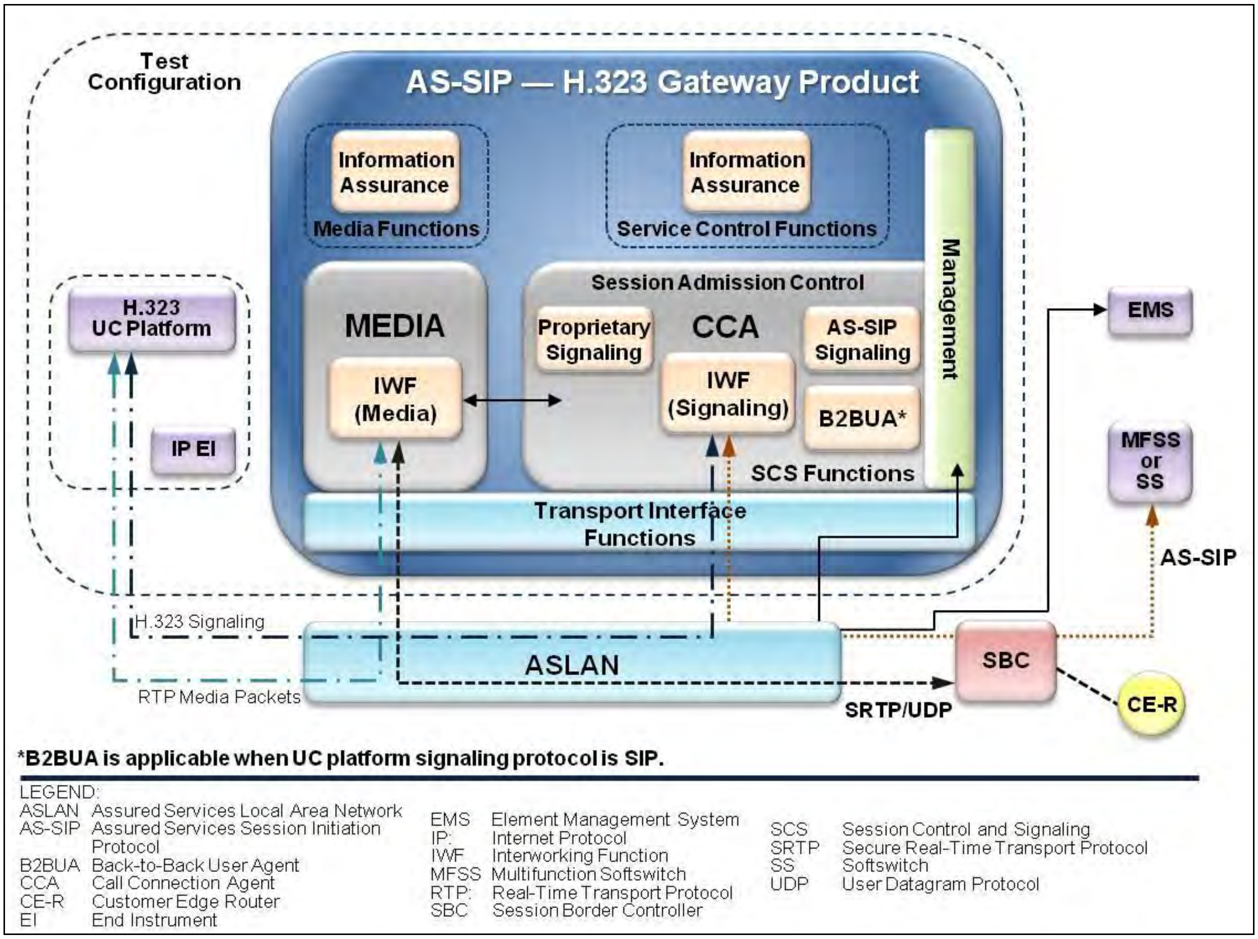

Test Configuration
AS-SIP — H.323 Gateway Product
Information Assurance
Media Functions
Information Assurance
Service Control Functions
Management
H.323 UC Platform
IP EI
MEDIA
IWF (Media)
Session Admission Control
Proprietary Signaling
CCA
AS-SIP Signaling
IWF (Signaling)
B2BUA*
SCS Functions
Transport Interface Functions
EMS
MFSS or SS
AS-SIP
H.323 Signaling
ASLAN
SBC
RTP Media Packets
SRTP/UDP
CE-R
*B2BUA is applicable when UC platform signaling protocol is SIP.
LEGEND:
ASLAN Assured Services Local Area Network
AS-SIP Assured Services Session Initiation Protocol
B2BUA Back-to-Back User Agent
CCA Call Connection Agent
CE-R Customer Edge Router
EI End Instrument
EMS Element Management System
IP: Internet Protocol
IWF Interworking Function
MFSS Multifunction Softswitch
RTP: Real-Time Transport Protocol
SBC Session Border Controller
SCS Session Control and Signaling
SRTP Secure Real-Time Transport Protocol
SS Softswitch
UDP User Datagram Protocol

Figure 2.9-6. Functional Reference Model – AS-SIP – H.323 Gateway

2.9.3.3 Summary of AS-SIP – H.323 Gateway Functions and Features

The AS-SIP – H.323 Gateway provides interworking functions for the signaling and bearer planes (see Table 2.9-3, Summary of AS-SIP – H.323 Gateway Functions).

Table 2.9-3. Summary of AS-SIP – H.323 Gateway Functions

FUNCTION	DESCRIPTION
SCS	Verifies call request is consistent with SAC: Signaling interworking (H.323 to AS-SIP; AS-SIP to H.323)
SAC	Maintains call thresholds. Maintains active session state knowledge (local access bandwidth used and available, direction, session type: voice, video).
Media IWF	Converts H.323 media packets to UCR-compliant IP/UDP/SRTP packets. Converts UCR compliant IP/UDP/SRTP packets to H.323 media packets.
NM	Provides traffic call information to, and responds to traffic flow control commands from, an EMS.
LEGEND AS-SIP: Assured Services Session Initiation Protocol SAC: Session Admission Control	

FUNCTION	DESCRIPTION
EMS: Element Management System	SCS: Session Control and Signaling
IP: Internet Protocol	SRTP: Secure Real-time Transport Protocol
IWF: Interworking Function	UCR: Unified Capabilities Requirements
NM: Network Management	UDP: User Datagram Protocol

2.9.3.4 AS-SIP – H.323 Gateway CCA Function Overview

The CCA is part of the SCS functions and includes the following:

- AS-SIP signaling protocol implementation for voice and video calls.
- H.323 signaling protocol implementation for voice and video calls (where signaling protocol implementation refers to the signaling being used by the H.323 UC signaling platform).
- Control of sessions within the AS-SIP – H.323 Gateway including the following:
  - H.323 sessions between the AS-SIP – H.323 Gateway and the H.323 UC signaling platform.
  - AS-SIP sessions between the AS-SIP – H.323 Gateway and the serving SS.
- Support for interactions with other network appliance functions including the following:
  - Admission control.
  - Information Assurance.
  - Media interworking.
  - Appliance Management functions.

Figure 2.9-7, CCA Relationships, illustrates the relationship between the CCA and other functional components.

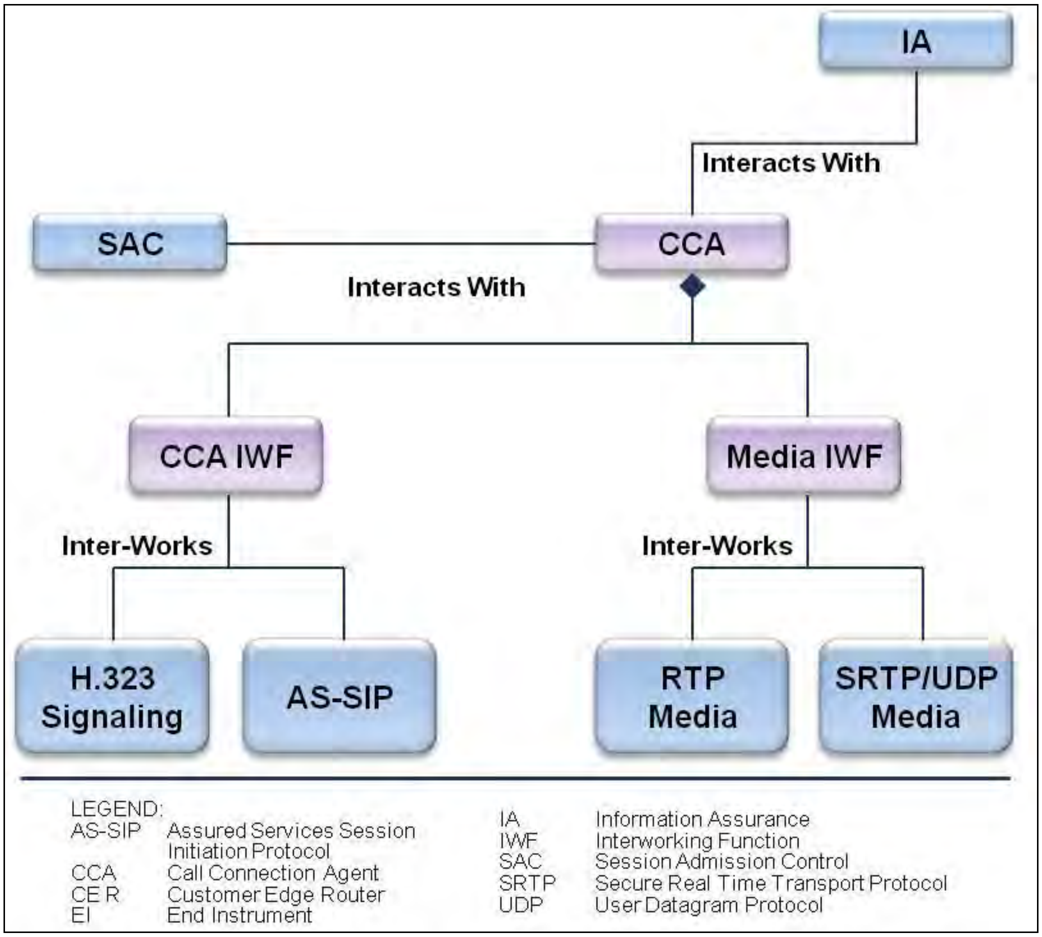

IA
Interacts With
SAC
CCA
Interacts With
CCA IWF
Media IWF
Inter-Works
Inter-Works
H.323 Signaling
AS-SIP
RTP Media
SRTP/UDP Media
LEGEND:
AS-SIP Assured Services Session Initiation Protocol
CCA Call Connection Agent
CE R Customer Edge Router
EI End Instrument
IA Information Assurance
IWF Interworking Function
SAC Session Admission Control
SRTP Secure Real Time Transport Protocol
UDP User Datagram Protocol

Figure 2.9-7. CCA Relationships

The role of the AS-SIP – H.323 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 – H.323 Gateway on behalf of the H.323 UC signaling platform. The signaling protocol used by the H.323 UC signaling platform is by definition an IP signaling protocol that is not compliant with the UCR AS-SIP requirements.

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.

2.10 NETWORK-LEVEL SOFTSWITCH

The network-level Softswitch (SS) is a backbone device that provides long-haul signaling between local service enclaves and acts as an AS-SIP B2BUA within the UC framework. It provides the equivalent functionality of a commercial SS.

A SS may serve EIs directly, if configured with an optional internal SC.

2.10.1 SS Functional Reference Model, Assumptions and Signaling Interfaces

Figure 2.10-1 shows the reference model for the SS:

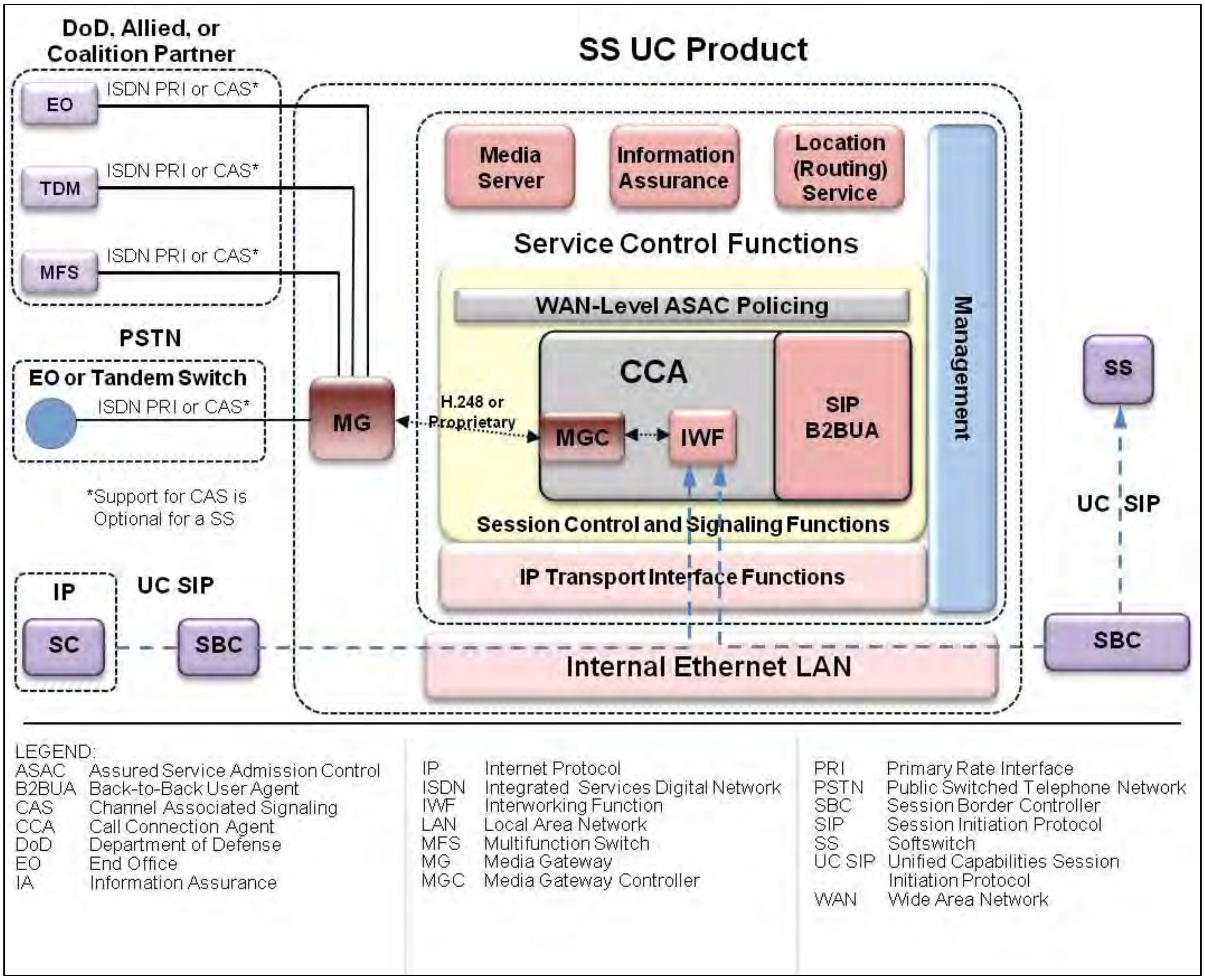

DoD, Allied, or Coalition Partner
SS UC Product
EO
ISDN PRI or CAS*
TDM
ISDN PRI or CAS*
MFS
ISDN PRI or CAS*
Media Server
Information Assurance
Location (Routing) Service
Service Control Functions
WAN-Level ASAC Policing
CCA
SIP B2BUA
Management
PSTN
EO or Tandem Switch
ISDN PRI or CAS*
MG
H.248 or Proprietary
MGC
IWF
SS
UC SIP
*Support for CAS is Optional for a SS
Session Control and Signaling Functions
IP Transport Interface Functions
IP
SC
UC SIP
SBC
Internal Ethernet LAN
SBC
LEGEND:
ASAC Assured Service Admission Control
B2BUA Back-to-Back User Agent
CAS Channel Associated Signaling
CCA Call Connection Agent
DoD Department of Defense
EO End Office
IA Information Assurance
IP Internet Protocol
ISDN Integrated Services Digital Network
IWF Interworking Function
LAN Local Area Network
MFS Multifunction Switch
MG Media Gateway
MGC Media Gateway Controller
PRI Primary Rate Interface
PSTN Public Switched Telephone Network
SBC Session Border Controller
SIP Session Initiation Protocol
SS Softswitch
UC SIP Unified Capabilities Session Initiation Protocol
WAN Wide Area Network

Figure 2.10-1. Functional Reference Model – SS

2.10.1.1 Assumptions – SS

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

1. External connections from an SS product are as follows:
   a. Connections to other IP-based products (e.g., SCs or other SSs) use AS-SIP signaling.
   b. Connections to TDM-based products (e.g., Multifunction Switch [MFS], EO, PBX, PSTN) use ISDN PRI or CAS.

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

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

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

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

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

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

   c. Support for CAS trunks is optional for the MG in the SS.

4. Figure 2.10-1, Functional Reference Model – SS, shows the SS supporting a single MG on a single ASLAN. A single SS also can support multiple MGs on multiple ASLANs, where those ASLANs are interconnected to form a Metropolitan Area Network (MAN) or Community of Interest Network (COIN). In this arrangement, it is expected that the set of ASLANs forming the MAN or COIN can meet the single-ASLAN performance requirements in Section 7, Network Edge Infrastructure. In this case, the SS supports sessions between an MG on one ASLAN and a PEI, AEI, MG, or SBC on another ASLAN, as long as both ASLANs are part of the same MAN or COIN.

   Another way of stating this is that a single SS is able to support MGs at multiple physical locations. In some voice deployments, an SS 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 SS supports MGs at multiple locations over MAN or COIN infrastructures that meet the ASLAN performance requirements in the UCR.

5. The SS Location Service (SSLS) functionality provides the CCA with information on call routing and called address translation for calls that are directed outside of the SS (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 maintained by the SSLS to:

   a. Route outgoing calls from SS EIs, if any, to other SSs and SCs, and

   b. Route incoming calls from SCs and other SSs to other SCs and other SSs.

However, the SS still uses the routing information stored in its SCLS to route internal calls, if any, from one SS PEI or AEI to another; to route internal calls from an SS PEI or AEI to an SS MG (and vice versa); and to route incoming AS-SIP calls from another SS or SC to local SS PEIs or AEIs.

6. The SS interactions with its SBC are different from the SC interactions with its SBCs.
   a. In the SC case, the SBC controls signaling streams between an SC connected to an ASLAN and an SS where its separate ASLAN is connected to the DISN WAN. In this case, the SBC also controls media streams between SC PEIs/AEIs and MGs connected to the ASLAN, and PEIs/AEIs and MGs on other SCs where separate ASLANs are connected to the DISN WAN. The SC accesses the DISN WAN via the SC SBC and an associated Provider Edge (PE) Router on the DISN WAN. As a result, it is possible for an SC MG to direct a VoIP media stream (interworked from a TDM media stream from the TDM side of that MG) through an SBC to the DISN WAN, and through the DISN WAN to a remote PEI, AEI, or MG.
   b. In the SS case, the SBC controls signaling streams between the SS where the SBC is connected to the DISN WAN and the SCs that it serves, which are connected to the DISN WAN via their own SBCs and PE Routers. The SS SBC also controls signaling streams between the SS with its SBC connected to the DISN WAN and other SSs that it communicates with (with their own SBCs connected to the DISN WAN). As a result, the SS SBC is responsible for boundary control for both SS-SC signaling and SS-SS signaling.
   c. If supported, an SC within an SS will serve a set of (SS-internal) SC PEIs/AEIs and MGs. These SC EIs and MGs will exchange media streams with EIs and MGs on other SCs located elsewhere on the DISN WAN. In this case, the SS SBC also controls these media streams between the (SS-internal) SC EIs and MGs connected to the SS ASLAN, and EIs and MGs on other SCs where separate ASLANs are connected to the DISN WAN.

2.10.1.2 Signaling Interfaces – SS

The SS supports the VoIP and Video signaling interfaces shown in Table 2.10-1, SS Support for VoIP and Video Signaling Interfaces.

Table 2.10-1. SS Support for VoIP and Video Signaling Interfaces

FUNCTIONAL COMPONENT	VOIP AND VIDEO SIGNALING INTERFACES	VOIP AND VIDEO SIGNALING PROTOCOLS
CCA	CCA (SS) – to – CCA (SC)	AS-SIP over IP
CCA	CCA (SS) – to – CCA (Other SS)	AS-SIP over IP
CCA	CCA (SS) – to – SS PEI	Proprietary VoIP over IP [Optional]
CCA	CCA (SS) – to – SS AEI	AS-SIP over IP [Optional]

FUNCTIONAL COMPONENT	VOIP AND VIDEO SIGNALING INTERFACES	VOIP AND VIDEO SIGNALING PROTOCOLS
CCA/MGC and MG	SS CCA (MGC) – to – SS MG	ITU-T H.248 over IP (Optional - used with ISDN PRI and CAS trunks)
CCA/MGC and MG	SS CCA (MGC) – to – SS MG	ISDN PRI over IP (Optional - North American National ISDN Version, used with ISDN PRI trunks only)
CCA/MGC and MG	SS CCA (MGC)– to – SS MG	Proprietary Supplier Protocols (used with ISDN PRI and CAS trunks)

LEGEND

AEI: AS-SIP Voice End Instrument
AS-SIP: Assured Services Session Initiation Protocol
CAS: Channel Associated Signaling
CCA: Call Connection Agent
DoD: Department of Defense
IP: Internet Protocol
ISDN: Integrated Services Digital Network
ISUP: ISDN User Part

ITU-T: International Telecommunications Union – Telecommunication
MG: Media Gateway
MGC: Media Gateway Controller
PEI: Proprietary End Instrument
PRI: Primary Rate Interface

SC: Session Controller
SS: Softswitch
TCAP: Transaction Capabilities Application Part
VoIP: Voice over IP

2.11 CALL CONNECTION AGENT

2.11.1 Introduction

Session Controllers (SCs) and Softswitches (SSs) have a design that includes Session Control and Signaling (SCS) functions. These functions include both a Signaling Protocol IWF and a Media Gateway Controller function. The Call Connection Agent (CCA) described in this section is part of the SCS functions, and includes both the IWF and the MGC.

CCA responsibilities include the following:

1. Control of AS-SIP sessions within the network appliance, including:
   a. AS-SIP sessions from/to AEIs served by an SC or SS appliance.

   (NOTE: Proprietary protocol sessions from/to SC PEIs and SS PEIs are supported also.)

   b. AS-SIP sessions from/to SCs served by an SS appliance.
   c. AS-SIP sessions between SS appliances (where sessions span multiple SSs).
2. Support for the following PSTN and VoIP signaling protocols:
   a. AS-SIP.
   b. ISDN PRI (North American National ISDN version), including MLPP.
   c. PSTN CAS, for dual-tone multifrequency (DTMF) and multifrequency (MF) trunks (North American version).

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 the continental United States (CONUS).
    d. PSTN Global (i.e., outside CONUS [OCONUS]).
4. CCA support for interactions with other network appliance functions, including:
    a. Admission control.
    b. The following Service Control functions:
        (1) Media servers.
        (2) UFS.
        (3) Information Assurance.
        (4) Session Controller Location Service (SCLS).
    c. Appliance Management functions.
    d. Softswitch Location Service (SSLS).
    e. SBCs.
5. CCA support for voice calls and video calls.
6. CCA support for Voice and Video services features and capabilities.

The CCA is also part of the SCS functions in AS-SIP Gateways. Please see Sections 2.9.1, 2.9.2 and 2.9.3 for the specific CCA responsibilities in those appliances.

2.11.2 Functional Overview of the CCA

Figure 2.11-1, CCA Relationships With Functional Components, illustrates the relationship between the CCA and other functional components. As indicated in the figure, the IWF and MGC are contained within a CCA.

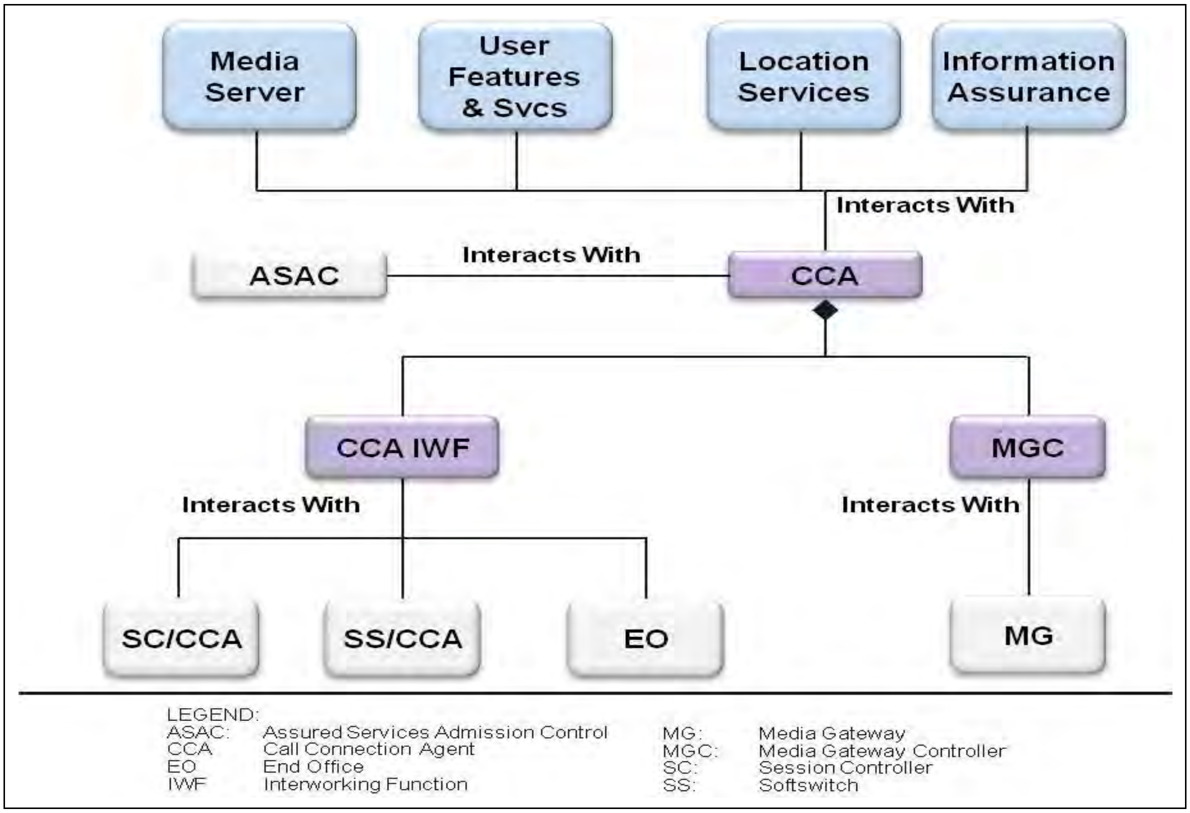


Figure 2.11-1. CCA Relationships With Functional Components

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/SC/SBC/SS 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 SBCs served by the SC, allowing PEIs, AEIs, MGs, and SBCs to register their SIP URIs (i.e., Addresses of Record) and current IP addresses with the CCA. The CCA is responsible for maintaining a SIP-URI-to-IP-address "binding" for each PEI, AEI, MG, and SBC that is active on the SC at any 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 SC PEI and AEI end users, on either a per-call basis or an all-calls basis, are controlled by the CCA.

In the current design for an SC, the CCA includes an IWF and an MGC, and the MGC controls all the TDM interfaces served by the MG (ISDN PRI trunks, and CAS trunks).

2.11.2.1 CCA IWF Component

The IWF has the following roles within the CCA:

- Support all the VoIP and TDM signaling protocols that the SC supports for EIs, MGs, and SBCs.
- Interwork all these various signaling protocols with one another.

2.11.2.2 CCA MGC Component

The MGC has the following roles within the CCA:

- Control all MGs within the SC or SS.
- Control all trunks (e.g., PRI, CAS) within each MG:
  - Support for DoD and PSTN ISDN trunks is required.
  - Support for CAS trunks is optional.
- Control all signaling and media streams on each trunk within each MG.
- Accept IP-encapsulated signaling streams from an MG, and return IP-encapsulated signaling streams to the MG accordingly.
- Within the SC, use either ITU-T Recommendation H.248 or a supplier-proprietary protocol to accomplish these controls.

  NOTE: The MGC and the MG that it controls are optional for deployable SCs.

2.11.3 CCA Interaction With Network Appliances and Functions

This section describes how the CCA interacts with network appliances and appliance functions, including the following:

- ASAC.
- Service Control functions.
- NM (FCAPS and audit logs).
- Transport Interface functions.
- SBC (not part of the SC, but part of the local Assured Services domain).

2.11.3.1 CCA Interactions With Transport Interface Functions

The Transport Interface functions in an appliance provide interface and connectivity functions with the ASLAN and its IP packet transport network. High-level requirements for these functions are outlined in this section. The detailed implementation methods for these requirements are left up to each vendor. Examples of Transport Interface functions include:

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

As an example, the CCA interacts with the SC 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 SBC over the ASLAN.

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

2.11.3.2 2CCA Interactions With the SBC

The SBC provides Session Border Control and firewall capabilities for the ASLAN, the PEIs/AEIs, and the IP-based components of the SC, including the CCA/IWF/MGC and the MGs.

The CCA interacts with the SBC by directing AS-SIP signaling packets to it (for signaling messages destined for an SS) and by accepting AS-SIP signaling packets from it (for signaling messages directed to the SC from an SS).

The SC EIs and MGs, which are controlled by the CCA, interact with the SBC by directing SRTP media streams to it (for call media destined for EIs and MGs on other SCs), and by accepting SRTP media streams from it (for call media directed to the SC PEIs/AEIs and MGs from EIs and MGs on other SCs).

The AS-SIP signaling packets exchanged between the SC and an SS must pass through the SBC. The SRTP media streams exchanged between SC EIs /MGs and EIs/ MGs on other SCs must also pass through the SBC.

The CCA in the SS and SC needs to interact with AS-SIP functions in the SBC, which

- Mediates AS-SIP signaling between an SC and an SS, and between two SSs.

- Supports commercial SBC functions, such as NAT and Network Address and Port Translation (NAPT).
- Supports IP firewall functions.

2.11.3.3 CCA Support for Admission Control

The CCA interacts with the ASAC component of the SC and SS to perform specific functions related to ASAC, such as counting internal, outgoing, and incoming calls; managing separate call budgets for VoIP and Video over IP calls; and providing preemption.

Requirements for ASAC are handled in two categories: CAC and ASAC. Call Admission Control 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 SC-Level ASAC (supported in the SC and the SS) and WAN-Level ASAC Policing (supported in the SS only). The SC and SS are responsible for maintaining the following:

- VoIP session budgets.
- VoIP session counts.
- VSU budgets.
- VSU counts.

2.11.3.4 CCA Support for User Features and Services

The User Features and Services (UFS) Server is responsible for providing features and services to VoIP and Video PEIs/AEIs on an SC or SS, where the CCA alone cannot provide the feature or service. 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 Forwarding, Call Transfer, 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, 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 a PEI that a CW call is available, and the UFS indicator that tells a PEI that there is a message waiting for that PEI.

The interface and protocols used to interconnect the CCA with the UFS Server are internal to the network appliance and, therefore, are supplier-specific.

2.11.3.5 CCA Support for Information Assurance

The Information Assurance function within the appliance ensures that end users, PEIs, AEIs, MGs, and SBCs that use the appliance are all properly authenticated and authorized by the appliance. The Information Assurance function ensures that Voice and Video signaling streams that traverse the appliance and its ASLAN are properly encrypted.

The interface and protocols used to interconnect the CCA with the Information Assurance function are internal to the appliance and, therefore, are supplier specific.

2.11.3.6 CCA Interactions With Session Controller Location Service

The Session Controller Location Service (SCLS) provides information on called address translation in response to call routing queries from the CCA. The CCA sends call routing queries to the SCLS for both outgoing calls from appliance PEIs or AEIs and incoming calls to appliance PEIs or AEIs.

The CCA uses the information returned by the SCLS to route the following:

- Internal calls from one appliance PEI or AEI to another.
- Outgoing calls from an appliance PEI or AEI to another appliance (via an SBC), or to a TDM network (via an Appliance MG).
- Incoming calls from another appliance (via an SBC), or from a TDM network (via an Appliance MG), to an SC PEI or AEI.

The interface and protocols used to interconnect the CCA with the SCLS are internal to the appliance and, therefore, are supplier specific.

2.11.3.7 CCA Interactions With Softswitch Location Service

Like the SCLS, the Softswitch Location Service (SSLS) provides information on call routing in response to call-routing queries from the CCA. The CCA sends call-routing queries to the SSLS for calls where the CCA determines that the call's destination lies outside the SS.

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 Numbering Plan Area [NPA]-NXX in the DoD dialing plan) pointed to a location in the DoD network outside the SS. The CCA may make this determination based on a previous call-routing response from the SS's SCLS that indicated, "This address is not assigned to any PEI, AEI, or MG on the SS."

As in the SCLS case, the query from the CCA to the SSLS 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 SSLS identifies either of the following:

- A remote IP address that points to the next appliance (i.e., an SC or an SS) that the call should be routed to.
- The local IP address of an SS MG trunk group that the call should be routed to. (This case applies when the MG TG connects to a TDM destination outside the SS that can be on the DoD TDM network, an allied or coalition partner TDM network, or on the PSTN (CONUS and Global)).

2.11.3.8 CCA Interactions With End Instrument(s)

The CCA in the SC, including an SC internal to an SS, needs to interact with VoIP PEIs and AEIs served by that SC. The VoIP interface between the PEI and the SC is left up to the network appliance supplier. The VoIP interface between the AEI and the SC is AS-SIP.

2.11.3.9 CCA Interactions With Service Control Functions

The interface and protocols used to interconnect the CCA with the media server are internal to the SC and SS and, therefore, supplier specific.

The Media Server function provides tones and announcements that the SC "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 SC 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 SC to the PEI or AEI that

mandate the "play" of the tones or announcements. (An example of this is the use of an SC 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 SC 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.

2.12 MEDIA GATEWAY

2.12.1 Introduction

This section describes the Media Gateway (MG) and Media Gateway Controller (MGC) functions in the SC and SS network appliances. These appliances have defined designs that include an MGC function and one or more MGs.

The scope of the MG requirements in UCR 2013 Section 2.18, Media Gateway, covers the following areas:

- Physical interfaces and protocols supported on the TDM side of the MG include the following:
  - ISDN PRI trunks: The TDM media (B channels) channels and the TDM signaling channels (D channels) both terminate on the MG.
  - CAS trunks: Both DTMF and MF; the TDM channel that carries both the media and the signaling terminates on the MG.
- VoIP interfaces and protocols supported on the IP side of the MG include the following:
  - Interface to the IP router network and the LAN (ASLAN, LANs internal to a UC product) that the network appliance is connected to.
  - VoIP protocol stacks supporting IP, IPSec, UDP, TCP, SCTP, and SRTP.

    - Secure VoIP media streams, packetized using IP, UDP, and SRTP, IAW Section 4, Information Assurance.
    - Secure VoIP signaling messages, packetized using IPSec, and UDP or TCP or SCTP, IAW, Section 4, Information Assurance:
        - H.248 signaling messages, for MGC control of ISDN PRI and CAS trunks, if the supplier supports ITU-T Recommendation H.248.
        - ISDN PRI signaling messages, for MGC control of ISDN PRI trunks.
- Support for the following VoIP codecs, at a minimum, on the IP side of the MG:
    - ITU-T Recommendation G.711 (uncompressed voice, both North American (μ-law and International A law)).
    - ITU-T Recommendation G.723.1.
    - ITU-T Recommendation G.729.
- Support for Fax over IP (FoIP) on the IP side of the MG.
- Support for Voiceband Modem over IP (MoIP) on the IP side of the MG. The following terms define "Modem over IP" traffic, as used in the UCR. The terms are listed here to clarify that SCIP over IP streams are a subset of all possible modem relay streams. In the UCR, 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.)
    - Modem over IP. The transport of modem data across an IP network, via either modem relay or modem passthrough techniques.
    - 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.
    - Voiceband Data (Modem Passthrough). A subset of MoIP in which modem signals are transmitted over a Voiceband Data channel in a packet network.
    - 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.
- 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, 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.
- Support for 64-Kbps unrestricted digital information (clear channel) ISDN over IP on the IP side of the MG.

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 2.12-1, MGC – MG Layered Interface, illustrates the relationship between the MGC, a component of the CCA, and a generic MG.

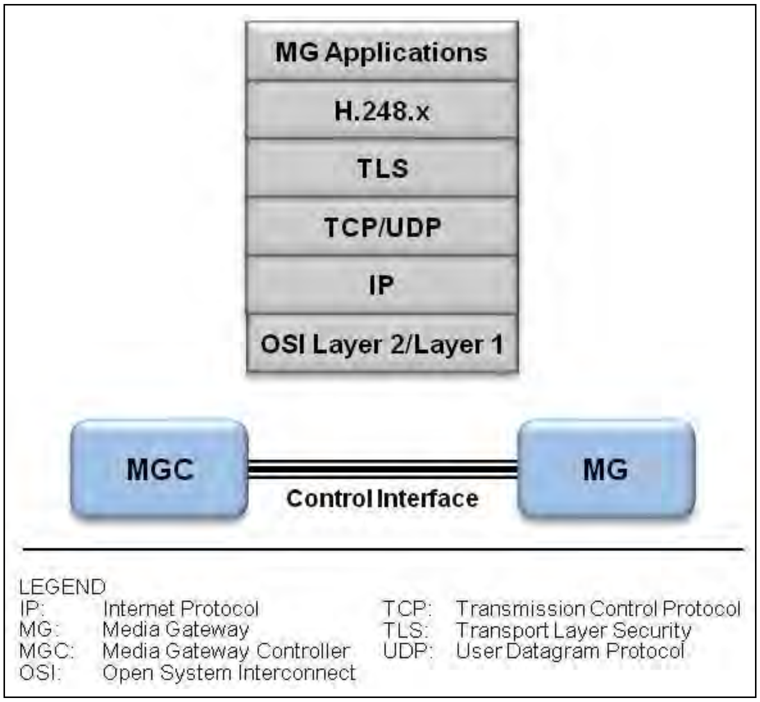

MG Applications
H.248.x
TLS
TCP/UDP
IP
OSI Layer 2/Layer 1
MGC
Control Interface
MG
LEGEND
IP: Internet Protocol
MG: Media Gateway
MGC: Media Gateway Controller
OSI: Open System Interconnect
TCP: Transmission Control Protocol
TLS: Transport Layer Security
UDP: User Datagram Protocol

Figure 2.12-1. MGC – MG Layered Interface

Figure 2.12-2, MG Trunk Function, illustrates the MG trunk function.

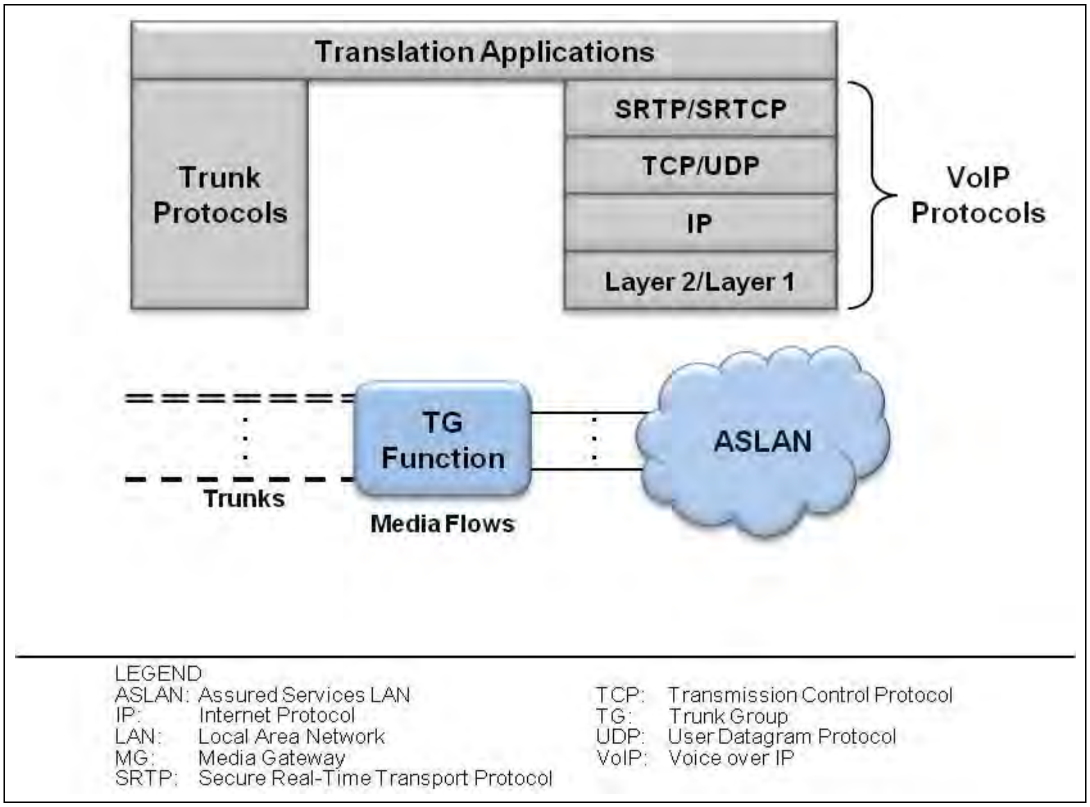


Figure 2.12-2. MG Trunk Function

2.12.2.1 Primary Trunk Functions and Interfaces

An MG may support a trunk-side interface to circuit-switched (CS) telephone networks. It terminates CS trunks in the CS 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.

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 Basic Rate Interface (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 2.12-3, MG Primary Access Functions and Interfaces).

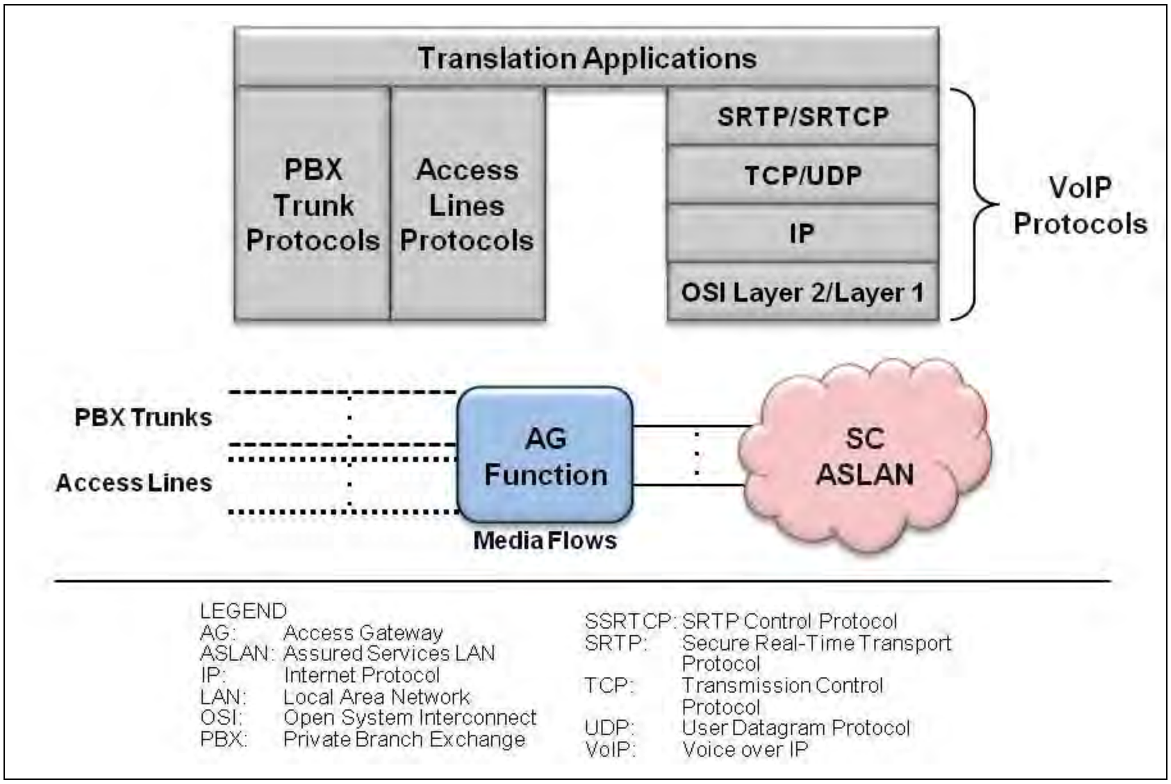


Figure 2.12-3. MG Primary Access Functions and Interfaces

2.12.2.3 MGC Functions

There are two options for the Gateway Control Protocol in the MGC and the MG:

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 SC and SS. (In some cases, this LAN may be the Internal LAN of the UC product, where the UC product also contains the SC or the SS. 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 SC and SS, which in turn is part of the SCS functions in these appliances. The MG function is a standalone appliance function in the SC and SS, and is not part of any other appliance function.

The role of the MGC within an SC and SS is to do the following:

- Control all MGs within the SC and SS.
- Control all trunks (e.g., PRI or CAS) within each MG.
- Control all signaling and media streams on each trunk within each MG.
- Accept IP-encapsulated signaling streams from an MG, and return IP-encapsulated signaling streams to the MG accordingly.

The MGC and the MG that it controls are optional for Deployable SCs.

2.12.3 Role of the MG in Appliances

The MG provides trunk termination for 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 SC supplier.

2.12.3.1 Role of the MG in the SC

Figure 2.8-1, Functional Reference Model – SC, illustrates the reference model for the SC, including the VoIP MG and MGC.

The roles of the MG within the SC are as follows:

- The MG terminates all TDM trunks that interconnect the SC with TDM networks, including the following:
  - DoD TDM networks (e.g., DSN, including EO and Tandem switches within the DSN), both in the United States and worldwide.
  - PSTNs, both in the United States and worldwide.
  - Allied and U.S. coalition partner TDM networks.
- The MG terminates all TDM trunks that interconnect the SC with TDM PBXs within the same DoD B/P/C/S.

  Media gateway support for TDM trunk groups is expected to be identical to the support for these trunk groups in DoD TDM PBXs, EOs, Tandem switches, and MFSs.
- The MG is responsible for terminating the TDM media trunks and signaling links on the TDM side, and for terminating the VoIP/FoIP/MoIP media streams and signaling streams on the VoIP side.
- 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.
- The MG supports interconnection of VoIP, FoIP, and MoIP media streams with the following SC functions and end-user devices:

  - The SC media server, which provides tones and announcements for SC calls and SC features.
  - Proprietary VoIP, FoIP, and MoIP EIs on the SC (when these EIs are supported on the SC).
  - Proprietary SIP EIs on the SC (when these EIs are supported on the SC).
  - Proprietary H.323 EIs on the SC (when these EIs are supported on the SC).
  - AS-SIP VoIP, FoIP, and MoIP AEIs on the SC.
- 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.
- 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.

NOTE: The MG and the MGC that controls the MG are considered “Optional – Deployable” for the SC. Some SC suppliers may include an MGC and MG in their Deployable SC product, and other SC suppliers may not. Those suppliers who do are to follow the MG requirements defined in the UCR.

2.12.3.1.1 SC MG VoIP Signaling Interfaces

The SC MG supports the VoIP signaling interfaces shown in Table 2.12-1, SC MG Support for VoIP Signaling Interfaces.

Table 2.12-1. SC 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 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 ISDN PRI and CAS trunks)
LEGEND		
CAS: Channel Associated Signaling		MG: Media Gateway
CCA: Call Connection Agent		MGC: Media Gateway Controller
DoD: Department of Defense		PRI: Primary Rate Interface

FUNCTIONAL COMPONENT	VOIP SIGNALING INTERFACES	VOIP SIGNALING PROTOCOLS
IP: Internet Protocol		VoIP: Voice over IP
ISDN: Integrated Services Digital Network		
ITU-T: International Telecommunications Union – Telecommunication		

2.12.3.2 Role of the MG in the SS

Figure 2.10-1, Functional Reference Model – SS, provides the functional reference model of the SS. The role of the MG in the SS is identical to the role of the MG in the SC (including the underlying assumptions, roles of the MG and MGC, interactions with other SC components, and VoIP signaling interfaces), with the following exceptions and extensions:

1. The MG in the SS assists the SS CCA in providing call denial treatments for CAC, and call preemption treatments for SC-Level ASAC and WAN-Level ASAC Policing. The SS supports SC-Level ASAC for admission control for calls to and from EIs that it serves directly. The SS also supports WAN-Level ASAC Policing for admission control for calls to and from SCs that it serves directly.
2. The MG in the SS supports ISDN PRI and, optionally, CAS trunks.

   NOTE: When an SC is included within a SS, it will serve a set of (SS-internal) SC EIs and MGs. These SC EIs and MGs will exchange media streams with EIs and MGs on other SCs located elsewhere on the DISN WAN. In addition, the SS SBC controls these media streams between the (SS-internal) SC EIs and MGs connected to the SS ASLAN, and EIs and MGs on other SCs, where separate ASLANs are connected to the DISN WAN.

2.12.3.2.1 SS MG VoIP Signaling Interfaces

The SS MG supports the VoIP signaling interfaces shown in Table 2.12-2, SS MG Support for VoIP Signaling Interfaces.

Table 2.12-2. SS MG Support for VoIP Signaling Interfaces

FUNCTIONAL COMPONENT	VOIP AND VIDEO SIGNALING INTERFACES	VOIP AND VIDEO SIGNALING PROTOCOLS
MG and MGC	SS MG – to – SS MGC	ITU-T H.248 over IP (used with ISDN PRI and CAS trunks)
MG and MGC	SS MG – to – SS MGC	ISDN PRI over IP (North American National ISDN Version, used with ISDN PRI trunks only)
MG and MGC	SS MG – to – SS MGC	Proprietary Supplier Protocols

FUNCTIONAL COMPONENT	VOIP AND VIDEO SIGNALING INTERFACES	VOIP AND VIDEO SIGNALING PROTOCOLS
LEGEND		
DoD: Department of Defense		MGC: MG Controller
IP: Internet Protocol		PRI: Primary Rate Interface
ISDN: Integrated Services Digital Network		SS: Softswitch
ITU-T: International Telecommunications Union – Telecommunication		
MG: Media Gateway		VoIP: Voice over IP

2.12.4 MG Interaction With NES and Functions

The MG is responsible for interacting with elements and functions of the SC and SS to support end-user calls, end-user features, and other operational capabilities needed by the DoD users. These other elements include the following:

- ASAC.
- Service Control functions (Information Assurance and media server).
- Management (FCAPS and audit logs).
- Transport Interface functions.
- SBC.

2.12.4.1 MG Support for ASAC

The MG interacts with the CCA, which in turn interacts with the ASAC component of the SC and SS to perform specific functions related to ASAC, such as providing denial treatments for calls that are denied admission to the SC and/or SS, 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: SC-Level ASAC, which is supported in the SC and the SS, and WAN-Level ASAC Policing, which is supported in the SS 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.

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 that treatment.

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.

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 UCR Section 4, Information Assurance.

The Information Assurance function within the appliance ensures that end users, PEIs, AEIs, MGs, and SBCs that interact with the appliance are all properly authenticated by the appliance. The Information Assurance function also ensures that VoIP signaling streams and media streams that traverse the appliance and its ASLAN are properly encrypted, using SIP/TLS and SRTP, respectively.

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 SC (NOTE: These functions may or may not use Information Assurance, depending on the internal design of the SC.):
   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.

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 SC end users (e.g., VoIP or video EIs).

The interface and protocols used to interconnect the MG with the media server are internal to the appliance and are, therefore, supplier-specific.

2.12.4.4 Interactions With IP Transport Interface Functions

The Transport Interface functions in the SC provide interface and connectivity functions with the ASLAN and its IP packet transport network. Examples of Transport Interface functions include the following:

- 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 SBC (and through the SBC to remote PEIs or AEIs and MGs served by other SCs and SSs) over the ASLAN. The following elements are all IP endpoints on the ASLAN:

- Each PEI or AEI served by the SC.
- The MG itself.
- Any other MGs that are served by the SC (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 SBC.

As an example, the MG interacts with the SC 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 SC Transport Interface functions when it uses IP, UDP, and the native ASLAN protocols to route SRTP media streams to and from EIs, other SC MGs, and the SBC over the ASLAN.

2.12.4.5 MG-SBC Interaction

The SBC provides Session Border Control and firewall capabilities for the ASLAN, the PEIs, AEIs, and the IP-based components of the SC, including the CCA, and its IWF and MGC, and the MGs.

The MG interacts with the SBC by sending SRTP media streams to it (for call media destined for a PEI, AEI, or MG that is served by another appliance outside the SC), or by accepting SRTP media streams from it (for call media arriving from a PEI, AEI, or MG that is served by another appliance outside the SC).

The SRTP media streams exchanged between the SC MG and a remote PEI, AEI, or MG must pass through the SBC. The SBC modifies these SRTP media streams by doing NAT/NAPT on them.

The VoIP MG in the SS or SC needs to interact with VoIP Media Transfer functions in the SBC. The SBC does the following:

- Transfers media streams between the PEIs or AEIs and MGs on the appliance, and PEIs or AEIs and MGs on remote appliances, located elsewhere on the DISN WAN.
- Supports commercial SBC functions, such as NAT and NAPT.
- Supports IP firewall functions.

2.12.4.6 MG Support for Appliance Management Functions

The Management function in the SBC, SC, and SS supports functions for SBC/SC/SS FCAPS management and audit logs.

The MG interacts with the Appliance Management function by doing the following:

- Making changes to its configuration and to its trunks' configuration in response to commands from the Management function that request these changes.
- Returning information to the Management function on its FCAPS in response to commands from the Management function that request this information.
- Sending information to the Management function on a periodic basis (e.g., on a set schedule), keeping the Management function up-to-date on MG activity. An example of this update would be a periodic transfer of trunk media error logs from the MG to the Management function so that the Management function could either store the records locally or transfer them to a remote NMS for remote storage and processing.

2.12.4.7 Interactions With VoIP EIs

The MG in the SS or SC needs to interact with VoIP EIs served by that SS or SC, and with VoIP EIs served by other SSs or SCs. The VoIP signaling interface between the PEI and the SS or SC is left up to the network appliance supplier. The VoIP signaling interface between the AEI and the SS or SC is AS-SIP.

2.12.5 MG and Echo Cancellation

The MG supports Echo Cancellation, consistent with commercial VoIP network practices.

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 because of 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.

2.12.5.1 Echo Control Design

An example MG echo control design is illustrated in Figure 2.12-4, Example IP Network Echo Control Design.

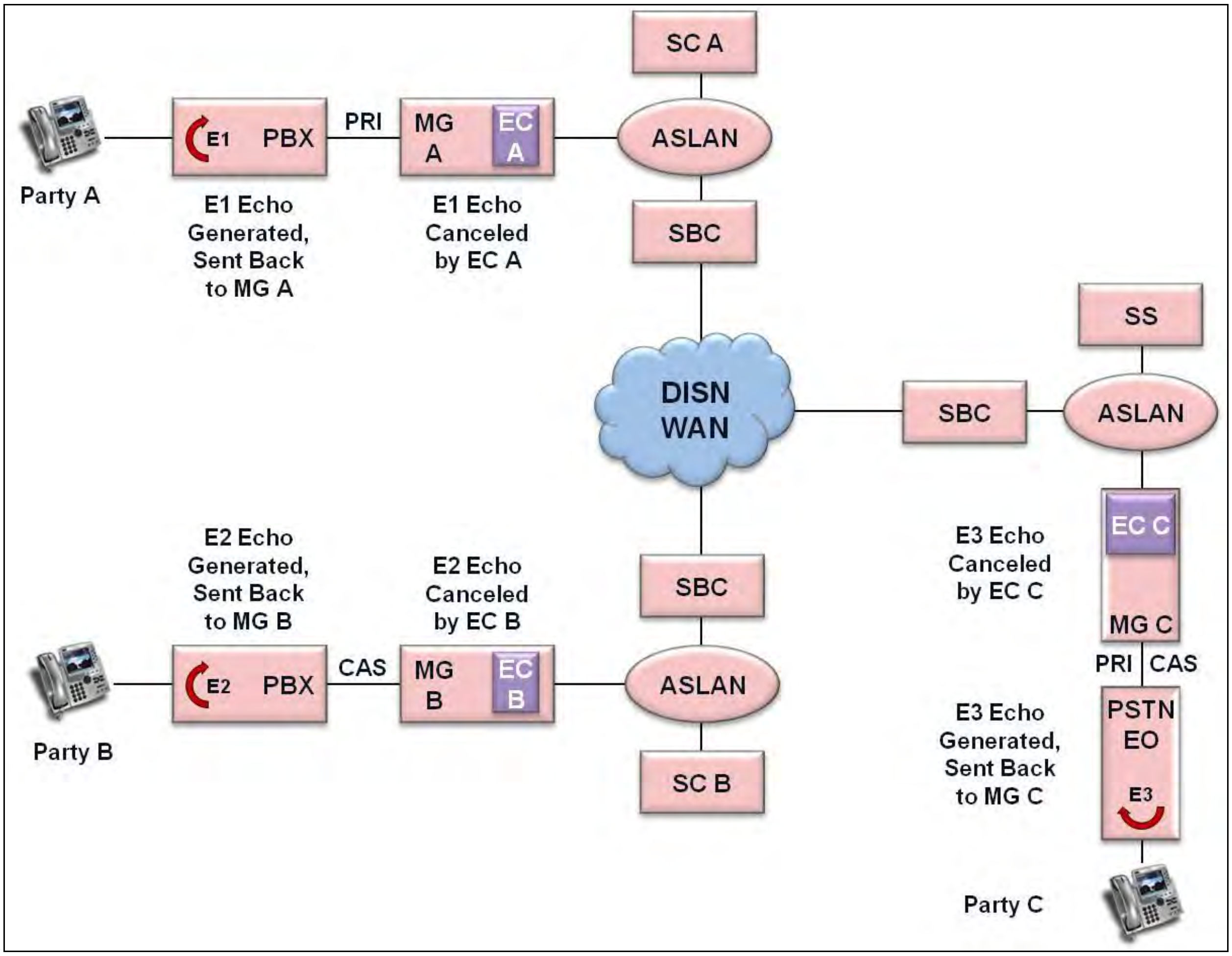


Figure 2.12-4. Example IP Network Echo Control Design

The EC function in MG A (controlled by SC 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 SC 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).

In addition, the EC function in MG C (controlled by the SS) 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).

The echo path capacity of an EC is the maximum echo path delay for which the device is designed to operate.

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.

2.12.6 MG and Synchronization

The use of digital switching systems and UC MGs directly interconnected with digital transmission facilities as an integral part of the DSN requires the use of techniques for synchronizing clock rates. The term synchronization refers to an arrangement for operating digital switching systems at a common (or uniform) clock rate where the data signal is accompanied by a phase-related clock. Improperly synchronized clock rates result in the loss of portions of the bit streams and a concomitant loss of information. The DISN Timing and Synchronization (T&S) subsystem uses Navigation Satellite Timing and Ranging (NAVSTAR) Global Positioning System (GPS) transmissions from which a precise frequency is derived. This precise frequency timing signal is phase related (referenced) to Universal Time Coordinated (UTC). The T&S subsystem frequency multiplier accepts precise frequency signals from a primary source or, in case of failure, switches to an alternate source provided by atomic clocks, e.g., cesium beam or rubidium, if available. The Clock Distribution System disseminates timing through the equipment hierarchy. The DSN switches and UC MGs also may receive system timing via digital transmission facilities to locations having direct access to (synchronized to) the timing sources already described.

2.12.7 MGC-MG CCA Functions

Per Section 2.12.2.2, CCA MGC Component, the role of the MGC within the CCA is to

- Control all MGs within the SC or SS.
- Control all trunks (PRI, CAS) within each MG:
- Control all signaling and media streams on each trunk within each MG.
- Accept IP-encapsulated signaling streams from an MG, and return IP-encapsulated signaling streams to the MG accordingly.
- Within the SC, use either ITU-T Recommendation H.248 or a supplier-proprietary protocol to accomplish these controls.

2.12.8 Remote Media Gateway Requirements

A Remote Media Gateway (MG) appliance is a media gateway that is geographically separated from the SC/SS media gateway controller (MGC) that controls it. The Remote MG may be controlled by an SC or a SS. An SC/SS MGC may control several MGs with some local to the MGC and some remote to the MGC. The Remote MG connects to its MGC via an IP

CAN/MAN/WAN. Implementing a remote MG architecture allows more architectural richness in the implementation of UC solutions:

1. Replacing existing TDM trunks between a TDM EO and its serving SS with IP connectivity, thus extending IP closer to the end point.
2. In the case of a large geographical serving area, you can retain the current TDM-based switches and serve them with a remote MG via an IP CAN/MAN/WAN from a single SC. This may be the case in Europe; e.g., Mannheim-Heidelberg area where today we have several EOs with their own TDM interfaces transitioning to IP trunking by employing multiple remote MGs and single regional SC.
3. In the case of regional enterprise solutions, the SC would be centrally located with the MGs distributed at the Military Department (MILDEP) locations to allow for local PSTN access.

The architecture of a remote MG application is shown in Figure 2.12-5, Remote MG Architecture Diagram.

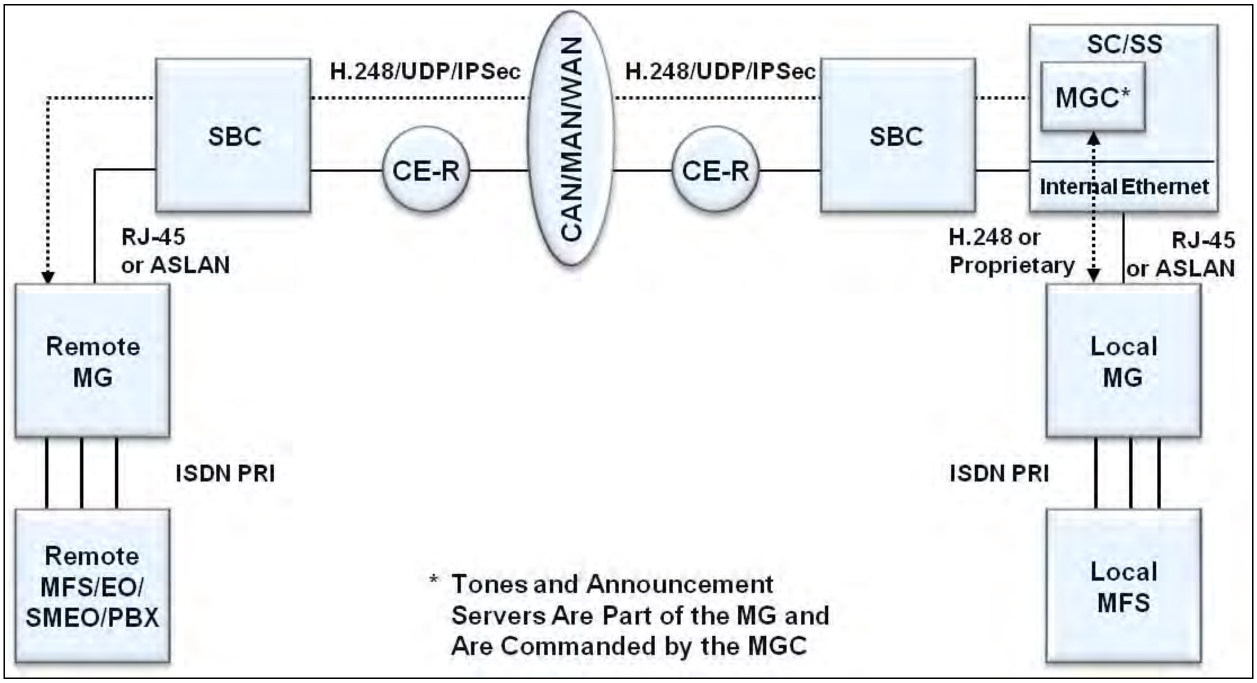


Figure 2.12-5. Remote MG Architecture Diagram

The protocol stack for Figure 2.12-5 is shown in Table 2.12-3.

Note that the H.248/UDP/IPSec signaling streams and the SRTP/IP media streams both flow through both SBCs (the SC SBC and the Remote MG SBC) in the above architecture.

Table 2.12-3. Protocol Stack

SIGNALING	MEDIA
H.248.1 with IPSec	Codec
UDP	SRTP
IP	IP
OSI Layer 2/Layer 1	OSI Layer 2/Layer 1
LEGEND	
IP: Internet Protocol	SRTP: Secure Real-Time Transport Protocol
IPSec: Internet Protocol Security	UDP: User Datagram Protocol
OSI: Open System Interconnect	

2.13 SESSION BORDER CONTROLLER

The Session Border Controller (SBC), formerly known as the Edge Boundary Controller (EBC), acts as a firewall for voice and video traffic at the ASLAN enclave boundary. All outgoing VVoIP media packets, that are marked for Assured Services and destined for points outside of the ASLAN, must be delivered to this SBC. All incoming VVoIP media packets on the WAN Access Circuit serving the ASLAN, that are marked for Assured Services and destined for points within the ASLAN, must be delivered to the SBC.

The SBC is a stateful, AS-SIP-aware application firewall that provides Intrusion Detection System/Intrusion Prevention System (IDS/IPS), Network Address Translation (NAT), and port pinholes for individual voice and video sessions. The SBC acts as AS-SIP Back-to-Back User Agent (B2BUA).

2.14 WORLDWIDE NUMBERING AND DIALING PLAN

The DSN Worldwide Numbering and Dialing Plan is used as the addressing schema within the current DSN and its migration into the SIP environment.

The DSN user dialing format is illustrated in Table 2.14-1, DSN User Dialing Format. The digits shown in parentheses may not be dialed by the DSN user on all calls. Note that a softkey or other method may be used to indicate that a call is Routine or Precedence in lieu of explicitly dialing 94 or 9P (where P = 0, 1, 2, or 3), respectively.

Table 2.14-1. 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.					

ACCESS DIGIT	PRECEDENCE OR SERVICE DIGIT	ROUTE CODE	AREA CODE	SWITCH CODE	LINE NUMBER
(N)	(P OR S)	(1X)	(KXX)	KXX	XXXX
• 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 following are highlights of the DSN Worldwide Numbering and Dialing Plan:

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 2.14-2, Examples of Internal DSN Numbers and Their Corresponding Global E.164 PSTN Telephone Numbers.

Table 2.14-2. 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 as follows:

      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 … 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 SC 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:

   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 (SC) providing the SIP resources. The Host field contains a Fully Qualified Domain Name (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 Domain Name Service (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 requirement in the UCR. Instead, UC support for DNS is conditional.

(3) Because we are addressing hosts that can process telephone numbers (e.g., an SC), we will use a "telephone-subscriber" field to populate the "user" field. [RFC 3966] This is accomplished by using the tel URI.

b. The tel URI specifies the telephone number as an identifier.

c. 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.

d. It can be fixed or wireless and address a fixed-wired, mobile, or nomadic terminal.

e. The terminal addressed can support any electronic communication service, including voice, data, and fax.

f. 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 SCs IAW 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 SC (patch.eur.uc.mil). In the near future, call requests will be forwarded (routed) based on the telephone number contained within the SIP request. Therefore, in the near future the 10 digit DSN number within the SIP URI will be used to route calls to their destination. The "phone-context=uc.mil" required by the SIP syntax is included strictly to indicate that the phone number is part of the UC network. In the long term future, the UC network may be enhanced to route calls based on FQDN within the SIP URI in addition to routing on the DSN number.

Table 2.14-3, 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 2.14-3. Mapping of DSN tel Numbers to SIP URIs

ALIAS TYPE	SIP URI
7-digit intradomain (SC enclave) call	sip:4305335;phone-context=uc.mil@patch.eur.uc.mil;user=phone
7-digit interdomain (SC enclave) call within same area code	sip:4801235;phone-context=uc.mil@rsx.eur.uc.mil;user=phone
10-digit interdomain (SC enclave) call to another area code	sip:3157261135;phone-context=uc.mil@ysm.pac.uc.mil;user=phone

2.14.1 Domain Directory

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.

Traditionally, the subscriber assignment information contained within telephone switching systems consisted of just the subscriber telephone number, line equipment assignment, and subscriber attributes 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 SC 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 SC 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 usually is 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 soft keys. 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 SC 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 SC, 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 SC-contained directory.

It is anticipated that long-range functionality should be provided so that the "telephone part" of the SC directory can be imported to an external "corporate" (e-mail) directory. 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 SC must have stored the subscriber directory information previously in an LDAP-based system as outlined in item 1f. 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 SC directory to an external "corporate" directory (and storing subscriber directory information in an LDAP-based format) applies to Fixed (Strategic) appliances only, and not to Tactical (Deployable) appliances. Requirements for SC directory exports for Tactical (Deployable) appliances are candidates for a future version of this document.

Table 2.14-4, White Pages Directory Data Elements, shows essential elements in the white pages directory portion of the SC subscriber database.

Table 2.14-4. 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

2.15 MANAGEMENT OF NETWORK APPLIANCES

Figure 2.15-1, 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 2.15-1.

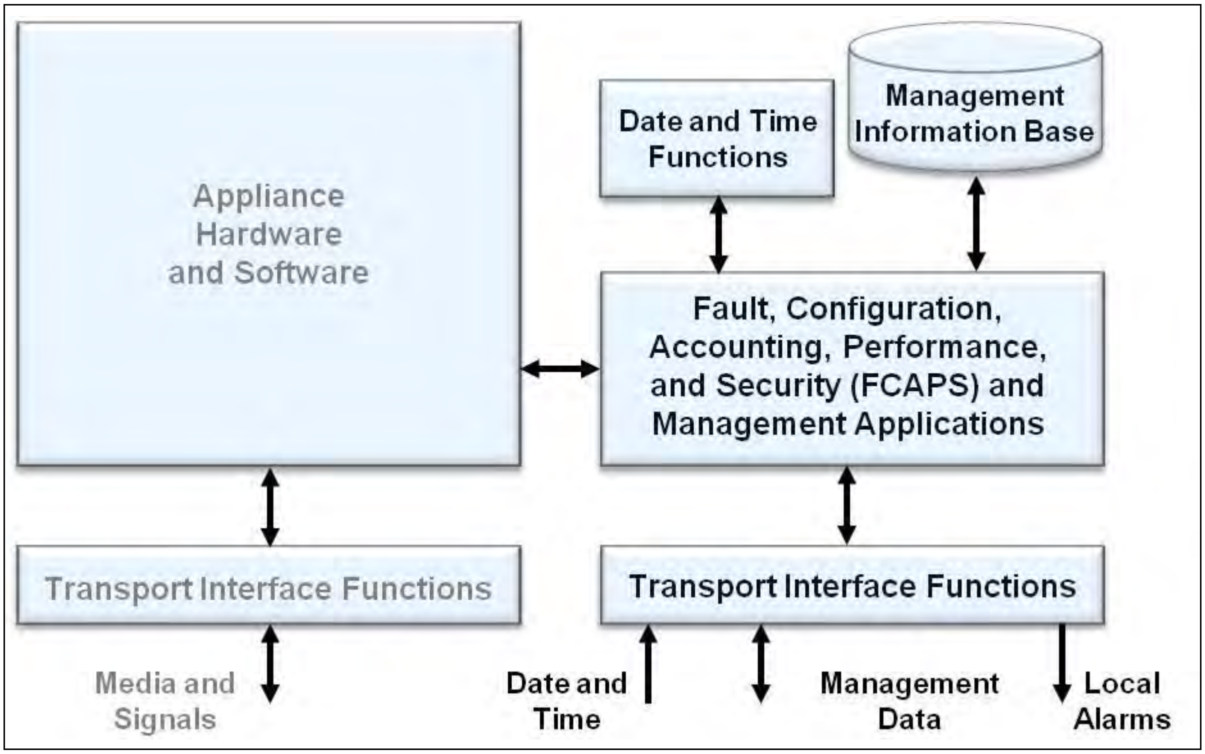

Appliance Hardware and Software
Date and Time Functions
Management Information Base
Fault, Configuration, Accounting, Performance, and Security (FCAPS) and Management Applications
Transport Interface Functions
Transport Interface Functions
Media and Signals
Date and Time
Management Data
Local Alarms

Figure 2.15-1. Network Appliance Management Model

2.15.1 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. One domain provides local, on-site craft person type support, typically referred to as Operations, Administration, Maintenance, and Performance (OAM&P), while the other domain provides 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 two domains must have simultaneous access to the UC products to effectively perform the DoD's end-to-end UC Management function. Where necessary, for clarification, the remote NM system will be referred to as the VVoIP Element Management System (EMS) and the local OAM&P system will be referred to as the Local EMS. See Figure 2.15-2, Relationship of UC Managements.

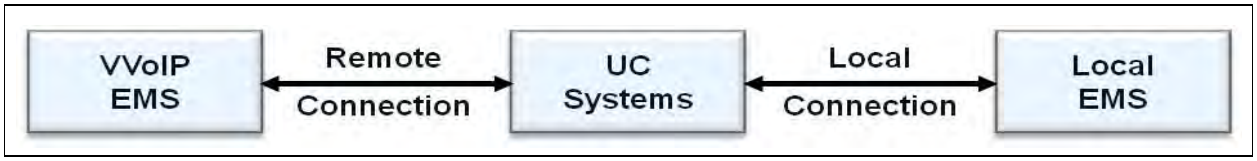


Figure 2.15-2. Relationship of UC Managements

2.15.2 General Management Approach

SCs and SSs must be capable of providing the following NM data to the VVoIP EMS:

- Alarm/log data.
- Performance data (e.g., traffic data).
- Accounting data (e.g., call detail recording).

SCs and SSs must allow the VVoIP EMS to have access to perform SC/SS datafill administration and network controls. Telcordia Technologies GR-740-CORE acts as guide for the interface between the network appliances (or components) and the external VVoIP EMS.

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.

RFC 1213 is also referenced for Management Information Base II (MIB-II) definitions.

In addition to the direction provided by the documents noted above, FCAPS, the International Organization for Standardization (ISO) Telecommunications Management Network model and framework, guides how UC network management is performed. The FCAPS model organizes network management into five functional areas: fault, configuration, accounting, performance, and security.

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.

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.

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.

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.

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 uses the security services of access control, confidentiality, integrity, availability, and non-repudiation as specified in UCR Section 4, Information Assurance.

2.15.3 Traffic Flow Control Overview

Performance management evaluates alarm and performance data and, to minimize the effect on network traffic caused by a network anomaly, implements traffic flow controls.

Within an IP network, the SC handles only call signaling, while the IP network connecting the two communicating end instruments handles the bearer stream. The SC 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 SC congestion occurs when the volume of AS-SIP messages exceeds the SC's capacity to process them. A particular vendor's SC solution may threshold and alarm on congestion, but a simpler approach may be monitoring the Central Processing Unit (CPU) utilization on the SC 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 SCs and their PEIs/AEIs from sending SIP (or proprietary protocol) messages to the overloaded SC. From the viewpoint of these other SCs, 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-R, NIPRNet AR traffic queues. For the ARs, 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. Place a code control on other SCs 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).
2. Change the call budget on the SC, with a corresponding change in the VVoIP queue bandwidths on the CE and PE Routers.
3. Reallocate the queue bandwidth on the CE and PE Routers.

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. The first two controls are in the Session Control domain and are described further below.

2.15.3.1 Destination Code Controls

Destination Code Control functionality is applied at the SC or SS 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 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 FLASH and FLASH OVERRIDE traffic to be passed to the minimized destination.

2.15.3.2 Call Budget Control

Setting the call budgets on the SS and SC involves setting the maximum number of calls (voice and video) that may be in service at one time within, and/or to and from a local service area (i.e., military installation).

See Section 2.4, ASAC Operation Overview, for more information on call budgets.

2.16 DYNAMIC ASAC

Dynamic ASAC (DASAC) enables an SC to admit, block, or preempt new voice and video sessions based on the bandwidth (bits/sec) required for the session and the link capacity available to support the session. Dynamic ASAC will augment the ASAC approach described earlier in Section 2.4, ASAC Operation Overview, in which SCs admit sessions based on a fixed session budget, either 110 Kbps for voice, or a multiple of 500 Kbps for video. The DASAC will be applied independently to voice and video sessions.

The method for ASAC described earlier could unnecessarily limit the number of sessions on capacity-constrained communications links, such as are common in Deployable (Tactical) networks and in some Fixed (Strategic) networks. For example, the current approach provisions 110 Kbps for each voice session, but some Deployable (Tactical) sessions only need 30 Kbps for good quality. The 110 Kbps number is based on the assumption that a voice session will use a G.711 codec and will be encapsulated in an IP packet in an Ethernet frame. These are reasonable conservative assumptions in a Fixed (Strategic) environment, but are not appropriate for a Deployable (Tactical) environment or a constrained Strategic environment, where lower bit rate codecs are used and link capacity is limited.

Dynamic ASAC will provide a more realistic estimate of capacity needed for a voice or video session and admit, block, or preempt sessions based on this estimate. However, parameter determination for DASAC can be quite complex. Some session packets might be tunneled over a communications link, others might not be; others might have header compression and some packets might be aggregated in a voice multiplexer also called a "voice mux." Engineering analysis and traffic analysis are required to determine the overheads on the SC Path (the path between cooperating SCs and SSs).

The SC and SS analyze each session initiation and session modification request to determine which overheads are appropriate, and the codec rate and packets per second (PPS) negotiated between the EIs involved in the session. This rate could change during a session; an example being a mid-session codec change; a factor that must be monitored by these devices if the change information is conveyed in AS-SIP messages. This may not be the case for all types of sessions; in some sessions the change information is conveyed in the bearer traffic. A bearer-based example would be a mid-session codec renegotiation via a modem protocol. In such cases, precautions during DASAC processing must be taken to ensure that there is sufficient capacity to accommodate the highest possible codec rate that could be renegotiated via the bearer mid-session. This could include using static, table driven parameters for session capacity, where these parameters represent the highest bits per second session capacity supported by the EI. Ideally, in lieu of the static table driven parameters, DASAC would process any bearer-based mid-session re-negotiation but such complexity is not currently required in the UCR.

The DASAC budget is based on metrics derived from the parameters shown in Table 2.16-1, EISC Estimation Parameters.

Table 2.16-1. EISC Estimation Parameters

#	PARAMETER	SOURCE	COMMENT
1	Codec Rate (bps)	Product extracts from SDP message; stored per codec class	Could change on a session-by-session basis per EI and within a session
2	Packet Rate (PPS)	Product extracts from information in SDP message	Could change on a session-by-session basis per EI and within a session. When the respective EIs support bearer-based mid-session renegotiation and if the product lacks the ability to process this bearer layer information, the PPS parameter needs to be set to the highest bits per second rate option available to the bearer-based mid-session renegotiation capability
3	Number of Sessions in Progress	Number of sessions in progress for this codec class. This includes sessions in both the setup and active states Running account kept by product	Initial value equals zero Incremented upon successful session connection Decremented upon successful session completion

#	PARAMETER	SOURCE	COMMENT
4	Tunnel Overhead Factor (bytes)	Pre-provisioned and entered into product	Indicates the number of overhead bytes that must be added to the IP packet size to account for encryption or other types of tunnels. If some sessions are tunneled and others are not, use the number of bytes associated with the largest overhead tunnel. Default is 100 bytes. Minimum 0 bytes. Maximum 512 bytes
5	IP Overhead (bytes)	Pre-provisioned and entered into product, includes IP, UDP, and RTP or SRTP overhead associated with packet flow over the target link	If IPv6, use 60 bytes If IPv4, use 40 bytes Default is 60 bytes
6	Layer 2 Overhead (bytes)	Pre-provisioned and entered into product	Sized according to layer 2 protocol used on target link—this parameter is the same for all packets in all codec classes. Default is 20 bytes
7	Safety Factor (%)	Pre-provisioned and entered into product	This parameter is used to provide a margin of error for the EISC calculation. Default is 10%
8	Voice Multiplexer (MUX) Overhead per Packet (bytes)	Pre-provisioned and entered into product	This parameter is used on a per packet basis if a voice MUX is used. There is no default value. Minimum 0 bytes. Maximum 512 bytes
9	Overhead per Voice MUX Sample (bytes)	Pre-provisioned and entered into product	This parameter is an overhead that is applied to each voice sample bundled in an output voice packet. There is no default value. Minimum 0 bytes. Maximum 512 bytes

Parameters 1 through 3 in Table 2.16-1, EISC Estimation Parameters, are dynamic and are calculated on a session-by-session basis. Parameters 4 through 9 are preloaded into the product based on traffic engineering analysis of the link.

The DASAC budget metrics are as follows:

- EI Session Capacity (EISC). The bandwidth required (in bps) for a session.
- Transmission Link Session Capacity (TSC). The capacity (bps) of the bottleneck link associated with the SC Path. The TSC is a pre-provisioned parameter entered for each SC Path link via NM commands. The TSC does not include an allocation for session signaling. Session signaling must be provisioned separately as part of traffic engineering for the bottleneck link on the path.
- Available Link Session Capacity (AVSC). The capacity (bps) currently available for sessions on the SC Path. The AVSC is calculated at each of the following events:
  - The session establishment AS-SIP dialog (specifically the AS-SIP message containing the SDP answer).
  - Mid-session re-INVITE dialog based on a mid-session codec change (specifically the AS-SIP message containing the new SDP answer to the new offer).
  - Session teardown (specifically based on SC detecting the AS-SIP 200 (OK) for the BYE).

The AVSC is calculated as follows:

> AVSC = TSC—the sum of EISCs for all sessions in progress and in the process of being established on the SC Path

Figure 2.16-1, AS-SIP Triggers for AVSC, illustrates the AS-SIP triggers for the AVSC calculations. For reasons of simplification, it assumes the EIs are AS-SIP enabled. It is also assumes that only one session is preempted to enable a new session to be accepted. This is not meant to preclude the preemption of multiple lower precedence setup and/or active sessions collectively, with a higher than or equal to, bits per second bearer rate, to allow a new, higher precedence session with a lower than or equal to, bits per second bearer rate to be admitted.

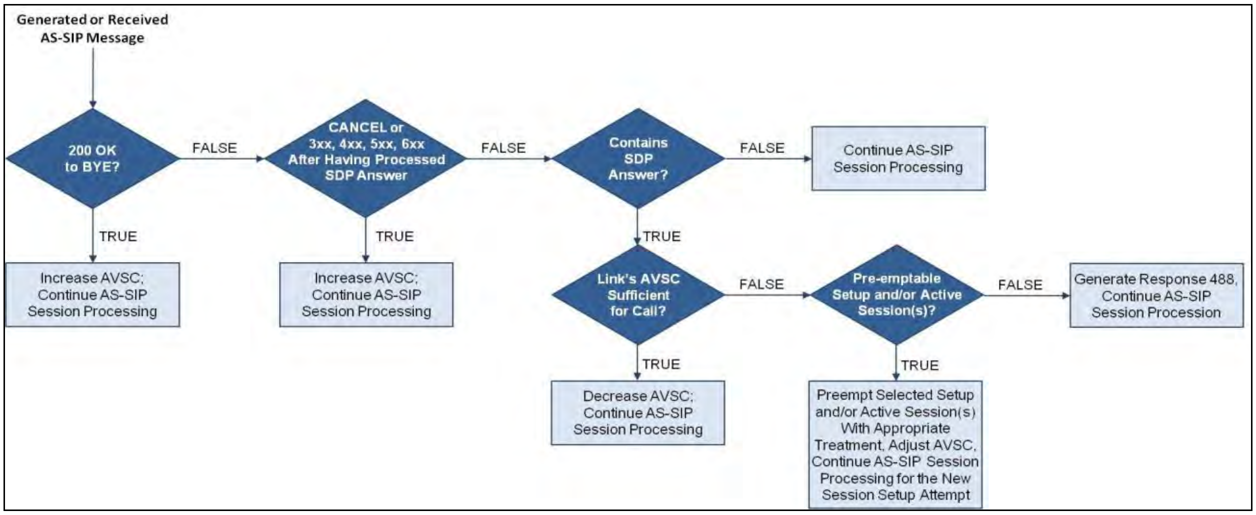

Generated or Received AS-SIP Message
200 OK to BYE?
FALSE
TRUE
Increase AVSC; Continue AS-SIP Session Processing
CANCEL or 3xx, 4xx, 5xx, 6xx After Having Processed SDP Answer
FALSE
TRUE
Increase AVSC; Continue AS-SIP Session Processing
Contains SDP Answer?
FALSE
Continue AS-SIP Session Processing
TRUE
Link's AVSC Sufficient for Call?
FALSE
TRUE
Decrease AVSC; Continue AS-SIP Session Processing
Pre-emptable Setup and/or Active Session(s)?
FALSE
Generate Response 488, Continue AS-SIP Session Procession
TRUE
Preempt Selected Setup and/or Active Session(s) With Appropriate Treatment, Adjust AVSC, Continue AS-SIP Session Processing for the New Session Setup Attempt

Figure 2.16-1. AS-SIP Triggers for AVSC

When a “200 OK” is received by the product, the bandwidth previously reserved for this session is released and thereby the AVSC is increased.

The “SDP Answer” message indicates the results of the codec negotiation between the EIs involved in the session request. The product processes the SDP Answer to determine whether there is sufficient capacity to support the new session. If so, the product will reserve bandwidth for the session and continue with AS-SIP session processing. If a Cancel or a 3xx, 4xx, 5xx, or 6xx message is received after the SDP Answer is processed but before the session setup is completed, the reserved capacity will be released and the AVSC increased accordingly.

If after receiving an SDP answer, the product determines if there is insufficient bandwidth for the new session. The product will review all sessions in progress, which includes those that are being set up (“setup sessions”) and those that are active, to determine if any have lower precedence than the new session. If there are none, the new session will be blocked. If lower precedence sessions do exist, the product will use the algorithm specified below or its equivalent to determine if the new session must be blocked or alternately admitted after the preemption of one or more setup and/or active sessions:

1. The product will determine the precedence level (P) of the new session attempt, where P is an integer between 1 and 5, representing increasing levels of precedence. The lowest precedence is Routine, with P =1. The precedence level of the new session attempt is P = N.

    a. If N=1, the new session attempt is blocked because a new session can only preempt a lower precedence session. The product will exit this algorithm.

    b. If N is >1, the product will determine if EISC(N), the capacity of the new session, is =< AVSC (where AVSC is the available capacity):

        (1) If so, the product will accept the new session, set AVSC to = AVSC - EISC(N) and exit this algorithm.

        (2) If not, the product will set P = 1. The product will continue to the next step.

2. The product will determine if there is any combination of setup sessions at precedence level P that, if preempted along with all sessions at a lower precedence, would provide sufficient capacity to support the new session.

    a. If so, the "optimum" combination of setup sessions will be preempted and the new session will be accepted. The optimum combination is the one that provides the required capacity with the least number of preempted setup sessions. The product will set AVSC = AVSC plus the capacity of all preempted calls (including all sessions at lower precedence levels) minus EISC(N). The product will exit this algorithm.

    b. If not, the product will determine if there is some optimum combination of one or more active sessions at P which, if preempted along with all setup sessions at P and all current sessions at a lower precedence than P, will provide sufficient capacity for the new session. The optimum combination is the one that provides the required capacity with the least number of preempted active sessions at P. The combination of all preemptable sessions is called the "identified sessions".

        (1) If there is such an optimum combination, all identified sessions will be preempted and the new session will be accepted. The product will set the new AVSC to equal AVSC plus the capacity of the identified sessions minus EISC(N). The product will exit this algorithm.

        (2) If not, the product will continue processing as described in the next step.

3. The product will increment P by 1.

    a. If P = N, the setup attempt will be blocked. The product will exit this algorithm.

    b. If P < N, the product will re-execute step 2.

If one or more preemptions occur and the new session is established, the resulting AVSC may be larger or smaller than before the preemption(s). If the preempting session's bandwidth requirement is less than that of the preempted session or sessions, the AVSC increases. If the preempting session's bandwidth requirement is more than that of the preempted session or sessions, the AVSC decreases.

If one or more preemptions occur and the new session is established, the resulting AVSC may be larger or smaller than before the preemption(s). If the preempting session's bandwidth requirement is less than that of the preempted session or sessions, the AVSC increases. If the preempting session's bandwidth requirement is more than that of the preempted session or sessions, the AVSC decreases.

2.16.1.1 Dynamic ASAC Calculation Examples

Examples of notional EISC calculation for voice sessions are given in Tables 2.16-2 through 2.16-5. The environment for Examples 1, 2, and 4 is shown in Figure 2.16-2, Notional System Architecture for Examples 1, 2, and 4. The environment for Example 3 is shown in Figure 2.16-3, Notional System Environment for Example 3 (Voice MUX with HAIPE Tunnel). The example environments consist of 20 VoIP phones, each of which can support G.711, G.729, G.723, and 2400 bps Enhanced Mixed Excitation Linear Production (MELPe) codecs. The TSC for the controlled link is 256 Kbps full duplex. The examples differ in the number and types of communication devices that are used to support UC traffic flow. Point-to-Point Protocol (PPP) is used as the layer 2 protocol. It provides a 7-byte layer 2 overhead per packet.

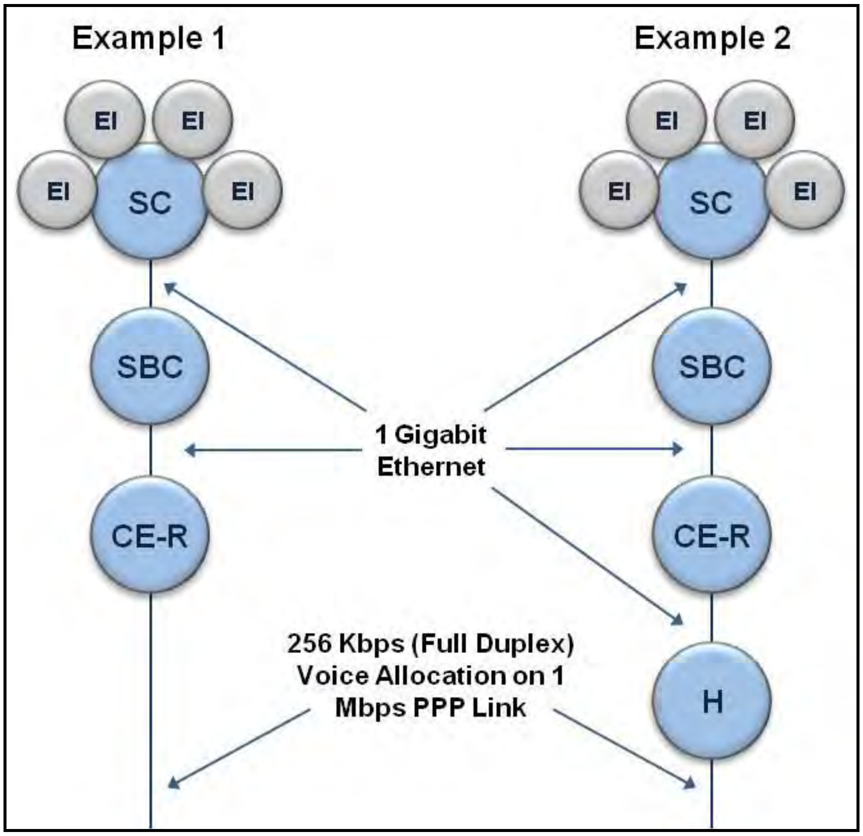


Figure 2.16-2. Notional System Architecture for Examples 1, 2, and 4

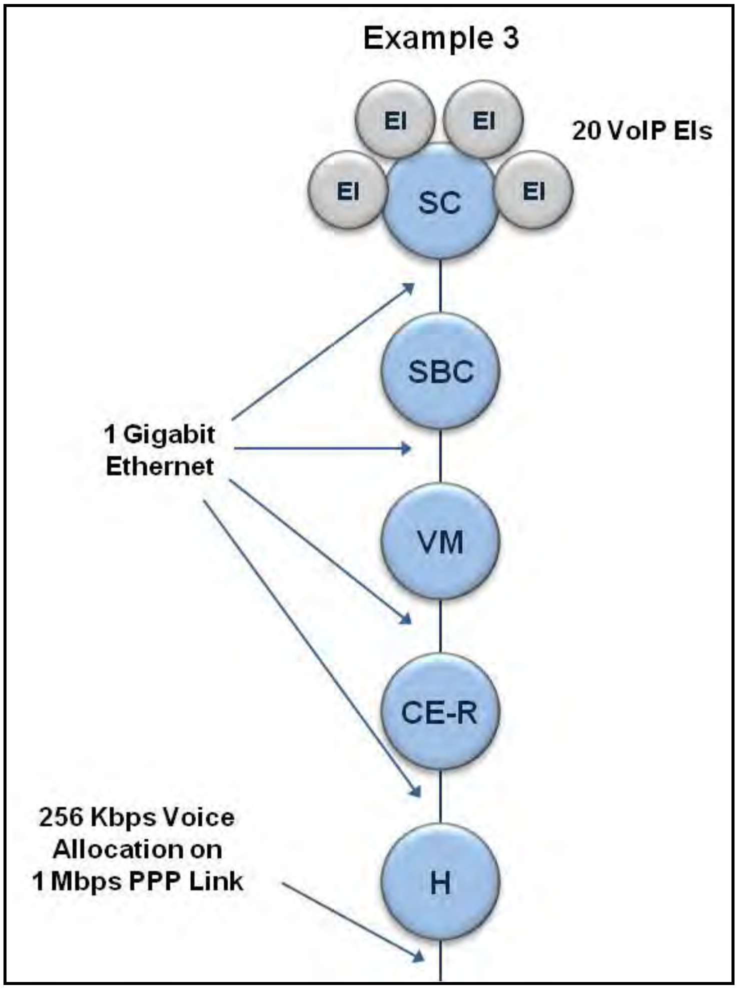


Figure 2.16-3. Notional System Environment for Example 3 (Voice MUX with HAIPE Tunnel)

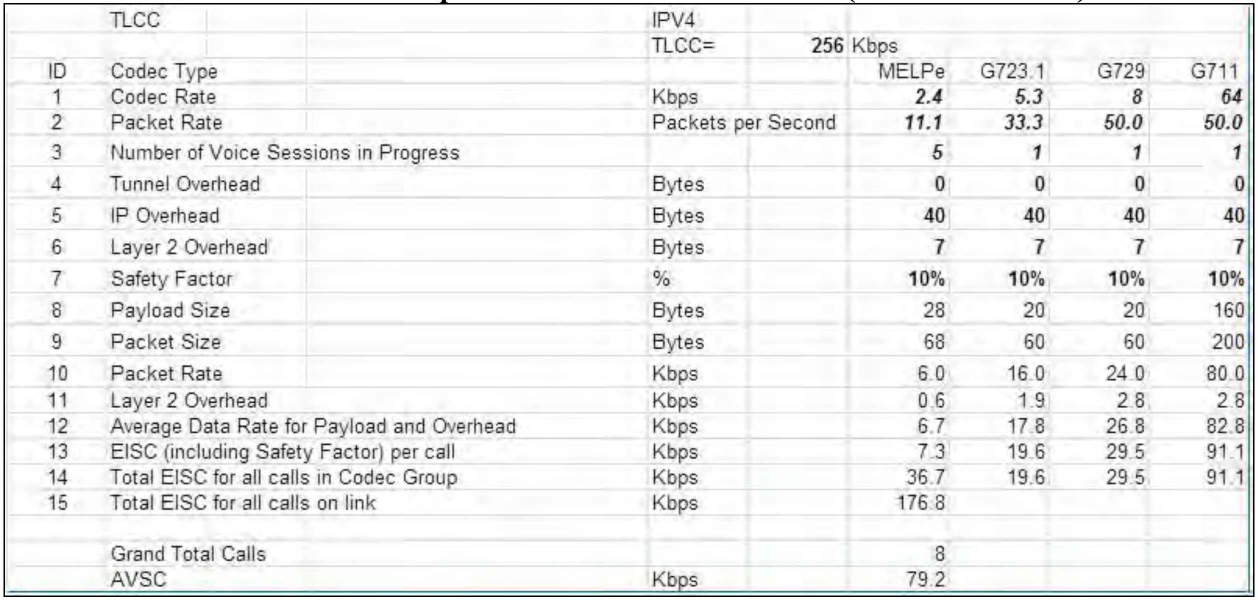
In Tables 2.16-2 through 2.16-5, the bolded, non-italicized numbers represent parameters that have been pre-entered into the product via NM commands. The bolded, italicized numbers are calculated by the product based on inspection of signaling packets. The non-bolded numbers are the calculations made by the product as part of the AVSC determination.

Example 1 (Table 2.16-2, Example 1: Current Session Status (No HAIPE Case)) shows a case where there is no HAIPE or voice MUX. There are eight sessions in progress. Five of these are MELPe sessions with one session each for the other codecs. The total EISC for these sessions is 176.8 Kbps, as shown in Table 2.16-2. The AVSC is 79.2 Kbps, based on a TSC of 256 Kbps. In this case, the SC could admit a new session using any of the codec types except G.711. If the next session offers a G.711 codec, the SC must block the session unless there is a lower precedence session that can be preempted.

Example 2 (Table 2.16-3, Example 2: AVSC Calculation assuming the G.711 Session is new (HAIPE Case) shows a case where a HAIPE is used to encrypt packets traversing the bottleneck link. In this example, there are seven sessions in progress: five MELPe sessions, one session for

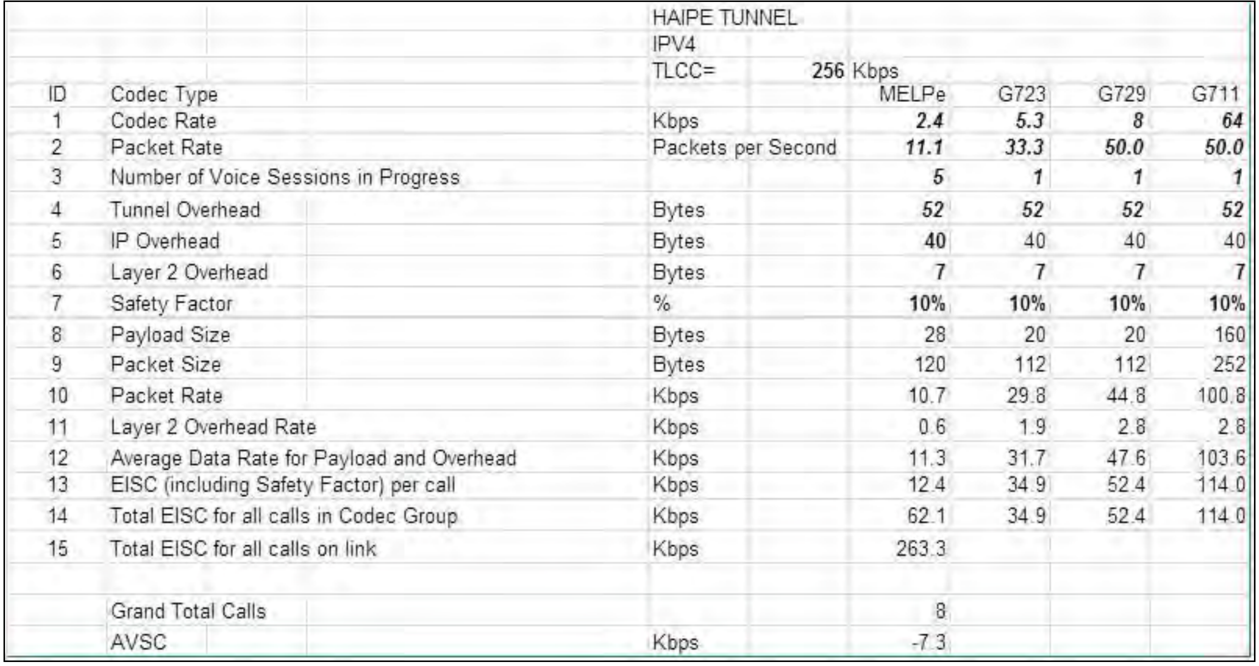
G.723.1, and one session for G.729. Also shown is one “potential” (new) G.711 session. The AVSC calculation takes place just after an INVITE request for a new G.711 session is generated. The SC calculates the AVSC for the G.711 session at negative 7.3 Kbps (see Table 2.16-3). The SC will reject the new session if it cannot preempt one of the existing sessions.

Table 2.16-2. Example 1: Current Session Status (No HAIPE Case)



	TLCC	IPV4				
		TLCC= 256	Kbps			
ID	Codec Type		MELPe	G723.1	G729	G711
1	Codec Rate	Kbps	*2.4*	*5.3*	*8*	*64*
2	Packet Rate	Packets per Second	*11.1*	*33.3*	*50.0*	*50.0*
3	Number of Voice Sessions in Progress		*5*	*1*	*1*	*1*
4	Tunnel Overhead	Bytes	0	0	0	0
5	IP Overhead	Bytes	40	40	40	40
6	Layer 2 Overhead	Bytes	*7*	*7*	*7*	*7*
7	Safety Factor	%	10%	10%	10%	10%
8	Payload Size	Bytes	28	20	20	160
9	Packet Size	Bytes	68	60	60	200
10	Packet Rate	Kbps	6.0	16.0	24.0	80.0
11	Layer 2 Overhead	Kbps	0.6	1.9	2.8	2.8
12	Average Data Rate for Payload and Overhead	Kbps	6.7	17.8	26.8	82.8
13	EISC (including Safety Factor) per call	Kbps	7.3	19.6	29.5	91.1
14	Total EISC for all calls in Codec Group	Kbps	36.7	19.6	29.5	91.1
15	Total EISC for all calls on link	Kbps	176.8			
	Grand Total Calls		8			
	AVSC	Kbps	79.2			

Table 2.16-3. Example 2: AVSC Calculation Assuming the G.711 Session Is New (HAIPE Case)

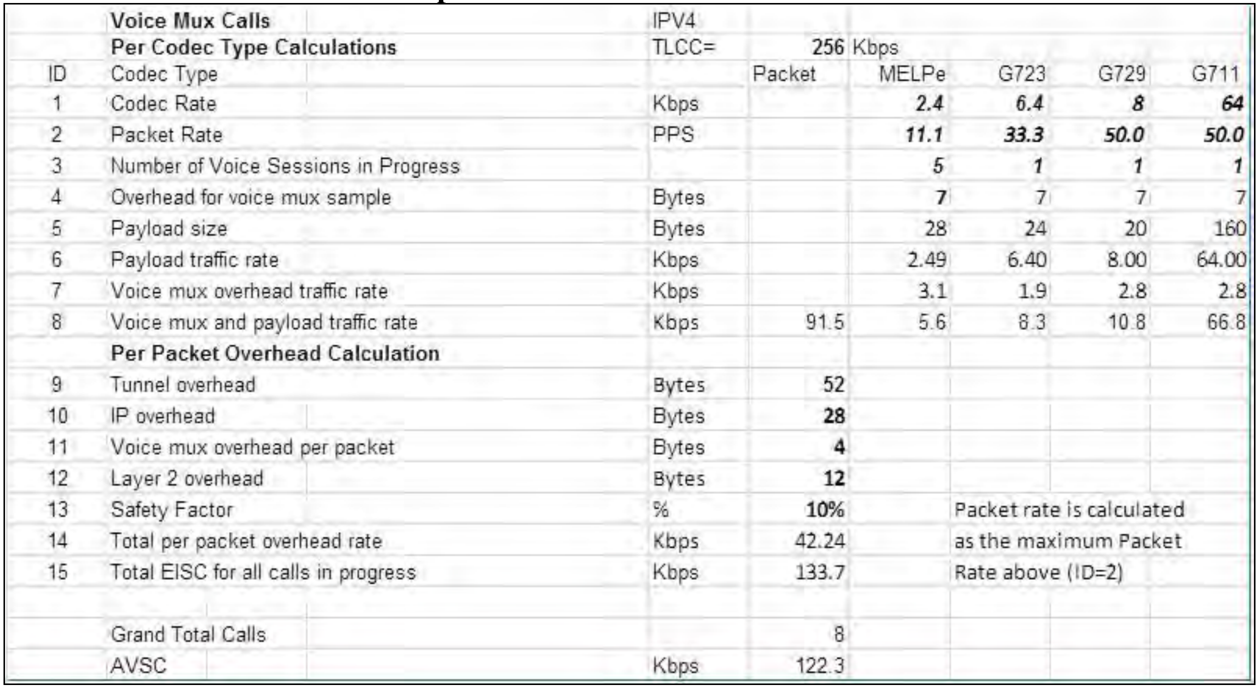


		HAIPE TUNNEL				
		IPV4				
		TLCC= 256	Kbps			
ID	Codec Type		MELPe	G723	G729	G711
1	Codec Rate	Kbps	*2.4*	*5.3*	*8*	*64*
2	Packet Rate	Packets per Second	*11.1*	*33.3*	*50.0*	*50.0*
3	Number of Voice Sessions in Progress		*5*	*1*	*1*	*1*
4	Tunnel Overhead	Bytes	*52*	*52*	*52*	*52*
5	IP Overhead	Bytes	40	40	40	40
6	Layer 2 Overhead	Bytes	*7*	*7*	*7*	*7*
7	Safety Factor	%	10%	10%	10%	10%
8	Payload Size	Bytes	28	20	20	160
9	Packet Size	Bytes	120	112	112	252
10	Packet Rate	Kbps	10.7	29.8	44.8	100.8
11	Layer 2 Overhead Rate	Kbps	0.6	1.9	2.8	2.8
12	Average Data Rate for Payload and Overhead	Kbps	11.3	31.7	47.6	103.6
13	EISC (including Safety Factor) per call	Kbps	12.4	34.9	52.4	114.0
14	Total EISC for all calls in Codec Group	Kbps	62.1	34.9	52.4	114.0
15	Total EISC for all calls on link	Kbps	263.3			
	Grand Total Calls		8			
	AVSC	Kbps	-7.3			

Example 3 (Table 2.16-4, Example 3: Use of Voice MUX with a HAIPE Tunnel) shows the case where a voice MUX is used to reduce the EISC per voice session. The environment for this

example is given in Figure 2.16-3, Notional System Environment for Example 3 (Voice MUX with HAIPE Tunnel). The TSC is 256 Kbps (full duplex). The network also contains a HAIPE device. Eight sessions are active: five MELPe sessions and one session each based on G.723.1, G.729, and G.711 codecs.

Table 2.16-4. Example 3: Use of Voice MUX With a HAIPE Tunnel



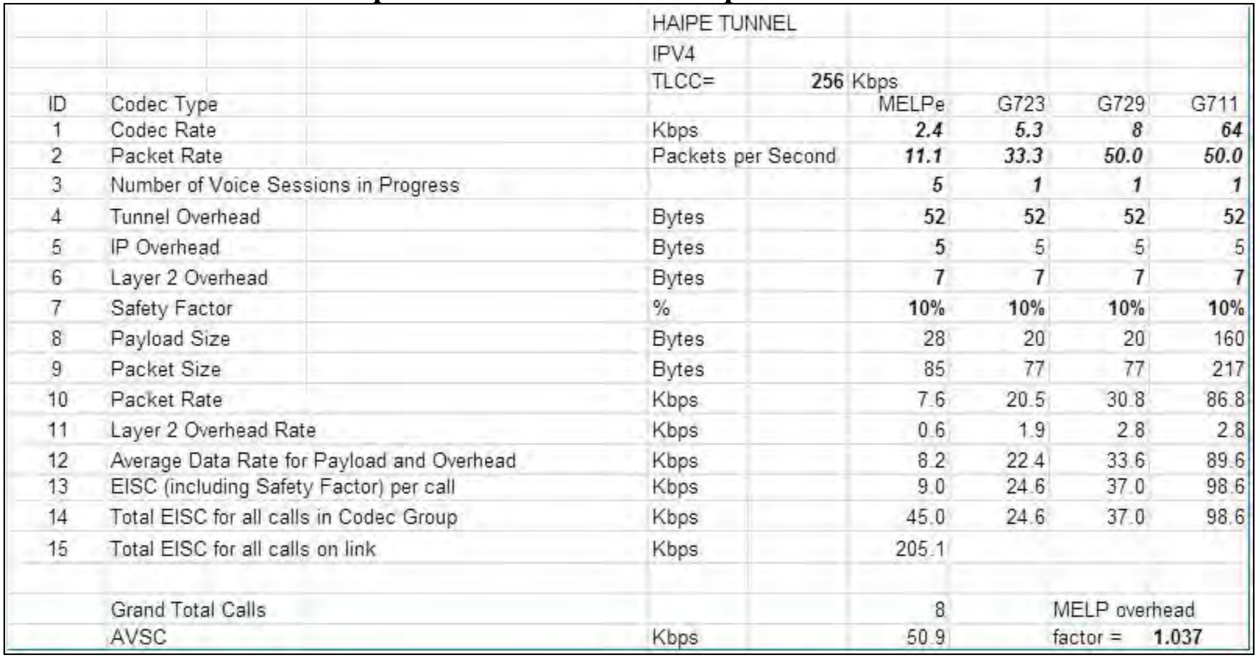
	Voice Mux Calls	IPV4					
	Per Codec Type Calculations	TLCC=	256	Kbps			
ID	Codec Type		Packet	MELPe	G723	G729	G711
1	Codec Rate	Kbps		***2.4***	***6.4***	***8***	***64***
2	Packet Rate	PPS		***11.1***	***33.3***	***50.0***	***50.0***
3	Number of Voice Sessions in Progress			***5***	***1***	***1***	***1***
4	Overhead for voice mux sample	Bytes		***7***	7	7	7
5	Payload size	Bytes		28	24	20	160
6	Payload traffic rate	Kbps		2.49	6.40	8.00	64.00
7	Voice mux overhead traffic rate	Kbps		3.1	1.9	2.8	2.8
8	Voice mux and payload traffic rate	Kbps	91.5	5.6	8.3	10.8	66.8
	Per Packet Overhead Calculation						
9	Tunnel overhead	Bytes	**52**				
10	IP overhead	Bytes	**28**				
11	Voice mux overhead per packet	Bytes	**4**				
12	Layer 2 overhead	Bytes	**12**				
13	Safety Factor	%	**10%**		Packet rate is calculated		
14	Total per packet overhead rate	Kbps	42.24		as the maximum Packet		
15	Total EISC for all calls in progress	Kbps	133.7		Rate above (ID=2)		
	Grand Total Calls		8				
	AVSC	Kbps	122.3				

The calculation takes into account two types of overhead; one for each output packet generated by the voice MUX; the other for each voice sample in the output packet. The per-packet overhead consists of the IP, tunnel and voice MUX byte overheads for each output packet. This overhead is multiplied by the output packet rate to determine the overhead rate in Kbps. The output packet rate is set at the highest rate of the codecs supported by the EIs on the SC side of the SC Path. The voice sample overhead is the number of bytes that the voice mux appends to each voice sample encapsulated in the output packet. The number of bytes per sample is multiplied by the voice sample rate of the input packets, to determine the overhead rate in Kbps.

The EISC, for this example, is 133.7 Kbps. The AVSC is 122.3 Kbps, based on a TSC of 256 Kbps. In this case the SC could admit a new session from any of the codec types. Compared to Table 2.16-3, Example 2: AVSC Calculation Assuming the G.711 Session in New (HAIPE Case), the use of the voice mux reduces the bandwidth demand from 263.3 Kbps to 133.7 Kbps, based on the notional numbers used in the examples.

Example 4 (Table 2.16-5, Example 4: Use of Header Compression with a HAIPE Tunnel) shows the case where header compression and HAIPEs are used. This example is based on the environment used in Example 2 with one addition: the CE-R supports header compression on the bottleneck link. The IP overhead parameter has been modified to account for a header compression mechanism that, on average, transmits 95 percent of packets with a compressed header of two bytes, and 5 percent of packets with a full IP, UDP, and RTP header of 40 bytes. This gives an average header size of 3.9 bytes, which has been rounded up to 5 bytes to provide a margin of safety. An approximate overhead factor of 4 percent has been added to account for MELPe overhead.

Table 2.16-5. Example 4: Use of Header Compression With a HAIPE Tunnel



		HAIPE TUNNEL					
		IPV4					
		TLCC=	256	Kbps			
ID	Codec Type			MELPe	G723	G729	G711
1	Codec Rate	Kbps		2.4	5.3	8	64
2	Packet Rate	Packets per Second		11.1	33.3	50.0	50.0
3	Number of Voice Sessions in Progress			5	1	1	1
4	Tunnel Overhead	Bytes		52	52	52	52
5	IP Overhead	Bytes		5	5	5	5
6	Layer 2 Overhead	Bytes		7	7	7	7
7	Safety Factor	%		10%	10%	10%	10%
8	Payload Size	Bytes		28	20	20	160
9	Packet Size	Bytes		85	77	77	217
10	Packet Rate	Kbps		7.6	20.5	30.8	86.8
11	Layer 2 Overhead Rate	Kbps		0.6	1.9	2.8	2.8
12	Average Data Rate for Payload and Overhead	Kbps		8.2	22.4	33.6	89.6
13	EISC (including Safety Factor) per call	Kbps		9.0	24.6	37.0	98.6
14	Total EISC for all calls in Codec Group	Kbps		45.0	24.6	37.0	98.6
15	Total EISC for all calls on link	Kbps		205.1			
	Grand Total Calls			8		MELP overhead	
	AVSC	Kbps		50.9		factor =	1.037

The AVSC is 50.9 Kbps, which would enable the SC to accept any new session request without preemption or blocking, except for a session that requires a G.711 codec.