

TABLE OF CONTENTS

<u>SECTION</u>	<u>PAGE</u>
Section 2 Session Control Products	2-1
2.1 Introduction.....	2-1
2.2 Voice Features and Capabilities.....	2-2
2.2.1 Call Forwarding	2-3
2.2.1.1 Call Forwarding Variable	2-4
2.2.1.2 Call Forwarding Busy Line.....	2-4
2.2.1.3 Call Forwarding – Don’t Answer – All Calls	2-5
2.2.1.4 Selective Call Forwarding.....	2-5
2.2.2 MLPP Interactions With Call Forwarding	2-5
2.2.2.1 Call Forwarding at a Busy Station	2-5
2.2.2.2 Call Forwarding – No Reply at Called Station	2-6
2.2.3 Precedence Call Waiting	2-6
2.2.3.1 Busy With Higher Precedence Call	2-6
2.2.3.2 Busy With Equal Precedence Call	2-6
2.2.3.3 Busy With Lower Precedence Call.....	2-7
2.2.3.4 No Answer	2-7
2.2.3.5 Line Active With a Lower Precedence Call	2-7
2.2.3.6 Call Waiting for Single Call Appearance VoIP Phones	2-7
2.2.4 Call Transfer.....	2-7
2.2.4.1 Call Transfer Interaction at Different Precedence Levels.....	2-8
2.2.4.2 Call Transfer Interaction at Same Precedence Levels	2-8
2.2.5 Call Hold	2-8
2.2.6 Three-Way Calling.....	2-9
2.2.6.1 Three-Way Calling for UEIs and PEIs	2-10
2.2.7 Hotline Service.....	2-10
2.2.7.1 Protected Hotline Calling.....	2-11
2.2.7.2 Hotline Service Protection	2-12
2.2.7.3 Non-Pair Protected Hotline Calling	2-13
2.2.7.4 Pair Protected Hotline Calling	2-14
2.2.8 Calling Number Delivery.....	2-14
2.2.8.1 Calling Name Delivery	2-14
2.2.8.2 Calling Party Organization and Location Delivery	2-14
2.2.9 Call Pick-Up.....	2-14
2.2.10 Precedence Call Diversion	2-15

2.2.11	Public Safety Voice Features	2-17
2.2.11.1	Basic Emergency Service (911).....	2-17
2.2.11.2	Tracing of Terminating Calls.....	2-18
2.2.11.3	Outgoing Call Tracing	2-18
2.2.11.4	of a Call in Progress	2-18
2.2.11.5	Tandem Call Trace.....	2-19
2.3	ASAC.....	2-19
2.3.1	ASAC Requirements Related to Voice	2-19
2.3.1.1	Voice Session Budget Unit	2-19
2.3.1.2	ASAC States	2-19
2.3.1.3	Session Control Processing With No Directionalization	2-21
2.3.1.4	SC Session Control Processing With Directionalization	2-23
2.3.2	ASAC Requirements for the SS Related to Voice	2-23
2.3.2.1	Voice Session Budget Unit	2-24
2.3.3	ASAC Requirements for the SC and the SS Related to Video Services.....	2-25
2.4	Signaling Protocols	2-26
2.4.1	Signaling Performance Guidelines.....	2-26
2.5	Registration and Authentication	2-27
2.6	SC and SS Failover	2-27
2.6.1	SC Monitors Primary SS for Status	2-28
2.6.2	Primary SS Monitors SC for Status	2-29
2.6.3	Each SS Monitors All Other SSs in the Network	2-29
2.6.4	Establish Subscriptions Using Failover Event Package.....	2-30
2.6.4.1	SC Creates Subscription With Primary SS	2-32
2.6.4.2	Exponential Back-Off.....	2-33
2.6.4.3	Invalid NOTIFY Body.....	2-33
2.6.4.4	Primary SS Creates Subscription With SC	2-33
2.6.4.5	SC Creates Subscription With Secondary SS	2-34
2.6.4.6	Secondary SS Creates Subscription With SC	2-34
2.6.4.7	Paired Softswitches (Active Primary/Secondary) Create Subscriptions With One Another	2-35
2.6.5	Subscription Refresh	2-35
2.6.5.1	SC Refreshes Subscription With Primary SS	2-35
2.6.5.2	Primary SS Refreshes Subscription With SC	2-36
2.6.5.3	SC Refreshes Subscription With Secondary SS	2-36
2.6.5.4	Secondary SS Refreshes Subscription With SC	2-37
2.6.5.5	SS Refreshes Subscription With Its Paired SS	2-37
2.6.6	SC Failover to Secondary SS	2-38

2.6.6.1	SSs Failover to Secondary SS.....	2-43
2.6.6.2	Failover to Secondary SS Triggered by Primary SS.....	2-44
2.6.7	SC Failback to Primary SS.....	2-44
2.6.7.1	SSs Failback to Primary SS	2-50
2.6.7.2	SC Failback to Primary SS Triggered by Primary SS	2-50
2.6.7.3	Security Considerations	2-50
2.6.8	SIP Event Package for Failover	2-51
2.6.8.1	Introduction.....	2-51
2.6.8.2	Subscription	2-51
2.6.8.3	Notifier Processing of SUBSCRIBE Requests.....	2-52
2.6.8.4	Notifier Generation of NOTIFY Requests.....	2-52
2.6.8.5	Subscriber Processing of NOTIFY Requests.....	2-53
2.6.8.6	Handling of Forked Requests.....	2-53
2.6.8.7	Rate of Notifications	2-53
2.6.8.8	NOTIFY Body Format.....	2-53
2.7	Product Interface.....	2-54
2.7.1	Internal Interface	2-54
2.7.2	External Physical Interfaces Between Network Components.....	2-54
2.7.3	Interfaces to Other Networks	2-55
2.7.3.1	Deployable Networks Interface	2-55
2.7.3.2	DISN Teleport Site Interface	2-55
2.7.3.3	PSTN Interface.....	2-55
2.7.3.4	Allied and Coalition Network Interface.....	2-55
2.7.4	DISA VVoIP EMS Interface.....	2-55
2.8	Product Physical, Quality, and Environmental Factors	2-56
2.8.1	Physical Characteristics	2-56
2.8.2	Product Quality Factors.....	2-56
2.8.2.1	Product Availability	2-56
2.8.2.2	Maximum Downtimes	2-58
2.8.3	Environmental Conditions	2-58
2.8.4	Voice Service Quality	2-59
2.9	End Instruments	2-59
2.9.1	IP Voice End Instruments	2-59
2.9.1.1	Basic.....	2-59
2.9.1.2	Tones and Announcements.....	2-60
2.9.1.3	Audio Codecs, Voice Instruments	2-64
2.9.1.4	VoIP PEI or UEI Telephone Audio Performance.....	2-64
2.9.1.5	Voice over IP Sampling Standard.....	2-64

2.9.1.6	Softphones.....	2-64
2.9.1.7	DSCP Packet Marking	2-65
2.9.2	Analog and ISDN BRI Telephone Support.....	2-66
2.9.2.1	ISDN BRI Telephone Support	2-67
2.9.3	Video End Instrument	2-68
2.9.3.1	Basic.....	2-68
2.9.3.2	Display Messages, Tones, and Announcements	2-68
2.9.3.3	Video Codecs (Including Associated Audio Codecs).....	2-69
2.9.3.4	Chg1-5.2.4.2 H.323 Video Teleconferencing.....	2-69
2.9.4	Authentication to SC	2-70
2.9.5	End Instrument to ASLAN Interface	2-70
2.9.6	Operational Framework for UEIs and Video EIs.....	2-70
2.9.6.1	Requirements for Supporting UC SIP EIs	2-71
2.9.6.2	Requirements for UC SIP Voice EIs	2-72
2.9.6.3	Requirements for UC SIP Secure Voice EIs.....	2-73
2.9.6.4	Requirements for UC SIP Video EIs	2-76
2.9.6.5	UC SIP Video EI Features	2-78
2.9.7	Multiple Call Appearance Requirements for UC SIP EIs.....	2-79
2.9.7.1	Multiple Call Appearance Scenarios	2-79
2.9.7.2	Multiple Call Appearances – Specific Requirements	2-80
2.9.7.3	Multiple Call Appearances – Interactions With Precedence Calls	2-82
2.9.8	PEIs, UEIs, TAs, and IADs Using the V.150.1 Protocol.....	2-84
2.9.9	UC Products With Non-Assured-Services Features	2-84
2.9.10	ROUTINE-Only EIs.....	2-85
2.10	Session Controller.....	2-86
2.10.1	PBAS/ASAC.....	2-86
2.10.2	SC Signaling	2-86
2.10.3	Session Controller Location Service.....	2-86
2.10.4	SC Management Function.....	2-87
2.10.5	SC-to-VVoIP EMS Interface	2-87
2.10.6	SC Transport Interface Functions	2-87
2.10.7	Custom Line-Side Features Interference.....	2-87
2.10.8	Loop Avoidance for SCs.....	2-88
2.10.9	Local Session Controller Application	2-88
2.10.9.1	Service Requirements Under Total Loss of WAN Transport Connectivity	2-89
2.11	UC SIP Gateways	2-89
2.11.1	UC SIP TDM Gateway	2-89

2.11.1.1	UC SIP TDM Gateway Signaling.....	2-90
2.11.1.2	SIP URI and Mapping of Telephone Number	2-91
2.11.1.3	UC SIP TDM Gateway Media.....	2-91
2.11.1.4	Information Assurance.....	2-91
2.11.1.5	UC SIP TDM Gateway Management Function	2-91
2.11.1.6	UC SIP TDM Gateway-to-EMS Interface	2-92
2.11.2	UC SIP IP Gateway.....	2-92
2.11.2.1	UC SIP IP Gateway Call Request Processing.....	2-93
2.11.2.2	SS Policing Requirements When Serving an UC SIP IP Gateway.....	2-94
2.11.2.3	Chg1-5.3.2.7.5.3.1 UC SIP IP Gateway SCS	2-95
2.11.2.4	Chg1-5.3.2.7.5.3.2 UC SIP IP Gateway Media Interworking	2-98
2.11.2.5	Chg1-5.3.2.7.5.3.3 Information Assurance.....	2-99
2.11.2.6	UC SIP IP Gateway Management Function	2-99
2.11.2.7	UC SIP TDM Gateway-to-EMS Interface	2-99
2.11.3	UC SIP – H.323 Gateway	2-99
2.11.3.1	UC SIP – H.323 Gateway Call Request Processing	2-100
2.11.3.2	SS Policing Requirements When Serving a UC SIP – H.323 Gateway	2-101
2.11.3.3	UC SIP – H.323 Gateway SCS	2-102
2.11.3.4	AS Precedence Capability Requirements and Resource Priority Header	2-103
2.11.3.5	SIP URI and Mapping of Telephone Number	2-104
2.11.3.6	Session Admission Control.....	2-105
2.11.3.7	UC SIP – H.323 Gateway Media Interworking.....	2-105
2.11.3.8	Information Assurance.....	2-106
2.11.3.9	UC SIP – H.323 Gateway Management Function	2-106
2.11.3.10	UC SIP – H.323 Gateway-to-EMS Interface	2-107
2.11.3.11	Product Quality Factors	2-107
2.12	Enterprise UC Services	2-107
2.12.1	Introduction	2-107
2.12.2	Centralized Enterprise Infrastructure	2-107
2.12.2.1	Enterprise Session Controller (ESC)	2-107
2.12.2.2	Enterprise Hosted UC Services.....	2-111
2.12.3	Edge Infrastructure.....	2-124
2.12.3.1	End Instruments	2-124
2.12.3.2	Media Gateway	2-125
2.12.3.3	COOP	2-125
2.12.4	Session Border Controller (SBC).....	2-128

2.12.4.1	General SBC Functionality	2-128
2.12.4.2	Enclave-Fronting SBC Functionality.....	2-128
2.12.4.3	ESC-fronting SBC Functionality	2-129
2.13	Network-Level Softswitch	2-130
2.13.1	Softswitch Location Server	2-131
2.13.2	SS Signaling Interfaces	2-132
2.13.3	Network Management System Interface	2-132
2.14	Call Connection Agent.....	2-132
2.14.1	Introduction	2-132
2.14.2	Functional.....	2-133
2.14.2.1	CCA IWF Component	2-133
2.14.2.2	CCA MGC Component.....	2-133
2.14.3	Role of the CCA in Network Appliances.....	2-134
2.14.4	CCA-IWF Signaling Protocol Support	2-134
2.14.4.1	CCA-IWF Support for UC SIP.....	2-135
2.14.4.2	CCA-IWF Support for PRI, via MG.....	2-135
2.14.4.3	CCA-IWF Support for CAS Trunks, via MG.....	2-138
2.14.4.4	CCA-IWF Support for PEI and UEI Signaling Protocols	2-142
2.14.4.5	CCA-IWF Support for VoIP and TDM Protocol Interworking.....	2-143
2.14.5	CCA Preservation of Call Ringing State During Failure Conditions	2-145
2.15	CCA Interaction With Network Appliances and Functions	2-145
2.15.1	CCA Interactions With Transport Interface Functions	2-146
2.15.2	CCA Interactions With the SBC	2-147
2.15.3	CCA Support for Admission Control.....	2-147
2.15.4	CCA Support for User Features and Services.....	2-148
2.15.5	CCA Support for Information Assurance	2-148
2.15.6	CCA Interactions With Session Controller Location Service.....	2-149
2.15.7	CCA Interactions With Softswitch Location Service	2-149
2.15.8	CCA Interactions With End Instrument(s).....	2-150
2.15.9	CCA Support for Assured Services Voice and Video	2-150
2.15.10	CCA Interactions With Service Control Functions.....	2-152
2.16	Media Gateway	2-152
2.16.1	MG Call Denial Treatments to Support CAC	2-153
2.16.1.1	MG Call Preemption Treatments to Support ASAC	2-153
2.16.1.2	MG and Information Assurance Functions.....	2-154
2.16.1.3	MG Interaction With Service Control Functions.....	2-155
2.16.1.4	Interactions With IP Transport Interface Functions.....	2-156
2.16.1.5	MG-SBC Interaction	2-156

2.16.1.6	MG Support for Appliance Management Functions.....	2-158
2.16.1.7	IP-Based PSTN Interface	2-158
2.16.1.8	MG Requirements: Interactions With VoIP EIs	2-158
2.16.1.9	MG Support for User Features and Services	2-159
2.16.2	MG Interfaces to TDM NEs in DOD Networks: PBXs, EOs, and MFSs...	2-159
2.16.3	MG Interfaces to TDM NEs in Allied and Coalition Partner Networks.....	2-160
2.16.4	MG Interfaces to TDM NEs in the PSTN in the United States	2-161
2.16.5	MG Interfaces to TDM NEs in OCONUS PSTN Networks.....	2-161
2.16.6	MG Support for ISDN PRI Trunks	2-162
2.16.7	MG Support for CAS Trunks.....	2-163
2.16.8	MG Requirements: VoIP Interfaces Internal to an Appliance	2-164
2.16.8.1	MG Support for VoIP Interconnection at the Physical and Data Link Layers	2-165
2.16.8.2	MG Support for VoIP Interconnection at the Network Layer	2-165
2.16.8.3	MG Support for VoIP Interconnection at the Transport Layer.....	2-165
2.16.8.4	MG Support for VoIP Interconnection for Media Stream Exchange Above the Transport Layer	2-166
2.16.8.5	MG Support for VoIP Interconnection for Signaling Stream Exchange Above the Transport Layer	2-167
2.16.8.6	MG Support for VoIP Interworking for ISDN PRI Trunks.....	2-167
2.16.8.7	MG Support for VoIP Interworking for CAS Trunks.....	2-168
2.16.8.8	MG Support for VoIP Codecs for Voice Calls	2-169
2.16.8.9	MG Support for Group 3 Fax Calls	2-170
2.16.8.10	MG Support for ISDN Over IP Calls and 64-Kbps Clear Channel Data Streams	2-173
2.16.8.11	MG Support for “Hairpinned” MG Calls.....	2-175
2.16.8.12	MG Support for Multiple Codecs for a Given Session.....	2-175
2.16.9	MG Requirements for Echo Cancellation	2-175
2.16.9.1	Trunk Gateway Echo Cancellation	2-175
2.16.10	MG Requirements for Clock Timing	2-176
2.16.11	MGC-MG CCA Functions.....	2-177
2.16.11.1	MG Support for MGC-MG Signaling Interface	2-177
2.16.11.2	MG Support for Encapsulated National ISDN PRI Signaling.....	2-179
2.16.11.3	MG Support for Mapped CAS Trunk Signaling Using H.248 Packages for MF and DTMF Trunks	2-179
2.16.11.4	MG Support for Glare Conditions on Trunks	2-181
2.16.11.5	MGC and IWF Treatments for PRI-to-UC SIP Mapping for TDM MLPP	2-182
2.16.11.6	MGC Support for MG-to-MG Calls	2-184

2.16.12	MGs Using the V.150.1 Protocol.....	2-184
2.16.13	MG Preservation of Call Ringing State During Failure Conditions	2-185
2.16.14	Remote Media Gateway.....	2-185
2.17	SBC.....	2-186
2.17.1	UC SIP Back-to-Back User Agent.....	2-186
2.17.2	Call Processing Load.....	2-187
2.17.3	Network Management.....	2-188
2.17.4	DSCP Policing	2-188
2.17.5	Codec Bandwidth Policing.....	2-188
2.17.6	Availability.....	2-188
2.17.7	IEEE 802.1Q Support	2-189
2.17.8	Packet Transit Time	2-189
2.17.9	H.323 Support	2-189
2.17.10	SBC Requirements to Support Remote MG	2-189
2.17.11	SBC Support for Multiple SCs.....	2-190
2.18	Worldwide Numbering and Dialing Plan	2-190
2.18.1	DSN Worldwide Numbering and Dialing Plan.....	2-191
2.18.1.1	CCA and SLS Support for Dual Assignment of DSN and E.164 Numbers to SS EIs	2-193
2.18.1.2	CCA Differentiation Between DSN Numbers and E.164 Numbers	2-194
2.18.1.3	CCA Use of SIP “phone-context” to Differentiate Between DSN and E.164 Numbers.....	2-195
2.18.1.4	Use of SIP URI Domain Name With DSN Numbers and E.164 Numbers.....	2-195
2.18.1.5	Domain Directory	2-197
2.19	Management of Network Appliances	2-198
2.19.1	General Management	2-198
2.19.2	Requirements for FCAPS Management.....	2-200
2.19.2.1	Fault Management	2-200
2.19.2.2	Configuration Management	2-201
2.19.2.3	Accounting Management	2-201
2.19.2.4	Performance Management	2-201
2.19.2.5	Security Management	2-204
2.20	Accounting Management	2-205
2.20.1	VoIP to PSTN	2-205
2.20.2	PSTN to VoIP	2-206
2.20.3	VoIP to VoIP.....	2-206
2.20.4	Quality of Service	2-207

2.21	V.150.1 Modem Relay Secure Phone Support	2-208
2.21.1	SCIP/V.150.1 Gateway	2-208
2.21.1.1	Basic Minimum Essential Requirements	2-208
2.21.1.2	Procedural Minimum Essential Requirements.....	2-211
2.21.1.3	SSE and SPRT Message Content.....	2-215
2.21.1.4	Use of Common UDP Port Numbers for SRTP, SSE, and SPRT Messages	2-216
2.21.1.5	UDP Port Number for SRTCP Media Control Packets	2-217
2.21.1.6	Use of V.150.1 SSE Messages for Media Transitions Between Audio and Modem Relay	2-218
2.21.1.7	Modem Relay and VoIP for SCIP/V.150.1 Gateways.....	2-219
2.21.1.8	Modem Relay Support for V.92 and V.90 Modulation Types	2-220
2.21.1.9	Going Secure, Glare Conditions, and Modem Relay Preferred Devices.....	2-221
2.21.2	SCIP/V.150.1 EI	2-222
2.21.2.1	Basic Minimum Essential Requirements (MERs)	2-223
2.21.2.2	Procedural MER.....	2-225
2.21.2.3	SSE and SPRT Message Content.....	2-227
2.21.2.4	Use of Common UDP Port Numbers for SRTP, SSE, and SPRT Messages	2-228
2.21.2.5	UDP Port Number for SRTCP Media Control Packets	2-228
2.21.2.6	Use of V.150.1 SSE Messages for Media Transitions Between Audio and Modem Relay	2-229
2.21.2.7	Going Secure, Glare Conditions, and Modem Relay Preferred Devices.....	2-230
2.21.3	SCIP/V.150.1 EI Requirements Using SCIP-214.2 Protocol	2-231
2.22	Requirements for Supporting UC SIP-Based Ethernet Interfaces for Voicemail Systems	2-232
2.22.1	Requirements for Supporting UC SIP Message Waiting Indications on UC SIP EIs, TAs, and IADs.....	2-234
2.23	Local Attendant Console Features	2-234
2.23.1	Precedence and Preemption	2-235
2.23.2	Call Display.....	2-235
2.23.3	Class of Service Override.....	2-235
2.23.4	Busy Override and Busy Verification	2-235
2.23.5	Night Service.....	2-236
2.23.6	Automatic Recall of Attendant.....	2-236
2.23.7	Calls in Queue to the Attendant	2-237
2.24	MSC and SSC	2-237

2.24.1	Highest Priority Sessions Method.....	2-238
2.24.2	Strict Budget for All SCs Method.....	2-238
2.24.3	EMS Access, UC SIP Signaling, Enclave Budgets, and MG Connections.....	2-240
2.25	MSC, SSC, and DYNAMIC ASAC Requirements in Support of Bandwidth- Constrained Links	2-241
2.25.1	MSC and SSC Architecture	2-242
2.25.1.1	Master/Subtended Architecture Applies to Both Voice and Video	2-242
2.25.1.2	MSC/SSC and DASAC.....	2-242
2.25.1.3	Directionalization Budget Inheritance	2-242
2.25.1.4	Minimum Number of Supportable SSCs per MSC.....	2-242
2.25.1.5	MSC Also an SSC.....	2-242
2.25.1.6	Two Budgets per Link per Media Type	2-242
2.25.1.7	Distinct Voice and Video DASAC Budgets	2-243
2.25.1.8	Long Locals	2-243
2.25.1.9	Logical SCs.....	2-243
2.25.2	Dynamic ASAC	2-243
2.26	Other UC Voice	2-249
2.26.1	Multilevel Precedence and Preemption.....	2-249
2.26.1.1	Precedence Levels.....	2-249
2.26.1.2	Invocation and Operation.....	2-249
2.26.1.3	Preemption in the Network.....	2-250
2.26.1.4	Preempt Signaling.....	2-255
2.26.1.5	Analog Line MLPP	2-259
2.26.1.6	ISDN MLPP BRI	2-259
2.26.1.7	ISDN MLPP PRI.....	2-261
2.26.1.8	MLPP Interactions With Common Optional Features and Services ...	2-265
2.26.1.9	MLPP Interactions With Electronic Key Telephone Systems Features	2-266
2.26.1.10	Network Management Manual Controls.....	2-267
2.26.2	Signaling	2-268
2.26.2.1	Introduction.....	2-268
2.26.2.2	Network Power Systems for External Interfaces	2-268
2.26.2.3	Line Signaling.....	2-268
2.26.2.4	Trunk Supervisory Signaling	2-269
2.26.2.5	Control Signaling.....	2-272
2.26.2.6	Alerting Signals and Tones.....	2-273
2.26.2.7	ISDN Digital Subscriber Signaling System No. 1 Signaling.....	2-273

2.26.3	ISDN	2-279
2.26.4	Backup Power	2-282
2.26.4.1	UPS	2-282
2.26.4.2	Backup Power (Environmental).....	2-282
2.26.4.3	Alarms.....	2-282
2.26.5	Echo Celler	2-282
2.26.5.1	EC Functionality	2-283
2.26.5.2	2100-Hertz EC Disabling Tone Capability.....	2-283
2.26.5.3	EC Hardware.....	2-284
2.26.5.4	Echo Cancellation on PCM Circuits.....	2-284
2.26.5.5	Device Management	2-284
2.26.5.6	Reliability.....	2-285
2.26.6	VoIP System Latency for MG Trunk Traffic.....	2-285
2.27	RTS Stateful Firewall	2-285
2.27.1	Introduction.....	2-285
2.27.2	Role of the RSF.....	2-285
2.27.3	Detailed RSF	2-286
2.27.3.1	RSF General.....	2-286
2.27.3.2	RSF Shall Not	2-287

LIST OF FIGURES

Figure 2.1-1.	Distributed UC Services Model	2-2
Figure 2.2-1.	Call Hold Scenarios.....	2-8
Figure 2.6-1.	Call Flow Diagram for Establishing Subscriptions Error Cases Not Included (Part 1).....	2-31
Figure 2.6-2.	Call Flow Diagram for Establishing Subscriptions Error Cases Not Included (Part 2).....	2-32
Figure 2.6-3.	Call Flow Diagram for SC Failover Error Cases Not Included	2-39
Figure 2.6-4.	Call Flow Diagram for SC Failback Error Cases Not Included.....	2-45
Figure 2.10-1.	Example of a Hairpin Routing Loop.....	2-88
Figure 2.25-1.	UC SIP Triggers for AVSC.....	2-246
Figure 2.26-1.	Example Hunt Sequence for Method 1	2-252
Figure 2.26-2.	Example Hunt Sequence for Method 2	2-254
Figure 2.26-3.	UC Preempt Signals (Part 1)	2-257
Figure 2.26-4.	UC Preempt Signals (Part 2).....	2-258

LIST OF TABLES

Table 2.2-1.	Assured Services Product Features and Capabilities	2-3
Table 2.2-2.	Route Code Assignments	2-10
Table 2.2-3.	Code Set 5 Optional Off-Hook Parameters.....	2-12
Table 2.2-4.	UC Hotline Service Protection Matrix.....	2-13
Table 2.9-1.	UC Ringing Tones and Cadences	2-60
Table 2.9-2.	UC Information Signals	2-61
Table 2.9-3.	Announcements.....	2-62
Table 2.11-1.	Summary of UC SIP TDM Gateway Functions.....	2-89
Table 2.11-2.	UC SIP TDM Gateway Support for VoIP and Video Signaling Interfaces	2-90
Table 2.11-3.	Summary of UC SIP IP Gateway Functions	2-92
Table 2.11-4.	UC SIP IP Gateway Support for VoIP and Video Signaling Interfaces	2-95
Table 2.11-5.	Summary of UC SIP – H.323 Gateway Functions.....	2-100
Table 2.11-6.	UC SIP – H.323 Gateway Support for VoIP and Video Signaling Interfaces	2-102
Table 2.14-1.	Full IWF Interworking Capabilities for VoIP and TDM Protocols	2-143
Table 2.16-1.	NI Digit Translation Table	2-182
Table 2.16-2.	Mapping of RPH r-priority Field to PRI Precedence Level Value	2-184

Table 2.18-1.	DSN User Dialing Format.....	2-191
Table 2.18-2.	Mapping of DSN tel Numbers to SIP URIs.....	2-191
Table 2.18-3.	Precedence and Service Access	2-193
Table 2.18-4.	White Pages Directory Data Elements	2-198
Table 2.25-1.	EISC Estimation Parameters	2-243
Table 2.26-1.	MLPP ISDN PRI Precedence Level Information Element (Code Set 5)....	2-262
Table 2.26-2.	Disconnect Message Cause Value	2-263
Table 2.26-3.	U.S. National Codepoints for Signal Values.....	2-263
Table 2.26-4.	ANSI T1.619a ISDN Setup Message Called Party Number Format	2-264
Table 2.26-5.	Reselect or Retrial	2-271
Table 2.26-6.	DTMF Generation and Reception From Users and Trunks	2-272
Table 2.26-7.	MF(R1) 2/6 Generation and Reception for Trunks.....	2-273
Table 2.26-8.	SETUP Message for MLPP Call.....	2-276
Table 2.26-9.	BRI Access, Call Control, and Signaling.....	2-279
Table 2.26-10.	Uniform Interface Configurations for BRIs.....	2-280
Table 2.26-11.	BRI Features	2-280
Table 2.26-12.	PRI Access, Call Control, and Signaling	2-281
Table 2.26-13.	PRI Features	2-281

SECTION 2

SESSION CONTROL PRODUCTS

2.1 INTRODUCTION

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

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

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

The application for how the various UC products are deployed within the network is described in the companion document entitled UC Framework 2013.

The SC product can be deployed in a distributed mode—physically located within the edge segment it serves—or as an enterprise services provider. [Figure 2.1-1](#), Distributed UC Services Model, shows an arrangement of SCs and SSs in the DISN assured services voice and video network. Please see UC Framework 2013, Section 2.2, for a description of the Enterprise UC Services model.

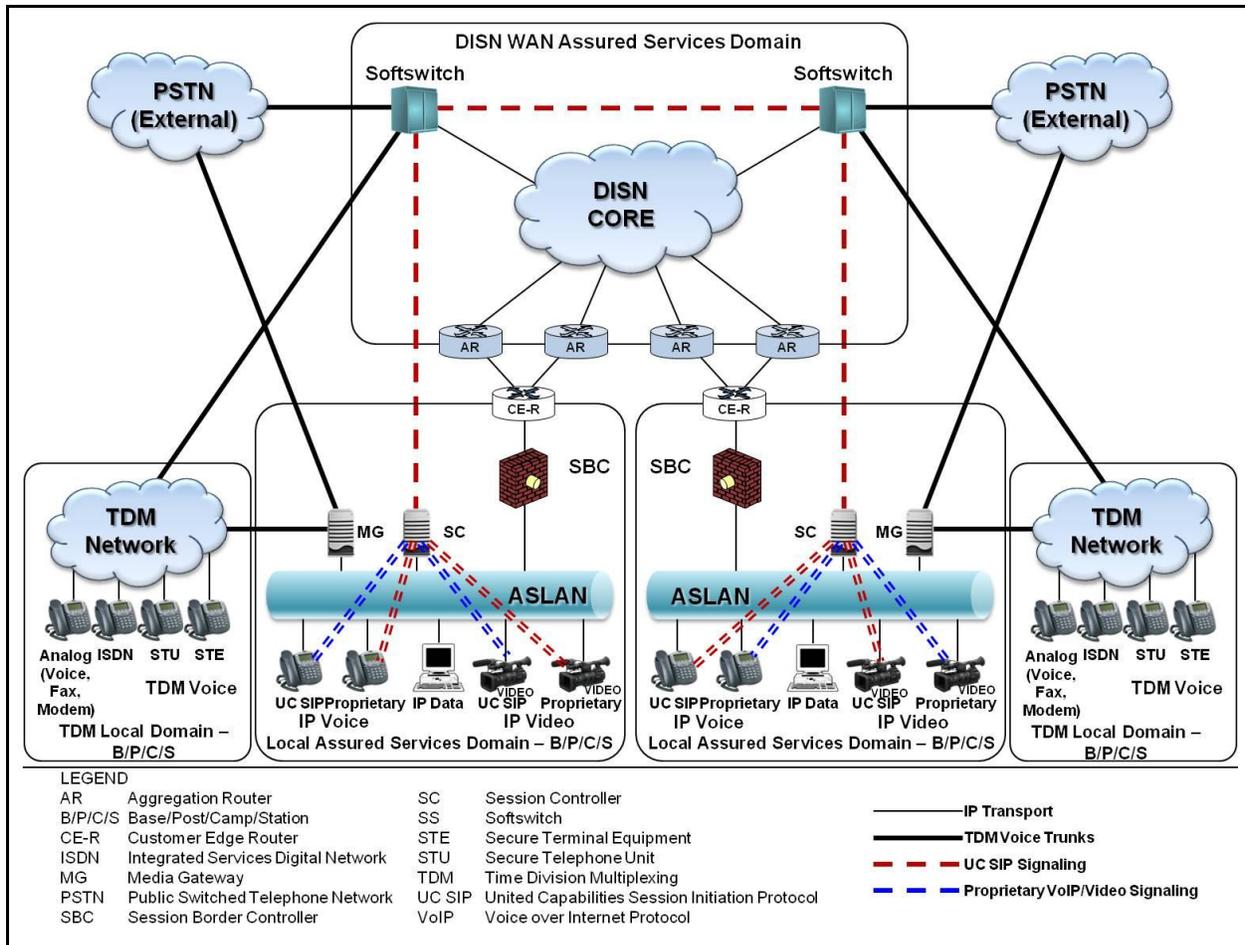


Figure 2.1-1. Distributed UC Services Model

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).

2.2 VOICE FEATURES AND CAPABILITIES

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

Table 2.2-1. Assured Services Product Features and Capabilities

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

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

SCM-000010 [Required: PEI, SC, SS] The Assured Services product's support for these vendor-proprietary VVoIP features and capabilities shall not adversely affect the required operation of the MLPP or ASAC features on that product. The required operation of the MLPP and ASAC features is specified in [Section 2.26.1](#), Multilevel Precedence and Preemption; this section; and UC SIP 2013.

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

2.2.1 Call Forwarding

Call Forwarding (CF) allows for incoming calls to a given line—or Directory Number (DN)—to be redirected to another DN, contingent upon feature activation and possibly other conditions.

The forwarded-to DN may be any telephone number, subject to the CoS restrictions of the DN activating the feature. Calls forwarded to DNs that have a call forwarding feature already activated may be forwarded again.

Four types of Call Forwarding features are considered for UC:

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

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

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

SCM-000030 [Optional: PEI, UEI, SC, SS] Reminder Ring for all call forwarding features, as specified in accordance with (IAW) Telcordia Technologies GR-217-CORE, GR-580-CORE, and GR-586-CORE, is optional.

2.2.1.1 Call Forwarding Variable

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

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

SCM-000050 [Optional: PEI, UEI, SC, SS] CFBL shall interact with MLPP IAW [Section 2.2.2.1](#), Call Forwarding at a Busy Station.

2.2.1.2 Call Forwarding Busy Line

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

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

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

2.2.1.3 Call Forwarding – Don’t Answer – All Calls

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

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

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

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

2.2.1.4 Selective Call Forwarding

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

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

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

2.2.2 MLPP Interactions With Call Forwarding

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

2.2.2.1 Call Forwarding at a Busy Station

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

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

- c. If the called IMMEDIATE/PRIORITY (I/P) user, FLASH/FLASH OVERRIDE (F/FO) user, or other UC user is non-preemptable (i.e., is not classmarked for preemption), the CF feature shall be invoked regardless of the precedence levels of incoming calls and established calls.
- d. The precedence level of calls is preserved during the forwarding process, and the forwarded-to user may be preempted.
- e. If the CFBL feature is activated and a precedence call (i.e., PRIORITY and above) is forwarded (including possible multiple forwarding), and if this forwarded call is not responded to by any forwarded-to party within a specified period (e.g., 30 seconds), the call shall be diverted to an attendant.

2.2.2.2 Call Forwarding – No Reply at Called Station

SCM-000140 [Conditional: PEI, UEI, SC, SS] If a called DN has a CF feature active or configured that supports MLPP:

- a. The precedence level of calls is preserved during the forwarding process, and the forwarded-to user may be preempted.
- b. If a precedence call (i.e., PRIORITY and above) is forwarded (including possible multiple forwarding) and is not responded to by any forwarded-to party (e.g., called party busy with a call of equal or higher precedence level; or called party busy and non-preemptable) within a specified period (e.g., 30 seconds), the call shall be diverted to an attendant.

2.2.3 Precedence Call Waiting

SCM-000150 [Required: PEI, UEI, SC, SS] The following Precedence Call Waiting (CW) treatment shall apply to precedence levels of PRIORITY and above.

2.2.3.1 Busy With Higher Precedence Call

SCM-000160 [Required: PEI, UEI, SC, SS] If the precedence level of the incoming call is lower than the existing MLPP call, Precedence CW shall be invoked. If the incoming call is PRIORITY precedence or above, the Precedence CW tone (see [Table 2.9-2](#), UC Information Signals) shall be applied to the called party.

2.2.3.2 Busy With Equal Precedence Call

SCM-000170 [Required: PEI, UEI, SC, SS] The End Instrument (EI) shall provide the Precedence CW tone (see [Table 2.9-2](#), UC Information Signals) to the called user. The EI shall apply this tone regardless of other programmed features, such as CF on busy or caller ID. The called EI shall be able to place the current active call on hold, or disconnect the current active call and answer the incoming call.

2.2.3.3 *Busy With Lower Precedence Call*

SCM-000180 [Required: PEI, UEI, SC, SS] The UC appliance shall preempt the active call. The active busy station EI shall receive continuous preemption tone until an “on-hook” signal is received and the other party on the preempted call shall receive a preemption tone for a minimum of 3 seconds. After going “on-hook,” the EI to which the precedence call is directed shall be provided precedence ringing. The EI shall be connected to the preempting call after going “off-hook.”

2.2.3.4 *No Answer*

SCM-000190 [Required: PEI, UEI, SC, SS] If, after receiving the Precedence CW signal, the busy called EI does not answer the incoming UC call within the maximum programmed time interval, then the SC/SS shall treat the call IAW [Section 2.2.10](#), Precedence Call Diversion.

2.2.3.5 *Line Active With a Lower Precedence Call*

SCM-000200 [Required: PEI, UEI, SC, SS] Precedence calls arriving at a busy EI that is classmarked as preemptable shall preempt the active lower precedence call. The active busy EI shall receive a continuous preemption tone until an “on-hook” signal is received and the other party shall receive a preemption tone for a minimum of 3 seconds (see [Table 2.9-2](#), UC Information Signals). After going “on-hook,” the station to which the precedence call is directed shall be provided precedence ringing (see [Table 2.9.1](#), UC Ringing Tones and Cadences). The station shall be connected to the preempting call after going “off-hook.”

If CW is invoked on the terminating DN, it shall be ignored and the existing lower precedence call shall be preempted.

2.2.3.6 *Call Waiting for Single Call Appearance VoIP Phones*

The UC CW feature is for single-call-appearance VoIP phones, Analog Terminal Adapters (ATAs), and Integrated Access Devices (IADs) only. It is not a feature for multiple-call-appearance VoIP phones.

2.2.4 *Call Transfer*

SCM-000210 [Required: PEI, UEI, SC, SS] Two types of call transfers are normal and explicit. A normal call transfer is a transfer of an incoming call to another party. An explicit call transfer happens when both calls are originated by the same subscriber. The UC signaling appliance shall provide the interactions described in the following paragraphs, with both normal and explicit call transfers.

2.2.4.1 Call Transfer Interaction at Different Precedence Levels

SCM-000220 [Required: PEI, UEI, SC, SS] When a call transfer is made at different precedence levels, the SC/SS that initiates the transfer shall classmark the connection at the highest precedence level of the two segments of the transfer.

2.2.4.2 Call Transfer Interaction at Same Precedence Levels

SCM-000230 [Required: PEI, UEI, SC, SS] The SC Service (SCS) that initiates a call transfer between two segments that have the same precedence level shall maintain the precedence level upon transfer.

2.2.5 Call Hold

SCM-000240 [Required: PEI, UEI, SC, SS] Call Hold is a function of the serving UC signaling appliance system and shall be invoked by going “on-hook,” then “off-hook.” Calls on hold shall retain the precedence of the originating call..

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

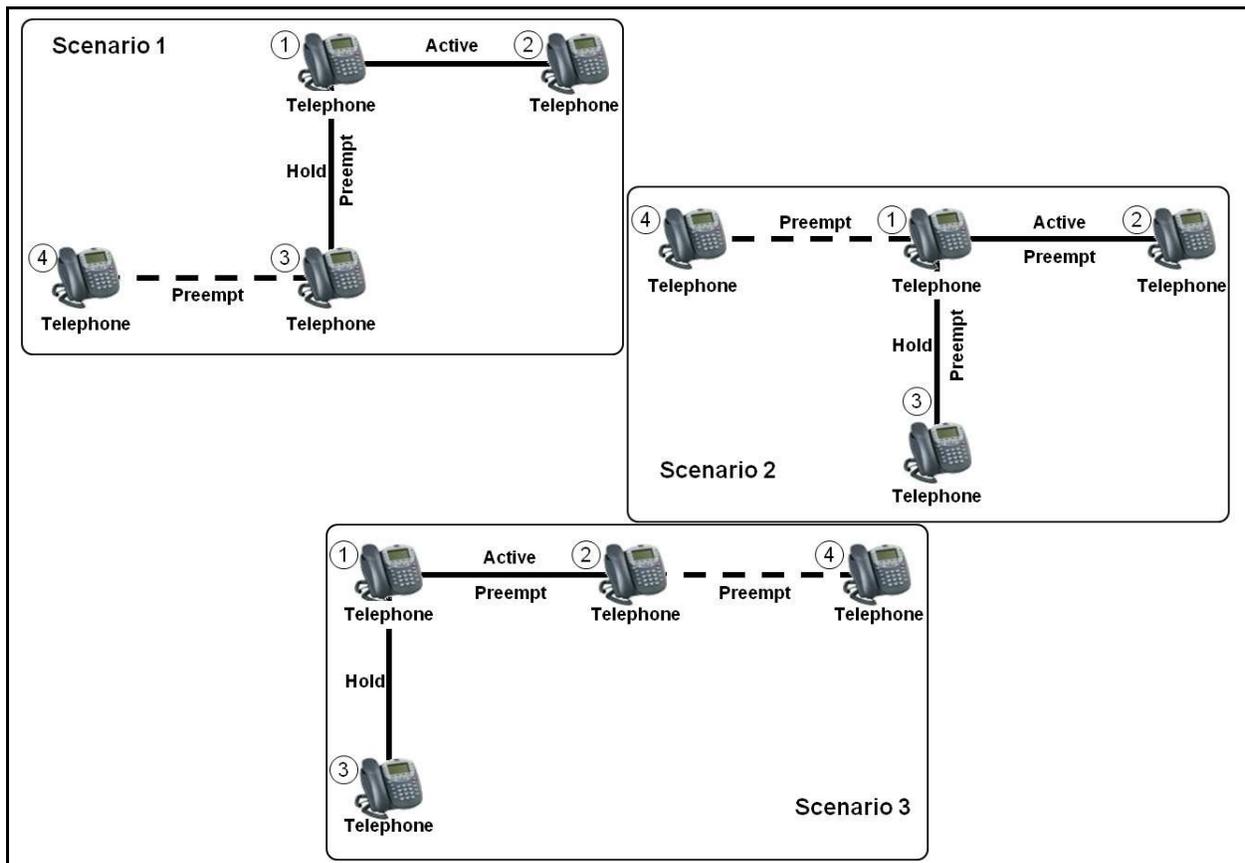


Figure 2.2-1. Call Hold Scenarios

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

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

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

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

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

2.2.6 Three-Way Calling

SCM-000250 [Required: PEI, UEI, SC, SS] In TWC, each call shall have its own precedence level. When a three-way conversation is established, each connection shall maintain its assigned precedence level. Each connection of a call resulting from a split operation shall maintain the precedence level that it was assigned upon being added to the three-way conversation.

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

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

SCM-000260 [Required: UEI, SC, SS] When the originator of the three-way call is on a UC SIP Video End Instrument (UEI) and is being preempted, the other two parties shall be disconnected from the three-way call.

SCM-000270 [Conditional: PEI, SC, SS] When the originator of the three-way call is on a PEI and is being preempted, if the TWC bridge is provided by the PEI, the other two parties shall be disconnected from the three-way call.

SCM-000280 [Conditional, Optional: PEI, SC, SS] When the originator of the three-way call is on a PEI and is being preempted, if the TWC bridge is provided by the SC or a Media Server, the other two parties may remain connected or may be disconnected.

2.2.6.1 *Three-Way Calling for UEIs and PEIs*

SCM-000290 [Required: UEI] Three-Way Calling shall be supported by UEIs consistent with UC SIP 2013, for TWC and the following sections of Request for Change (RFC) 5359:

- a. Section 2.10, Three-Way Conference – Third Party is Added.
- b. Section 2.11, Three-Way Conference – Third Party Joins.

SCM-000300 [Required: UEI] The TWC mixer/bridge shall be located in the UEI.

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

2.2.7 **Hotline Service**

SCM-000310 [Optional: PEI, TA, IAD, SC – Required: SS] The Hotline Service shall allow an analog subscriber or user to initiate a voice or data call to a predetermined party automatically by going off hook. The PEI or SC/SS shall dial hotline calls automatically when an “off-hook” condition occurs and the MG outpulses the appropriate routing digit, i.e., “5” for voice and “6” for circuit mode data calls when transported on non-Integrated Services Digital Network (ISDN) circuits. In addition, the hotline information can be carried in the Information Elements on ISDN circuits. Refer to [Table 2.2-2](#), Route Code Assignments.

Table 2.2-2. Route Code Assignments

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

* The user does not dial these route codes. The PEI or SC/SS shall dial hotline calls automatically when an off-hook condition occurs and outpulses the appropriate route digit (i.e., hotline voice-5 or hotline data-6).

LEGEND

CAS: Channel-Associated Signaling CCS: Common Channel Signaling N/A: Not Applicable

SCM-000320 [Optional: PEI, TA, IAD, SC – Required: SS] This service may be allowed for VVoIP end users (on a PEI) or Time Division Multiplexing (TDM) end users (on an analog or ISDN device behind an TA, IAD, or MG).

SCM-000330 [Optional: PEI, SC – Required: SS] The PEI or SC/SS shall have the ability to classmark a designated hotline user with a hotline indicator of either voice or data. The PEI or SC/SS also shall have the ability to make optional a hotline user as follows: origination only, termination only, and both origination and termination. Hotline users assigned a hotline indicator of voice shall only be allowed to connect with other hotline users assigned as voice, and hotline users assigned a hotline indicator of data shall be allowed only to connect with other hotline users assigned as data.

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

2.2.7.1 *Protected Hotline Calling*

SCM-000340 [Optional: PEI, SC; Required: SS] The Hotline Service Protection shall be accomplished within the same UC appliance and outside the serving UC appliance as follows:

- a. Classmarking the Hotline User for Data or Voice. This protection shall allow calls to complete only between hotline users with the same hotline indicator (i.e., data or voice).
 - (1) Only allowing completion of calls from hotline users found in a specified screening list. (This feature is required only between hotline users on the same UC appliance.)
 - (2) The MLPP interaction between hotline users shall be allowed only between hotline users classmarked with the same hotline indicator (i.e., voice or data), as described in [Section 2.26.1](#), Multilevel Precedence and Preemption, with the exception that unanswered hotline calls above ROUTINE precedence will not divert as defined in [Section 2.2.10](#), Precedence Call Diversion. Hotline user calls regardless of precedence level placed between hotline users with unlike hotline indicators (i.e., voice or data) shall receive a Vacant Code Announcement (VCA).

2.2.7.2 Hotline Service Protection

SCM-000350 [Optional: PEI, SC; Required: MG, SS] The Hotline Service Protection between an UC appliance and a circuit switch shall be accomplished between hotline users as follows:

- a. T1/E1 CAS, ANSI T1.619a, and E1 SS7 Q.735.3 Interfaces. The Hotline Service Protection via these interfaces shall be accomplished by the use of the Route Digit (i.e., hotline voice-5, hotline data-6). Hotline users classmarked as voice originating a call over these interfaces shall outpulse a Route Digit of 5, and hotline users classmarked as data shall outpulse a Route Digit of 6. Incoming calls, via these trunk types, with a Route Digit of 5 shall be allowed only to terminate at voice classmarked hotline users. Incoming calls with a Route Digit of 6 shall be allowed only to terminate at data classmarked hotline users. The hotline Route Digit of 5 or 6 shall be included in the worldwide numbering and dialing plan.
- b. T1 ISDN PRI ANSI T1.619a and E1 ISDN PRI ANSI Q.955.3 Interfaces. The Hotline Service Protection via this interface shall be accomplished by the use of the Optional Off-Hook Indicator parameter in the Setup message. This indicator shall be assigned in Code Set 5 with an element identifier of 01100101 binary (i.e., 65 hexadecimal). The data value within this identifier shall be one of two values: 00000001 (1) for hotline voice or 00000010 (2) for hotline data in Octet 3 as shown in [Table 2.2-3](#). These parameters will correlate directly to Route Digit 5 (voice) or Route Digit 6 (data), respectively. Interaction between Hotline Voice and Hotline Data Indicator parameters via this interface, and voice and data hotline users shall be the same as described in [Section 2.2.7.1](#), Protected Hotline Calling.

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

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

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

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

SCM-000360 [Optional: PEI, SC – Required: MG, SS] Hotline Service Protection interaction between hotline user indicators shall be as depicted in [Table 2.2-4](#), UC Hotline Service Protection Matrix.

Table 2.2-4. UC Hotline Service Protection Matrix

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

SCM-000370 [Optional: PEI, SC – Required: MG, SS] The UC Hotline service shall not be allowed to interact with the following services (This restriction shall be applied manually in software or by default when a user is classmarked as a hotline user):

- a. Hold (EI denied to put call on “HOLD”).
- b. Three way calling.
- c. Normal call transfer.
- d. Electronic Key Telephone System (EKTS).
- e. UC conferencing.

2.2.7.3 *Non-Pair Protected Hotline Calling*

SCM-000380 [Optional: PEI, SC – Required: SS] A Non-Pair Protected Hotline user shall be able to receive calls from any other hotline user with the same hotline indicator (i.e., voice or data) as described in [Section 2.2.7.1](#), Protected Hotline Calling. The Non-Pair Protected Hotline

user shall originate calls to a specified destination only, called the Designated Called Party (DCP).

2.2.7.4 *Pair Protected Hotline Calling*

SCM-000390 [Optional: PEI, SC – Required: SS] Pair Protected Hotline users shall only be able to call each other and shall not be allowed to receive calls from a third party. This protection shall be required for intra-UC appliance hotlines. It may be allowed for hotlines between a UC appliance and a circuit switch when end-to-end ISDN is supported between hotline users.

2.2.8 *Calling Number Delivery*

SCM-000400 [Required: PEI, UEI, SC, SS] The calling number provided to the called party shall be determined by the dialing plan used by the calling instrument, IAW Telcordia Technologies GR-31-CORE.

- a. If the incoming call is from another DSN user, the calling number shall be delivered to the called party in 10-digit DSN number format.
- b. If the incoming call is from a commercial user, the calling number shall be delivered to the called party in national or international calling number format.

2.2.8.1 *Calling Name Delivery*

SCM-000410 [Optional: PEI, UEI, TA, IAD, SC, SS] The UC products may support delivery of Calling Name information to SC end users on incoming UC calls.

2.2.8.2 *Calling Party Organization and Location Delivery*

SCM-000420 [Optional: PEI, UEI, TA, IAD, SC] The UC products may support delivery of Calling Party Org and Location information (e.g., the caller's military unit and location identity) to SC end users.

2.2.9 *Call Pick-Up*

SCM-000430 [Optional: PEI, UEI, SC, SS] A user EI may be equipped to answer any calls directed to other EI within the user's own preset pick-up group, as established by an administrative facility, by dialing the appropriate feature code.

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

- a. Basic Call Pick-Up. An EI may answer a call that has been offered to another EI in its common call pick up group in a business group. This is accomplished by dialing a pick-up access code while the called EI is 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.

- b. Directed Call Pick-Up. Directed call pick-up permits a user to dial a code and destination number and pick up a call that has been answered or is ringing at another telephone, provided the rung telephone permits dial pick-up. If the other EI has answered, a TWC is established.
- c. Directed Call Pick-Up Without Barge-In. This feature is identical to the Directed Call Pick-Up feature, except that if the destination number being picked up has already answered, the party dialing the pick-up code shall be routed to reorder rather than be permitted to barge in on the established connection to create a TWC.

SCM-000440 [Conditional: PEI, UEI, SC, SS] If a Call Pick-Up feature is provided, it shall be IAW Telcordia Technologies GR-590-CORE.

SCM-000450 [Conditional: PEI, UEI, SC, SS] If a Call Pick-Up feature is provided, it shall interact with MLPP IAW the following:

- a. If a call pick-up group has more than one party in an unanswered condition and the unanswered parties are at different precedence levels, a call pick-up attempt in that group shall retrieve the highest precedence call first. If multiple calls of equal precedence are ringing simultaneously, a call pick-up attempt in that group shall retrieve the longest ringing call first.
- b. If a party in a call pick-up group is busy, and an incoming precedence call is placed to that number, normal MLPP rules shall apply. This call cannot be picked up within the call pick-up group unless it is an unanswered call, provided there are no additional features such as CW or CF.

2.2.10 Precedence Call Diversion

The following limitations apply to Precedence Call Diversion (PCD):

- Support for Precedence Call Diversion from one UC EI to another UC EI on the same SC (or internal SC within a SS) 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 End Office (EO), SMEO, Private Branch Exchange (PBX) 1, or PBX 2] is not required.
- Support for Precedence Call Diversion from a DSN EI (on an EO, SMEO, PBX 1, or PBX 2) to an UC EI on an SC is not required.

SCM-000460 [Required: SC, SS] The UC SIP signaling appliance shall divert ALL unanswered UC VoIP calls above the ROUTINE level to a designated UC DN for PCD (e.g., the number of an attendant console or group of attendant consoles). This diversion shall occur after a specified PCD time period, selectable from 15–45 seconds, and configurable at the per-appliance level

SCM-000470 [Required: SC, SS] Unanswered UC VoIP calls above the ROUTINE precedence level shall not be forwarded to voicemail, and shall not be forwarded to ACD systems. Instead, they shall divert to the PCD DN when the PCD time period expires.

SCM-000480 [Required: SC, SS] Unanswered UC VoIP ROUTINE calls to DNs that are configured with voicemail or an ACD system shall be forwarded to voicemail or to the ACD system.

SCM-000490 [Required: SC, SS] Calls above the ROUTINE precedence level that are directly dialed to DNs assigned to voicemail or ACD systems shall divert to the PCD DN as specified above (i.e., when they are unanswered at the voicemail or ACD system, and the PCD time period expires).

SCM-000500 [Required: SC, SS] The UC SIP signaling appliance shall support a per-appliance configuration option that, when activated, diverts ROUTINE calls directly dialed to DNs assigned to voicemail or ACD systems to the PCD DN, if they go unanswered and the PCD time period expires. These calls shall keep their ROUTINE precedence level after they are diverted by PCD. When this configuration option is not used, unanswered ROUTINE calls shall continue to be offered to the voicemail or ACD system, and shall not be diverted by PCD.

Precedence Call Diversion may divert calls to the DN of an Attendant Console (or group of attendant consoles). End users can also place precedence calls directly to this attendant console (or group of attendant consoles) by dialing its number from their EIs. The following requirements cover the handling of these precedence calls in these cases. Each attendant console is an UC EI served by an SC in the subsequent requirements.

SCM-000510 [Required: SC, SS] Incoming precedence calls to the attendant's listed DN, and incoming calls that are diverted to this attendant DN, shall be placed in a queue for the attendant console (or group of attendant consoles). A distinctive visual signal indicating the precedence level of the call (including ROUTINE, when a ROUTINE call is placed or diverted to the attendant's DN) shall be sent to the attendant console (or group of attendant consoles) when this call is queued.

SCM-000520 [Required: SC, SS] When a group of attendant consoles on the same SC is used, and calls are either placed or diverted to the attendant console DN, call distribution across the Console Group shall be used to reduce excessive caller waiting times. Each attendant console in the group shall operate from a common queue (or common set of queues) associated with the Console DN.

SCM-000530 [Required: SC, SS] Incoming calls (placed and diverted) to the console DN shall be queued for attendant service by call precedence and time of arrival. The highest precedence call with the longest holding time in the queue shall be offered to an attendant first.

SCM-000540 [Required: SC, SS] A recorded message of explanation (e.g., ATQA) shall be applied automatically to all the waiting calls in the attendant console queue (refer to [Table 2.9-3](#), Announcements).

NOTE: In the set of announcements in UC SIP 2013, Table 5.3.4-9 (i.e., BPA, Unauthorized Precedence Announcement (UPA), BNEA, ATQA), ATQA is now a UCR requirement.

SCM-000550 [Conditional: SC, SS] If the B/P/C/S where the SC or SS is located does not have a continuously manned Attendant Station (or set of Attendant Stations), an announcement shall be provided 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 Station (or Stations) on another SC or SS.

2.2.11 Public Safety Voice Features

2.2.11.1 Basic Emergency Service (911)

SCM-000560 [Required: SC, SS] The Basic 911 Emergency Service feature provides a three-digit universal telephone number (e.g., 911) that gives the public direct access to an emergency service bureau. The emergency service is one way only, terminating to the service bureau. A given local switching system shall serve no more than one emergency service bureau. When the originating line and the emergency service bureau are served by the same switching system, the bureau can hold and disconnect the connection and monitoring the supervisory state, and ringing the originating station back. When the local switching system is in an area with enhanced emergency service (E911) served through a tandem switch, the emergency call is advanced to the tandem switch with calling line Automatic Number Identification (ANI) or Calling Number Delivery (CND).

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

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

In the continental United States (CONUS), calls from UC users to 911 are not subject to Multilevel Precedence and Preemption, i.e., 911 calls shall not be preempted. This requirement

also applies to 911 calls outside CONUS (OCONUS) from UC users in Hawaii, Alaska, and the U.S. overseas territories (e.g., Guam).

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

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

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

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

2.2.11.2 Tracing of Terminating Calls

SCM-000570 [Required: SC, SS] The Tracing of Terminating Calls feature identifies the calling number on intraoffice and interoffice calls terminating to a specified DN. When this feature is activated, the originating DN, the terminating DN, and the time and date are recorded for each call to the specified line.

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

2.2.11.3 Outgoing Call Tracing

SCM-000580 [Required: SC, SS] The Outgoing Call Tracing feature allows the tracing of nuisance calls to a specified DN suspected of originating from a given local office. The tracing is activated when the specified DN is entered. A record of the originating DN, and the time and date, are generated for every call to the specified DN.

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

2.2.11.4 of a Call in Progress

SCM-000590 [Required: SC, SS] The Tracing of a Call in Progress feature identifies the originating DN for a call in progress. Authorized personnel entering a request that includes the specific terminating DN involved in the call activate the feature.

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

2.2.11.5 Tandem Call Trace

SCM-000600 [Optional: SC – Required: SS] The Tandem Call Trace feature identifies the calling party of a tandem call to a specified office DN. The feature is activated by entering the specified distant office DN for a tandem call trace. A record of the calling party number and terminating DN, and the time and date, is generated for every call to the specified DN. The Calling Party Number shall be taken from the P-Asserted-Identity, From, or Contact header in the incoming UC SIP INVITE message for this call. The P-Asserted-Identity header is preferred over the From and Contact headers because the value in the P-Asserted-Identity header is UC-network-validated.

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

2.3 ASAC

This section presents the ASAC requirements for the SC and the SS. In the execution of ASAC, certain procedures need to be followed, such as (a) actions to be taken if a precedence session request cannot be completed because existing sessions are at equal or higher precedence, or (b) tones to be generated when a session is preempted. [Section 2.26.1](#), Multilevel Precedence and Preemption, addresses these issues. UC SIP 2013, provides a more detailed description of the session control signaling requirements of the SC and the SS.

2.3.1 ASAC Requirements Related to Voice

2.3.1.1 Voice Session Budget Unit

SCM-000610 [Required: SC, SS] One voice session budget unit shall be equivalent to 110 kilobits per second (kbps) of access circuit bandwidth independent of the PEI or UEI codec used. This bandwidth equivalent is based on International Telecommunications Union – Telecommunication (ITU-T) Standardization Sector Recommendation G.711 encoding rate plus IPv6 packet overhead plus Assured Services (AS) Local Area Network (ASLAN) Ethernet overhead. IPv6 overhead, not IPv4 overhead, is used to determine bandwidth equivalents here.

2.3.1.2 ASAC States

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

SCM-000620 [Required: SC, SS] The states that shall be maintained for ASAC purposes are as follows:

- a. **[Required: SC]** Line Side States. The SC shall maintain the session state of each local PEI and UEI in its domain as follows:
 - (1) **Busy/Not Busy**. The Busy State includes the session setup phase and the active session phase.
 - (2) **Session Precedence**. If the PEI or UEI is busy, the state shall include the precedence level of the session (FO, F, I, P, R).
 - (3) The Line Side States also apply to multi-appearance EIs, but at this time, no more than two line appearances are dealt with, and the procedures are the same as for ISDN Basic Rate Interface (BRI) instruments.
- b. Trunk Side States.
 - (1) **[Required: SC, SS]** The SC and its associated SS shall be configurable with the following VoIP Session Budgets:
 - (a) **IP Budget (IPB)**. The total budget of VoIP sessions plus session attempts in the session setup phase that are allowed on the Customer Edge (CE) Router (CE-R) to Wide Area Network (WAN) IP access link.
 - (b) **[Optional] IPBo**. The budget for outbound VoIP sessions plus session attempts in the session setup phase that are allowed on the IP access link.
 - i. IPBo may take any value in the range (0, IPB) or “null.”
 - ii. Null implies that there are no outbound directionalization restrictions.
 - (c) **[Optional] IPBi**. The budget for inbound VoIP sessions plus session attempts in the session setup phase that are allowed on the IP access link.
 - i. IPBi may take any value in the range (0, IPB) or “null.”
 - ii. Null implies that there are no inbound directionalization restrictions.Note the relationship among IPB, IPBo, and IPBi:
 - iii. IPBi plus IPBo equals IPB, if there is directionalization.
 - iv. IPBi equals null if, and only if, IPBo equals null.
 - (2) **[Required: SC, SS]** The SC and its associated SS shall maintain the following VoIP Session Counts:
 - (a) **IP Count (IPC)**. The total number of interbase IP sessions in progress plus the number of session attempts in the session setup phase.
 - (b) **[Optional] IPCo**. The number of outbound IP sessions in progress plus the number of outbound session attempts in the session setup phase.

- (c) [**Optional**] IPC_i. The number of inbound IP sessions in progress plus the number of inbound session attempts in the session setup phase.
- (3) [**Required: SC**] A TDM Session Budget (TDMB) shall be configurable on an SC. This amount is the budget for the overall number of TDM sessions plus sessions in the session setup phase on the SC's TDM links. This budget equals the number of digital signal level 0s (DS0s) on the trunk between the SC MG and the EO/SMEO/PBX1/PBX2.
- (4) [**Required: SC**] The SC shall maintain a TDM Session Count that is the total number of sessions in progress between the TDM switch and the SC's Media Gateway, plus the total number of session attempts in the session setup phase.

2.3.1.3 *Session Control Processing With No Directionalization*

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

1. SC Processing for an Outbound Session.

SCM-000630 [**Required: SC**] The SC shall take the following actions when an outbound session request is initiated by a local PEI or UEI:

- a. Users and/or PEIs and/or UEIs that place sessions shall be authenticated as per Section 4, Information Assurance Requirement, before processing the outbound session.
 - (1) If IPC is less than IPB, the session request shall be forwarded to the SS for forwarding to the sessioned SC for processing (see item 2, SC Processing for an Inbound Session).
 - (2) If IPC equals IPB and all existing sessions are at precedence equal to or greater than the new session request, then the SC shall not place the session, and the caller shall receive a Blocked Precedence Announcement (BPA). If it is a ROUTINE call, the caller shall receive an All Circuits Busy indication as per Table 2.9-2, UC Information Signals.
 - (3) If IPC equals IPB and at least one existing session is of lower precedence than the new session, the SC shall preempt one of the lowest precedence sessions and shall forward the session INVITE (via the SS) to the sessioned SC for processing. The algorithm for selecting the session to preempt shall be deterministic.
 - (4) IPC is greater than IPB is not an allowed state. If this occurs, the SC shall either:
 - (a) Deterministically preempt sessions starting with those of lowest precedence until IPC equals IPB, and then proceed as specified in items (3) and (4) previously.
 - (b) Allow the sessions to terminate naturally until IPC equals IPB.

The SC shall notify the Network Management System (NMS) of this fault state.

(5) The SC shall increment and decrement its IPC as follows:

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

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

2. SC Processing for an Inbound Session.

SCM-000640 [Required: SC] The SC shall take the following actions when a new inbound session INVITE is received from a remote SC:

- a. If IPC is less than IPB and the local PEI or UEI is not busy, then the SC shall place the session.
- b. If IPC is less than IPB and the local PEI or UEI is busy with a session that is of lower precedence level than the one being placed, the SC shall preempt the existing session and place the new session.
- c. If IPC is less than IPB and the local PEI or UEI is busy with a session that is of an equal or higher precedence level than the session being placed, the new session is not placed. The caller shall receive a BPA, and if it is a ROUTINE call, the caller shall receive an All Circuits Busy indication as per [Table 2.9-2](#), UC Information Signals.
- d. If IPC equals IPB and the local PEI or UEI is not busy, and all existing sessions on the access link are at a precedence level equal to or greater than the new session, the SC shall not place the new session. The caller shall receive a BPA, and if it is a ROUTINE call, the caller shall receive an All Circuits Busy indication as per [Table 2.9-2](#), UC Information Signals.
- e. If IPC equals IPB and the local PEI or UEI is not busy, and at least one existing session on the access link is of a lower precedence level than the new session, the SC shall deterministically preempt one of the lowest precedence sessions. Then it shall forward the session INVITE to the sessioned SC via the SS for processing.
- f. If IPC equals IPB and the local PEI or UEI is busy with a session that is of a lower precedence level than the new session, then the SC shall preempt the session and forward the session INVITE to the local PEI or UEI.
- g. If IPC equals IPB and the local PEI or UEI is busy with a session that is of an equal to or higher precedence level than the new session, the SC shall not place the session. The caller shall receive a BPA, and if it is a ROUTINE call, the caller shall receive an All Circuits Busy indication as per [Table 2.9-2](#), UC Information Signals.
- h. The IPC is greater than IPB is not an allowed state. If this occurs, the SC shall deterministically preempt sessions starting with those of the lowest precedence level until IPC equals IPB, and then proceed as specified in items d, e, f, and g. The SC shall notify the NMS of this fault state.

SCM-000650 [Required: SC] The SC shall increment and decrement its IPC as specified in, UC SIP 2013.

SCM-000660 [Required: SC] SC Processing for a Local Session. A local session is one that is initiated by a local PEI or UEI intended for another local PEI or UEI.

- a. If the sessioned PEI or UEI is not busy, the SC shall complete the session.
- b. If the sessioned PEI or UEI is busy with a session that is of a lower precedence level than the new session, the SC shall preempt the session, and then complete the new session.
- c. If the call attempt is at a precedence level above ROUTINE and the local PEI or UEI is busy with a session that is equal to or higher than the precedence level of the new session, the SC shall not complete it. The caller shall receive a BPA. If the call attempt is a ROUTINE call and the local PEI or UEI is busy with a session, the caller shall receive Station Busy tone as per [Section 2.9.1.2.1](#), UC Ringing Tones, Cadences, and Information Signals.
- d. The SC does not modify its IPC when local sessions are connected or disconnected because they do not affect traffic in the access link to the WAN.
- e. **[Optional]** An intrabase session count shall be maintained separately, independent of precedence, and when this valve is reached no more ROUTINE precedence level session requests shall be processed for intrabase connection. PRIORITY, IMMEDIATE, FLASH, and FLASH OVERRIDE session requests shall be processed as specified in items a, b, and c.

2.3.1.4 SC Session Control Processing With Directionalization

The requirements for ASAC directionalization are optional.

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

SCM-000670 [Optional: SC] When ASAC directionalization is implemented and applied, directionalized session budgets (IPBo and IPBi) will be set and the SC may keep a running count of IPCo and IPCi to ensure that these counts do not exceed their respective budgets. The IPCo processing is carried out independently from that of IPCi. Each process is identical to that carried for IPC for non-directionalization, as specified earlier. Since the IPCo and IPCi control processes are independent, a FLASH OVERRIDE inbound session will not be able to preempt a ROUTINE outbound session.

2.3.2 ASAC Requirements for the SS Related to Voice

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

2.3.2.1 Voice Session Budget Unit

(The requirements on directionalization in this section are optional.)

SCM-000680 [Required: SS] The SS shall be configurable with the IPB, IPBi, and IPBo VoIP Session Budgets for each SC in its domain, consistent with the requirements in [Section 2.3.1.2](#), ASAC States.

SCM-000690 [Required: SS] The SS shall maintain a running count of IPC, IPCo, and IPCi for each SC in its domain. It shall do this by monitoring the UC SIP messages associated with each of its subordinate SCs as specified in UC SIP 2013.

SCM-000700 [Required: SS] SS Session Processing with no Directionalization. Initially, the IPC for each SC is set to zero. The SS shall increment and decrement the IPC as follows:

- a. For outbound sessions:
 - (1) After having received a session request (i.e., INVITE) from its local SC, the SS increments the corresponding IPC upon forwarding that session request to the far-end SC.
 - (2) The SS decrements its IPC when it determines that a session request is completely terminated or an established session is completely terminated.
- b. For inbound sessions:
 - (1) The SS increments its IPC upon transmitting to the far-end SC a “session accepted” (i.e., 1XX or 2XX) response to an INVITE request that it received from the far-end SC. (The IPC is not incremented for INVITE requests.)
 - (2) The SS decrements its IPC when it determines that a session request is completely terminated or an established session is completely terminated.

SCM-000710 [Required: SS] The SS shall police each SC in its domain to ensure that the IPC does not exceed IPB.

- a. If IPC equals IPB, and an SC attempts to place another session by forwarding a session INVITE to its SS, the SS shall not forward the session INVITE and shall send an error message to the NMS. The caller shall receive a busy announcement as per [Section 2.9.1.2.2](#), Announcements.
- b. If IPC equals IPB at an SC, and its SS receives a session INVITE intended for that SC (either from another SC or another SS), the SS shall forward the session INVITE to the SC. If the SC accepts the session (without preempting another session so that IPC would be greater than IPB), the SS shall not forward the “session accepted” to the sessioning SC/SS, and shall send an error message to the NMS. The caller shall receive a busy announcement as per [Section 2.9.1.2.2](#), Announcements.

SCM-000720 [Required: SS] If the SS's count of an IPC is greater than or equal to the corresponding IPB, and it receives an INVITE request for a precedence session, the SS shall preempt a lower priority session (if such a session exists), and then proceed with processing the higher precedence session connect request.

SCM-000730 [Required: SS] If the SS receives a CCA-ID for which there is no entry in ASAC budget table, the SS will reject the session and generate an alarm for the NMS.

SCM-000740 [Optional: SS] SS Session Processing with Directionalization. When directionalization is implemented and applied, the SS shall police IPCi and IPCo to ensure that they do not exceed their respective budgets. The IPCi processing is independent of that for IPCo, and both are identical to that carried out for IPC in the non-directionalization case.

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

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

Since the bandwidth of a video session can vary, video sessions will be budgeted in terms of Video Session Units (VSUs). One VSU equals 500 Kbps, and bandwidth for video sessions will be allocated in multiples of VSUs. For example, the bandwidth allocated to video sessions may be 500 Kbps, 1000 Kbps, 2500 Kbps, and 4000 Kbps. Thus, a video session that requires 2500 Kbps will be allocated five VSUs, and a video session that requires 4000 Kbps will be allocated eight VSUs.

The requirements on directionalization in this section are optional.

SCM-000750 [Required: SC, SS] The SC and its corresponding SS shall be configurable with the following VSU budget (VDB): the total number of inbound and outbound VSUs plus the in-progress VSU connection attempts that an SC is allowed to have over the IP access link.

SCM-000760 [Required: SC, SS] Since video and voice services are separately allocated bandwidth, preemption of low-precedence video sessions by high-precedence voice sessions (and vice versa) shall not be implemented. Voice sessions shall strictly preempt within their allocated bandwidth, and video sessions likewise.

SCM-000770 [Required: SC] The SC processing requirements of video sessions shall be similar to its processing of VoIP sessions. For the no-directionalization case (i.e., VDBi equals VDBo equals null), the SC shall manage VSU count (VDC) to ensure that it does not exceed VDB. For the directionalization case where VDBi and VDBo are not null, the SC will manage VDCo and VDCi independently to ensure that neither one exceeds its corresponding budget. The preemption rules for video sessions are the same as for voice sessions as specified in [Section 2.26.1](#), Multilevel Precedence and Preemption. However, some extensions to the rules are required to take into account that video sessions can be of different budgets (i.e., 1, 2, 5, or

8 budgets corresponding to 500 Kbps, 1000 Kbps, 2500 Kbps, and 4000 Kbps, respectively). The following rule extensions apply to a video session request of 1, 2, 5, or 8 budgets:

- a. Preempt sessions in the process of signaling setup (progress) before preempting active sessions.
- b. Preempt the minimum number of sessions to accumulate the number of budgets needed to satisfy the video session request.
- c. 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.
- d. 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.

SCM-000780 [Required: SS] The SS processing requirements of video sessions shall be similar to its processing of VoIP sessions. For the no-directionalization case (i.e., VDBi equals VDBo equals null), the SS shall police by blocking to ensure that the respective budgets are not exceeded: VDC to ensure that it does not exceed VDB.

SCM-000790 [Required: SS] If necessary, the SS shall preempt for a session request that is at precedence level FLASH OVERRIDE or FLASH and the counts equal the budgets.

2.4 SIGNALING PROTOCOLS

SCM-000800 [Required: PEI, SC, SS] The control/management protocol between the PEI and the SC is, in general, proprietary.

SCM-000810 [Required: UEI, SC, SS] The control/management protocol between the UEI and the SC is UC SIP as specified in UC SIP 2013.

SCM-000820 [Required: SC, SS] The signaling protocol used on UC IP trunks is UC SIP as specified in UC SIP 2013.

SCM-000830 [Required: SS] The TDM-side of an SS uses DSN CCS7 signaling on CCS7-like trunks.

SCM-000840 [Required: SC, MG within the SS] The SC and the MG within the SS use DSN T1-619a PRI signaling on DSN PRI trunks.

SCM-000850 [Optional: SC, MG within the SS] The SC and the MG within the SS may support CAS trunks. CAS signaling is used on CAS trunks.

2.4.1 Signaling Performance Guidelines

Call setup times should adhere to the following guidelines:

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

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

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

2.5 REGISTRATION AND AUTHENTICATION

SCM-000860 [Required: PEI UEI, SC, SS] Registration and authentication between NEs shall follow the requirements set forth in Section 4, Information Assurance.

SCM-000870 [Conditional] If a Session Control appliance uses Network Time Protocol (NTP), then NTP version 3 shall be used and authentication shall be performed, using either of the following:

- a. Public Key Infrastructure (PKI), or, if not supported on the NTPv3 implementation used.
- b. SHA-1 hashing algorithm.

If SHA-1 is not supported by both the NTP client and server, then MD5 may be used.

2.6 SC AND SS FAILOVER

SCM-000880 [Required: SC, SS] The SCs shall be registered to a primary SS and a secondary (backup) SS. In case of failure of the primary SS, the SC will default to the secondary SS.

SCM-000890 [Required: SS] Each SS shall be provided with the VoIP Session Budgets (IPB, IPBo, IPBi) and the Video Session Budgets (VPB, VPBo, VPBi) for every SC for which the SS is the primary SS.

SCM-000900 [Required: SS] Each SS shall be provided with the VoIP Session Budgets (IPB, IPBo, IPBi) and the Video Session Budgets (VPB, VPBo, VPBi) for every SC for which the SS is a secondary SS.

SCM-000910 [Required: SC, SS] The SC and SS failover requirements make use of SUBSCRIBE and NOTIFY requests associated with the failover event package ([Section 2.6.8](#),

SIP Event Package for Failover). The failover event package is incorporated by reference into these requirements.

SCM-000920 [Required: SC, SS] The Content-type of the NOTIFY body for every NOTIFY message generated in accordance with the failover package, and therefore every NOTIFY message mandated in this section, shall be text/plain; charset=us-ascii. In other words, the Content-Type header is as follows:

Content-Type: text/plain; charset=us-ascii.

2.6.1 SC Monitors Primary SS for Status

SCM-000930 [Required: SC] The SC shall send an OPTIONS request with a Request-URI identifying the primary SS (the Request-URI does not have a userinfo part) on a configurable periodic time interval (default equals 60 seconds; minimum time interval equals 35 seconds).

SCM-000940 [Required: SS] It is NOT required that the hostname in the Request-URI of a SIP Request take the form of a fully qualified domain name (FQDN) (see UC SIP 2013, Section 4.6.8). Therefore, the hostname of the Request-URI of the OPTIONS request received by an SS may not match the SS's FQDN. This being the case, an SS that receives an OPTIONS request whose Request-URI does not have a userinfo part shall treat the OPTIONS request as being intended for the SS itself and shall respond to the OPTIONS request.

SCM-000950 [Required: SS] When a properly functioning primary SS receives the OPTIONS request from a served SC, the primary SS shall respond with a 200 (OK) response that includes the Accept header and the Supported header.

SCM-000960 [Required: SC] If one of the periodic OPTIONS requests sent by the SC either times out without a response or receives a response other than 200 OK (e.g., 408 (Request Time-Out), 500 (Server Internal Error), 503 (Service Unavailable), 504 (Server Time-Out)) the SC waits a short configurable time interval (default equals 1 to 10 seconds) and sends a second OPTIONS request.

NOTE: If the SC fails to receive a 200 (OK) response for this second OPTIONS request, then the SC concludes that the primary SS currently is unreachable.

SCM-000970 [Required: SC] The OPTIONS requests sent by the SC shall include a route set composed of two Route Headers, where the first Route Header is the SIP Universal Resource Identifier (URI) for the SBC at the enclave, and the second Route Header is the SIP URI for the SBC serving the primary SS.

SCM-000980 [Required: SC] Whenever the SC sends an INVITE request to its SBC and receives a 408 (Request Time-Out) or 504 (Server Time-Out) response and the SC is not already awaiting a response to a pending OPTIONS request, then the SC shall immediately send an OPTIONS request with a Request-URI identifying the primary SS (the Request-URI does not have a userinfo part).

SCM-000990 [Required: SC] The SC shall be capable of sending periodic OPTIONS requests to the primary SS, or to both the primary and secondary SSs via a configuration setting.

2.6.2 Primary SS Monitors SC for Status

SCM-001000 [Required: SS] The primary SS shall send an OPTIONS request to each of its served SCs on a configurable periodic time interval (default equals 240 seconds; minimum time interval equals 60 seconds). Each OPTIONS request shall have a Request-URI identifying the intended SC (the Request-URI does not have a userinfo part). The Primary SS shall maintain this configurable periodic time interval on either a per-homed-SC basis (one interval for each homed SC), or on an all-homed-SCs basis (one time interval for all homed SCs).

SCM-001010 [Required: SC] It is NOT required that the hostname in the Request-URI of a SIP Request take the form of an FQDN (see UC SIP 2013, Section 4.6.8). Therefore, the hostname of the Request-URI of the OPTIONS request received by an SC may not match the SC's FQDN. This being the case, an SC that receives an OPTIONS request whose Request-URI does not have a userinfo part shall treat the OPTIONS request as being intended for the SC itself and shall respond to the OPTIONS request.

SCM-001020 [Required: SC] When a properly functioning SC receives the OPTIONS request from its primary SC, the SC shall respond with a 200 (OK) response that includes the Accept header and the Supported header.

SCM-001030 [Required: SS] If one of the periodic OPTIONS requests sent by the primary SS to a served SC either times out without a response or receives a response other than a 200 (OK) (e.g., 408 (Request Time-Out), 500 (Server Internal Error), 503 (Service Unavailable), 504 (Server Time-Out)), the primary SS waits a short configurable time interval (default equals 1 to 10 seconds) and sends a second OPTIONS request. If this second OPTIONS request succeeds, then the primary SS returns to sending the OPTIONS requests on the periodic schedule. If this second OPTIONS request fails, then the primary SS again waits a short configurable time interval (default equals 1 to 10 seconds) and sends a third OPTIONS request.

NOTE: If the primary SS again fails to receive a 200 (OK) response from the SC for this third OPTIONS request, then the primary SS concludes that the given SC is unreachable currently.

SCM-001040 [Required: SS] Each OPTIONS request sent by the primary SS shall include a route set composed of two Route Headers, where the first Route Header is the SIP URI for the SBC serving the primary SS and the second Route Header is the SIP URI for the SBC at the SC enclave.

2.6.3 Each SS Monitors All Other SSs in the Network

SCM-001050 [Required: SS] Each SS shall send an OPTIONS request to every other SS (with the exception of its own paired SS) on a "standard" configurable periodic time interval (default

equals 90 seconds; minimum time interval equals 35 seconds). In each OPTIONS request, the Request-URI identifies the destination SS (the Request-URI does not have a userinfo part).

SCM-001060 [Required: SS] If one of the periodic OPTIONS requests sent by a first SS to another SS either times out without a response or receives a response other than 200 (OK) response (e.g., 408 (Request Time-Out), 500 (Server Internal Error), 503 (Service Unavailable), 504 (Server Time-Out), the first SS waits a short configurable time interval (default equals 1 to 10 seconds) and sends a second OPTIONS request.

NOTE: If the first SS fails to receive a 200 OK for this second OPTIONS request, then the first SS concludes that the target SS is unreachable currently.

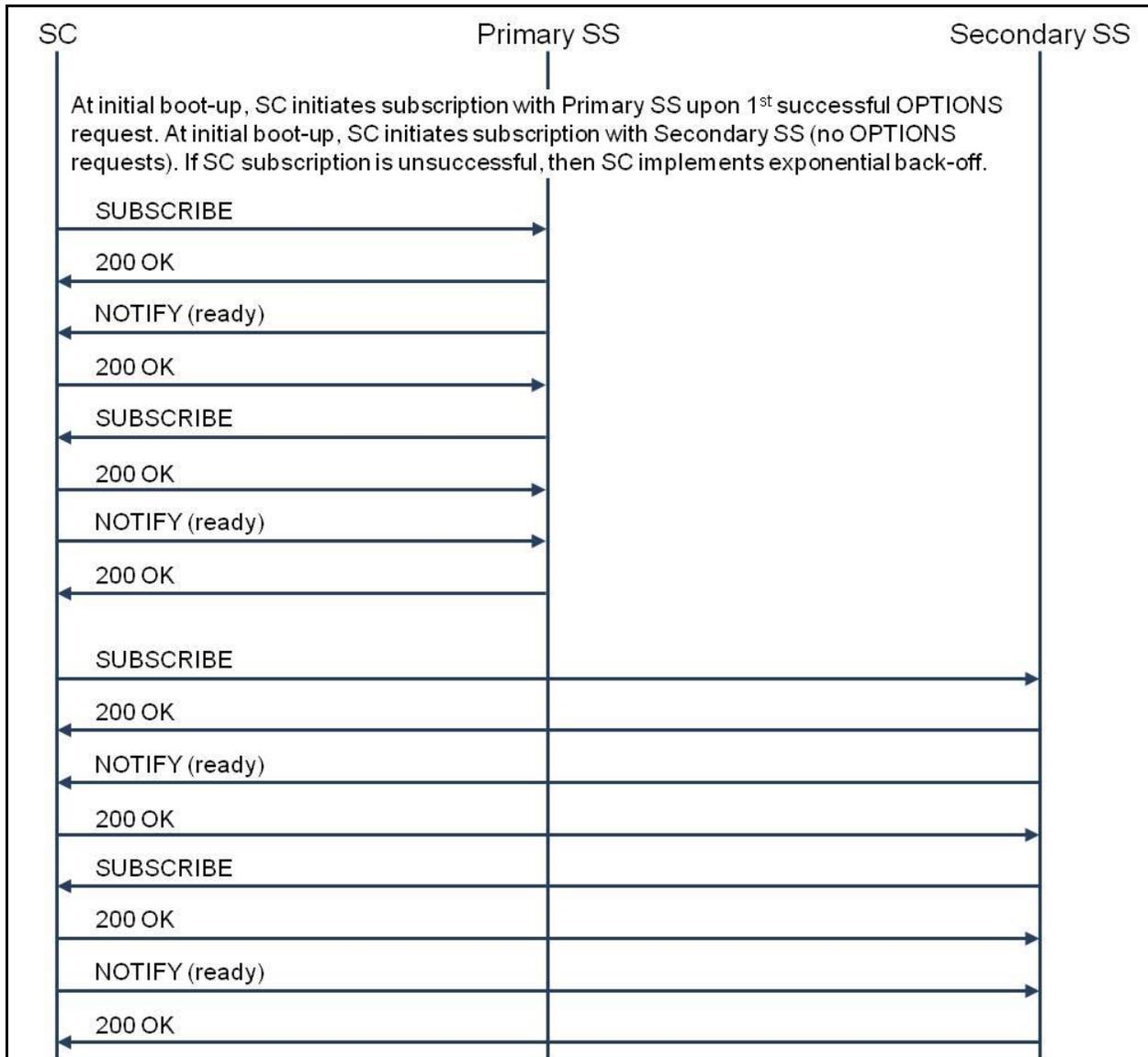
SCM-001070 [Required: SS] The OPTIONS requests shall include a route set composed of two Route Headers, where the first Route Header is the SIP URI for the SBC of the SS originating the OPTIONS request, and the second Route Header is the SIP URI for the SBC serving the destination SS.

SCM-001080 [Required: SS] When a properly functioning SS receives the OPTIONS request, the SS shall respond with a 200 (OK) response that includes the Accept header and the Supported header.

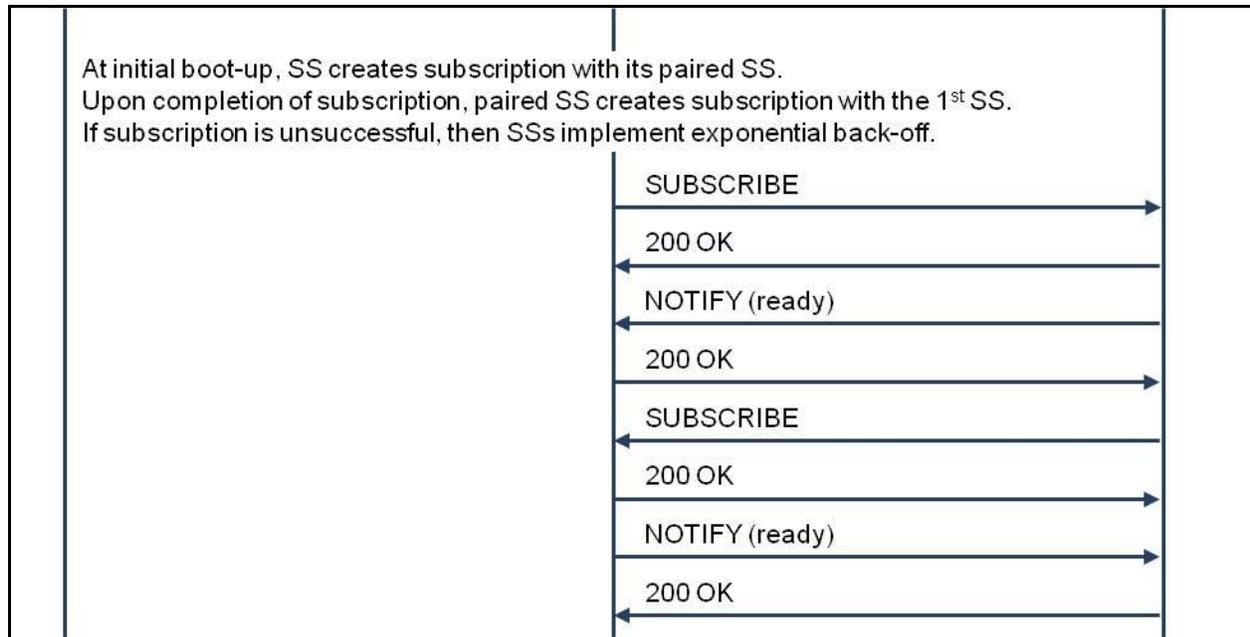
SCM-001090 [Required: SS] Whenever a first SS sends an INVITE request to another SS and receives either a 408 (Request Time-Out) or 504 (Server Time-Out) response and the first SS is not already awaiting a response to a pending OPTIONS request to the other SS, then the first SS shall immediately send an OPTIONS request with a Request-URI identifying the SS. The OPTIONS request shall include a route set composed of two Route Headers, where the first Route Header is the SIP URI for the SBC of the SS originating the OPTIONS request, and the second Route Header is the SIP URI for the SBC serving the destination SS.

2.6.4 Establish Subscriptions Using Failover Event Package

[Figure 2.6-1](#) and [Figure 2.6-2](#) depict the basic call flow for establishing subscriptions from SC to primary SS, from primary SS to SC, from SC to secondary SS, from secondary SS to SC from primary SS to secondary SS, and from secondary SS to primary SS.



**Figure 2.6-1. Call Flow Diagram for Establishing Subscriptions
Error Cases Not Included (Part 1)**



**Figure 2.6-2. Call Flow Diagram for Establishing Subscriptions
 Error Cases Not Included (Part 2)**

2.6.4.1 SC Creates Subscription With Primary SS

SCM-001100 [Required: SC] Whenever the SC boots up and the SC has no existing subscription with the primary SS, then upon the first successful OPTIONS request to the primary SS (i.e., primary SS responds with 200 (OK) response) the SC shall create a subscription with the primary SS based upon the UC event package “failover.”

SCM-001110 [Required: SC] The SC shall send a SUBSCRIBE message to the primary SS in which the Expires header shall have a value not less than 1,209,600 seconds (14 days) as per the failover event package (see [Section 2.6.8.2.1](#), Subscription Creation).

- a. **[Required: SC, SS]** If the primary SS is not ready to support the failover/failback process, then the primary SS shall respond with a 500 (Server Internal Error). Then the SC shall implement exponential back-off (see [Section 2.6.4.2](#), Exponential Back-Off).
- b. **[Required: SS]** If the primary SS is ready to support the failover/failback process, then the primary SS shall respond to the SUBSCRIBE request with a 200 (OK) response in which the Expires header shall have a value not less than 1,209,600 seconds (14 days) as per the failover event package (see [Section 2.6.8.2.1](#), Subscription Creation).
 - (1) **[Required: SS]** The primary SS shall immediately send a NOTIFY request with the body: Primary SS CCA-ID, ready, SC CCA-ID.
 - (2) **[Required: SC]** The SC shall respond with 200 (OK) response.

2.6.4.2 *Exponential Back-Off*

SCM-001120 [Required: SC, SS] In the event a subscription fails, the subscriber shall implement a subscription establishment or refresh scheme using exponential back-off starting at 30 minutes and doubling on each attempt until reaching 240 minutes (i.e., 30, 60, 120, 240). Thereafter, the time interval between subscription establishment attempts stays at 240 minutes until the subscription is completed successfully.

2.6.4.3 *Invalid NOTIFY Body*

SCM-001130 [Required: SC, SS] Whenever an SC or SS receives a NOTIFY message where the syntax does not conform to the requirements set forth in the failover event package or where the failstate parameter is not a member of the enumerated list in the failover event package, then the recipient of the NOTIFY message shall send a 400 response with the Reason-Phrase:

failover NOTIFY body invalid.

SCM-001140 [Required: SC, SS] Whenever an SC or SS receives a NOTIFY message in which either the value of the first CCA-ID field (first element) or the second CCA-ID field (third element) either is unknown to the recipient or otherwise invalid, the recipient shall send a 400 response with the Reason-Phrase: failover NOTIFY body CCA-ID field invalid.

SCM-001150 [Required: SC, SS] The text of the NOTIFY body is case insensitive. The SC and SS shall not reject a NOTIFY body simply because a character is either uppercase or lowercase.

2.6.4.4 *Primary SS Creates Subscription With SC*

SCM-001160 [Required: SS] Upon successful completion of the SC subscription with the primary SS ([Section 2.6.4.1](#), SC Creates Subscription with Primary SS) and if the primary SS has no existing subscription with the SC, then the primary SS shall immediately send a SUBSCRIBE message to the SC in which the Expires header shall have a value not less than 1,209,600 seconds (14 days) per the failover event package (see [Section 2.6.8.2.1](#), Subscription Creation).

- a. **[Required: SC]** The SC shall respond to the SUBSCRIBE message with a 200 (OK) response in which the Expires header shall have a value not less than 1,209,600 seconds (14 days) as per the failover event package (see [Section 2.6.8.2.1](#), Subscription Creation).
- b. **[Required: SC]** The SC shall immediately send a NOTIFY with the body: SC CCA-ID, ready, SC CCA-ID.
- c. **[Required: SS]** The primary SS shall respond with a 200 (OK) response.

SCM-001170 [Required: SS] In the event the subscription fails, then the primary SS uses Exponential back-off (see [Section 2.6.4.2](#), Exponential Back-Off).

2.6.4.5 *SC Creates Subscription With Secondary SS*

SCM-001180 [Required: SC] Whenever the SC boots up, and the SC has no existing subscription with the secondary SS, the SC shall create a subscription with the secondary SS based on the UC event package “failover.”

SCM-001190 [Required: SC] The SC shall send a SUBSCRIBE message to the secondary SS in which the Expires header shall have a value not less than 1,209,600 seconds (14 days) as per the failover event package (see [Section 2.6.8.2.1](#), Subscription Creation).

- a. **[Required: SC, SS]** If the secondary SS is not ready to support the failover/failback process, then the secondary SS shall respond with a 500 (Server Internal Error). Then the SC shall implement exponential back-off (see [Section 2.6.4.2](#), Exponential Back-Off).
- b. **[Required: SS]** If the secondary SS is ready to support the failover/failback process, then the primary SS shall respond to the SUBSCRIBE message with a 200 (OK) response in which the Expires header shall have a value not less than 1,209,600 seconds (14 days) as per the failover event package (see [Section 2.6.8.2.1](#), Subscription Creation).
 - (1) **[Required: SS]** The secondary SS shall immediately send a NOTIFY with the body: Secondary SS CCA-ID, ready, SC CCA-ID.
 - (2) **[Required: SC]** The SC shall respond with 200 (OK) response.

2.6.4.6 *Secondary SS Creates Subscription With SC*

SCM-001200 [Required: SS] Upon successful completion of the SC subscription with the secondary SS (see [Section 2.6.4.5](#), SC Creates Subscription With Secondary SS) and if the secondary SS has no existing subscription with the SC, the secondary SS shall immediately send a SUBSCRIBE message to the SC in which the Expires header shall have a value not less than 1,209,600 seconds (14 days) as per the failover event package (see [Section 2.6.8.2.1](#), Subscription Creation).

SCM-001210 [Required: SC] The SC shall respond to the SUBSCRIBE message with a 200 (OK) response in which the Expires header shall have a value not less than 1,209,600 seconds (14 days) as per the failover event package (see [Section 2.6.8.2.1](#), Subscription Creation).

SCM-001220 [Required: SC] The SC shall immediately send a NOTIFY with body: SC CCA-ID, ready, SC CCA-ID.

SCM-001230 [Required: SS] The secondary SS shall respond with a 200 (OK) response.

SCM-001240 [Required: SS] In the event the subscription fails, then the secondary SS uses exponential back-off (see [Section 2.6.4.2](#), Exponential Back-Off).

2.6.4.7 Paired Softswitches (Active Primary/Secondary) Create Subscriptions With One Another

SCM-001250 [Required: SS] Whenever an SS boots up and the SS does not have an existing subscription with its paired SS, then the SS creates a subscription with the paired SS based on the UC event package “failover.”

SCM-001260 [Required: SS] The SUBSCRIBE message shall include an Expires header that has a value not less than 1,209,600 seconds (14 days) as per the failover event package (see [Section 2.6.8.2.1](#), Subscription Creation).

- a. **[Required: SS]** If the paired SS is not ready to support the failover/failback process, then the paired SS shall respond with a 500 (Server Internal Error). Then the SS implements exponential back-off (see [Section 2.6.4.2](#), Exponential Back-Off).
- b. **[Required: SS]** If the paired SS is ready to support the failover/failback process, then the paired SS shall respond to the SUBSCRIBE message with a 200 (OK) response in which the Expires header shall have a value not less than 1,209,600 seconds (14 days) as per the failover event package (see [Section 2.6.8.2.1](#), Subscription Creation).
 - (1) **[Required: SS]** The paired SS shall immediately send a NOTIFY message with body: Paired SS CCA-ID, ready, all.
 - (2) **[Required: SS]** The SS shall respond with a 200 (OK) response.
 - (3) **[Required: SS]** If the paired SS does not have a subscription with the peer SS, then the paired SS shall immediately create a new subscription with its peer per this section.

2.6.5 Subscription Refresh

2.6.5.1 SC Refreshes Subscription With Primary SS

SCM-001270 [Required: SC] The SC shall refresh the subscription with the primary SS at between 864,000 seconds (10 days) and 950,400 seconds (11 days) so that the subscription does not lapse. The Expires header of the SUBSCRIBE message shall have a value not less than 1,209,600 seconds (14 days) as per the failover event package (see [Section 2.6.8.2.1](#), Subscription Creation, and [Section 2.6.8.2.2](#), Subscription Duration).

- a. **[Required: SC, SS]** If for some reason the primary SS is unable to support the subscription refresh, then the primary SS shall respond with a 500 (Server Internal Error) response. Then the SC shall implement exponential back-off (see [Section 2.6.4.2](#), Exponential Back-Off).
- b. **[Required: SS]** If the primary SS is ready to support the subscription refresh, then the primary SS shall respond to the SUBSCRIBE message with a 200 (OK) in which the

Expires header shall have a value not less than 1,209,600 seconds (14 days) as per the failover event package (see [Section 2.6.8.2.1](#), Subscription Creation).

- (1) **[Required: SS]** The primary SS shall immediately send a NOTIFY message with the body: Primary SS CCA-ID, ready, SC CCA-ID
- (2) **[Required: SC]** The SC shall respond with a 200 (OK) response.

SCM-001280 [Required: SC] If the SC is unable to refresh the subscription before the subscription expires, then the SC shall create a new subscription as if the SC were booting up for the first time (see [Section 2.6.4.1](#), SC Creates Subscription With Primary SS).

2.6.5.2 Primary SS Refreshes Subscription With SC

SCM-001290 [Required: SC, SS] Upon successful completion of the SC subscription refresh with the primary SS, the primary SS shall immediately refresh its subscription with the SC so that the subscription does not lapse. The Expires header of the SUBSCRIBE message shall have a value not less than 1,209,600 seconds (14 days) as per the failover event package (see [Section 2.6.8.2.1](#), Subscription Creation). The SC shall respond to the SUBSCRIBE with a 200 (OK) response in which the Expires header shall have a value not less than 1,209,600 seconds (14 days) as per the failover event package (see [Section 2.6.8.2.1](#), Subscription Creation).

- a. **[Required: SC]** The SC shall immediately send a NOTIFY request with the body: SC CCA-ID, ready, SC CCA-ID
- b. **[Required: SS]** The primary SS shall respond with a 200 (OK) response.

SCM-001300 [Required: SS] In the event the subscription refresh fails, then the primary SS shall use exponential back-off (see [Section 2.6.4.2](#), Exponential Back-Off).

SCM-001310 [Required: SS] If the primary SS is unable to refresh the subscription before the subscription expires, then the primary SS shall create a new subscription (see [Section 2.6.4.4](#), Primary SS Creates Subscription With SC.)

SCM-001320 [Required: SS] If the current subscription with the SC exceeds 950,400 seconds (11 days) and the SC has not conducted a subscription refresh with the primary SS, then the primary SS shall refresh its subscription with the SC.

2.6.5.3 SC Refreshes Subscription With Secondary SS

SCM-001330 [Required: SC] The SC shall refresh the subscription with the secondary SS at between 864,000 seconds (10 days) and 950,400 seconds (11 days) so that the subscription does not lapse. The Expires header of the SUBSCRIBE message shall have a value not less than 1,209,600 seconds (14 days) as per the failover event package (see [Section 2.6.8.2.1](#), Subscription Creation, and [Section 2.6.8.2.2](#), Subscription Duration).

- a. **[Required: SC, SS]** If for some reason the secondary SS is unable to support the subscription refresh, then the secondary SS shall respond with a 500 (Server Internal

Error). Then the SC implements exponential back-off (see [Section 2.6.4.2](#), Exponential Back-Off).

- b. **[Required: SS]** If the secondary SS is ready to support the subscription refresh, then the secondary SS shall respond to the SUBSCRIBE message with a 200 (OK) response in which the Expires header shall have a value not less than 1,209,600 seconds (14 days) as per the failover event package (see [Section 2.6.8.2.1](#), Subscription Creation).
 - (1) **[Required: SS]** The secondary SS shall immediately send a NOTIFY request with the body: Secondary SS CCA-ID, ready, SC CCA-ID
 - (2) **[Required: SC]** The SC shall respond with a 200 (OK) response.

SCM-001340 [Required: SC] If the SC is unable to refresh the subscription before the subscription expires, then the SC shall create a new subscription as if the SC were booting up for the first time (see [Section 2.6.4.5](#), SC Creates Subscription With Secondary SS).

2.6.5.4 Secondary SS Refreshes Subscription With SC

SCM-001350 [Required: SC, SS] Upon successful completion of the SC subscription refresh with the secondary SS, the secondary SS shall immediately refresh its subscription with the SC so that the subscription does not lapse . The Expires header of the SUBSCRIBE message shall have a value not less than 1,209,600 seconds (14 days) as per the failover event package (see [Section 2.6.8.2.1](#), Subscription Creation). The SC shall respond to the SUBSCRIBE with a 200 (OK) response in which the Expires header shall have a value not less than 1,209,600 seconds (14 days) as per the failover event package (see [Section 2.6.8.2.1](#), Subscription Creation).

- a. **[Required: SC]** The SC shall immediately send a NOTIFY request with the body: SC CCA-ID, ready, SC CCA-ID.
- b. **[Required: SS]** The secondary SS shall respond with a 200 (OK) response.

SCM-001360 [Required: SS] In the event the subscription refresh fails, then the secondary SS shall use exponential back-off (see [Section 2.6.4.2](#), Exponential Back-Off).

SCM-001370 [Required: SS] If the secondary SS is unable to refresh the subscription before the subscription expires, then the secondary SS shall create a new subscription (see [Section 2.6.4.6](#), Secondary SS Creates Subscription With SC).

SCM-001380 [Required: SS] If the current subscription with the SC exceeds 950,400 seconds (11 days) and the SC has not conducted a subscription refresh with the secondary SS, then the secondary SS shall refresh its subscription with the SC.

2.6.5.5 SS Refreshes Subscription With Its Paired SS

SCM-001390 [Required: SS] An SS shall refresh the subscription with its paired SS at between 864,000 seconds (10 days) and 950,400 seconds (11 days) so that the subscription does not lapse. The Expires header of the SUBSCRIBE message shall have a value not less than 1,209,600

seconds (14 days) as per the failover event package (see [Section 2.6.8.2.1](#), Subscription Creation, and [Section 2.6.8.2.2](#), Subscription Duration).

- a. **[Required: SS]** If the paired SS is not ready to support the failover/failback process, then the paired SS shall respond with a 500 (Server Internal Error). In the event the subscription refresh fails, then the SS shall use Exponential back-off (see [Section 2.6.4.2](#), Exponential Back-Off).
- b. **[Required: SS]** If the paired SS is ready to support the failover/failback process, then the paired SS shall respond to the SUBSCRIBE message with a 200 (OK) response in which the Expires header shall have a value not less than 1,209,600 seconds (14 days) as per the failover event package (see [Section 2.6.8.2.1](#), Subscription Creation).
 - (1) **[Required: SS]** The paired SS shall immediately send a NOTIFY request with the body: Paired SS CCA-ID, ready, all
 - (2) **[Required: SS]** The SS shall respond with a 200 (OK) response.
 - (3) **[Required: SS]** If the paired SS either has no subscription or has an expired subscription with the peer SS, then the paired SS shall immediately create a new subscription with its peer per [Section 2.6.4.7](#), Paired Softswitches (Active Primary/Secondary) Create Subscriptions With One Another.
 - (4) **[Required: SS]** If the paired SS has a subscription with its peer SS that is already beyond 950,400 seconds (11 days), then the paired SS shall immediately refresh its subscription with its peer per [Section 2.6.5.5](#), SS Refreshes Subscription With Its Paired SS.

SCM-001400 [Required: SS] If the SS is unable to refresh the subscription before the subscription expires, then the SS shall create a new subscription as if the SS were booting up for the first time (see [Section 2.6.4.7](#), Paired Softswitches (Active Primary/Secondary) Create Subscriptions With One Another).

2.6.6 SC Failover to Secondary SS

[Figure 2.6-3](#) depicts the basic call flow for SC failover from the primary SS to the secondary SS.

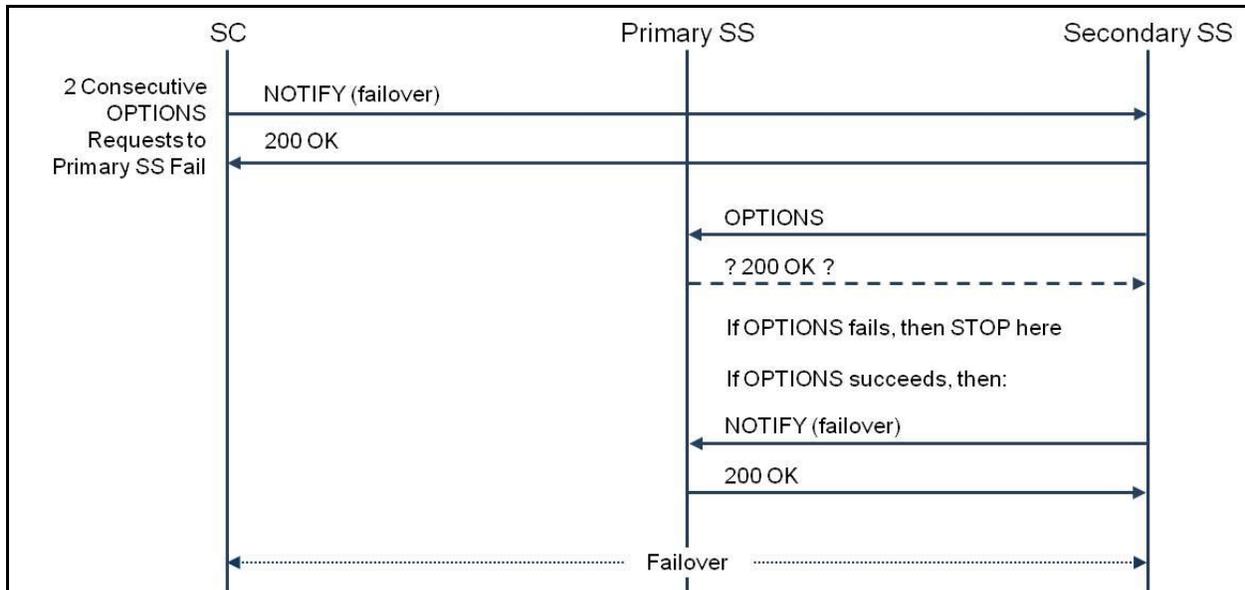


Figure 2.6-3. Call Flow Diagram for SC Failover Error Cases Not Included

SCM-001410 [Required: SC, SS] When the SC sends to the primary SS a defined configurable number of successive OPTIONS requests (default equals 2) for which there either is no response or a response other than 200 OK [e.g., 408 (Request Time-Out), 500 (Server Internal Error), 503 (Service Unavailable), 504 (Server Time-Out)], then the following steps are taken:

- a. Step 1 [**Required: SC**] The SC shall send a NOTIFY request to the secondary SS with the body: SC CCA-ID, failover, SC CCA-ID.
 - (1) [**Required: SS**] If the secondary SS recognizes the NOTIFY request as belonging to an active subscription with the SC, then the secondary SS shall respond with 200 (OK) response.
 - (a) [**Required: SC**] The SC shall send all new outbound SIP messages (with the exception of OPTIONS requests destined for the primary SS) to the secondary SS.
 - (b) [**Required: SC**] The SC shall wait a configurable time interval (default equals 30–60 minutes), and then resume sending OPTIONS requests to the primary SS per [Section 2.6.1](#), SC Monitors Primary SS for Status. However, if the SC receives an inbound INVITE message from the primary SS before sending an OPTIONS request to the primary SS, then the SC shall immediately send an OPTIONS request to the primary SS in response to the receipt of the inbound INVITE message. (See Step 1, [Section 2.6.7](#), SC Failback to Primary SS).
 - (c) [**Required: SBC**] The SBC serving the secondary SS shall respond with a 481 (Call/Transaction Does Not Exist) response upon receipt of any Re-INVITE, UPDATE, or BYE request from the SC that relates to an existing call that had been established through the primary SS.

- (d) **[Required: SC]** All outbound UC SIP requests sent by the SC to its SBC (with the exception of OPTIONS requests) shall include a route set composed of two Route headers, where the first Route header is the SIP URI for the SBC at the enclave, and the second Route header is the SIP URI for the SBC serving the secondary SS.

Proceed to Step 2.

- (2) **[Required: SC, SS]** If the secondary SS does NOT recognize the “failover” NOTIFY request of Step 1 as belonging to an active subscription with the SC, then the secondary SS shall respond with a 481 (Subscription Does Not Exist) and the SC shall begin the subscription refresh process by refreshing its existing subscription with the secondary SS.

- (a) **[Required: SC, SS]** If the SC’s subscription refresh with the secondary SS is successful, then the secondary SS shall immediately initiate a subscription with the SC. Upon completion of the secondary SS’s subscription with the SC, the SC immediately sends a NOTIFY request to the secondary SS with the body: SC CCA-ID, failover, SC CCA-ID.

- i. **[Required: SS]** The secondary SS shall respond with 200 (OK) response. The requirements set forth in Step 1.a apply. The secondary SS proceeds to Step 2.

- ii. **[Required: SC]** If the secondary SS does NOT respond with a 200 (OK) response and the NOTIFY message either times out or the secondary SS responds with a failure response, then the SC immediately sends a second “failover” NOTIFY message.

- (i) **[Required: SC, SS]** If the secondary SS responds with 200 (OK) response, then failover shall occur and the requirements set forth in Step 1.a apply. The secondary SS proceeds to Step 2.

- (ii) **[Required: SC]** If the secondary SS does NOT respond with a 200 (OK) response and the NOTIFY message either times out or the secondary SS responds with a failure response, then the SC is isolated from both the primary SS and secondary SS. The SC shall continue to send OPTIONS requests to the primary SS per [Section 2.6.1](#), SC Monitors Primary SS for Status, and the SC shall wait 60–120 seconds and return to Step 1.

- (iii) **[Required: SC, SS]** If the SC receives a 200 (OK) response from the primary SS before being able to successfully send the “failover” NOTIFY to the secondary SS, then the SC terminates the failover process. Failover does NOT occur.

- (b) **[Required: SC, SS]** If the SC’s SUBSCRIBE request for the subscription refresh with the secondary SS (in 1.b) results in a 481 (Subscription does not exist) response from the secondary SS, then the SC shall consider its current

subscription with the secondary SS to be invalid and shall establish a new subscription with the secondary SS. Upon completion of the SC's new subscription with the secondary SS, the secondary SS shall immediately establish a subscription with the SC. Upon completion of the secondary SS's subscription with the SC, the SC shall send a NOTIFY request to the secondary SS with the body: SC CCA-ID, failover, SC CCA-ID.

- i. **[Required: SS]** The secondary SS shall respond with 200 (OK) response. The requirements set forth in Step 1.a apply. The secondary SS proceeds to Step 2.
 - ii. **[Required: SC]** If the secondary SS does NOT respond with a 200 (OK) response and the NOTIFY message either times out or the secondary SS responds with a failure response, then the SC immediately sends a second "failover" NOTIFY message.
 - (i) **[Required: SC, SS]** If the secondary SS responds with 200 (OK) response, then failover shall occur and the requirements set forth in Step 1.a. apply. The secondary SS proceeds to Step 2.
 - (ii) **[Required: SC]** If the secondary SS does NOT respond with a 200 (OK) response and the NOTIFY message either times out or the secondary SS responds with a failure response, then the SC is isolated from both the primary SS and secondary SS. The SC shall continue to send OPTIONS requests to the primary SS per [Section 2.6.1](#), SC Monitors Primary SS for Status, and the SC shall wait 60–120 seconds and return to Step 1.
 - (iii) **[Required: SC, SS]** If the SC receives a 200 (OK) response from the primary SS before being able to successfully send the "failover" NOTIFY message to the secondary SS, then the SC terminates the failover process. Failover does NOT occur.
- (3) **[Required: SC]** If the secondary SS either does not provide a response to the "failover" NOTIFY request of Step 1 or provides a failure response other than 481 (Subscription Does Not Exist), then the SC immediately sends a second "failover" NOTIFY message.
- (a) **[Required: SC, SS]** If the secondary SS responds with a 200 (OK) response, then failover shall occur and the requirements of Step 1.a apply. The secondary SS proceeds to Step 2.
 - (b) **[Required: SC]** If the secondary SS does NOT respond with a 200 (OK) response and the NOTIFY message either times out or the secondary SS responds with a failure response, then the SC is isolated from both the primary SS and secondary SS. The SC shall continue to send OPTIONS requests to the primary SS per [Section 2.6.1](#), SC Monitors Primary SS for Status, and the SC shall wait 60–120 seconds and return to Step 1.

-
- i. **[Required: SC, SS]** If the SC receives a 200 (OK) response from the primary SS before being able to successfully send the “failover” NOTIFY message to the secondary SS, then the SC terminates the failover process. Failover does NOT occur.
 - b. Step 2 **[Required: SS]** Upon responding to the “failover” NOTIFY message from the SC with a 200 (OK), the Secondary SS shall immediately send an OPTIONS request to the primary SS to determine whether the primary SS is reachable at the SIP layer from the secondary SS.
 - (1) **[Required: SS]** If the primary SS responds with a 200 (OK) response, then the secondary SS shall send a NOTIFY message to the primary SS with a body that has the following content: Secondary SS CCA-ID, failover, SC CCA-ID.
 - (a) **[Required: SS]** If the primary SS responds with 200 (OK) response, then the primary SS shall forward all inbound UC SIP messages intended for the designated SC to the secondary SS.
 - i. **[Required: SBC]** The SBC serving the secondary SS shall respond with a 481 (Call/Transaction Does Not Exist) response upon receipt of any Re-INVITE, UPDATE, or BYE request from the primary SS that relates to a call that is not established through the secondary SS.

Failover is complete; STOP here.

- (b) **[Required: SS]** If the primary SS responds to the “failover” NOTIFY message from the secondary SS (Step 2.a) with a 481 (Subscription Does Not Exist), then the secondary SS shall refresh its existing subscription with the primary SS.
 - i. **[Required: SS]** If the secondary SS’s subscription refresh with the primary SS is successful, then the primary SS shall immediately initiate a subscription with the secondary SS. Upon completion of the primary SS’s subscription with the secondary SS, the secondary SS immediately sends a NOTIFY message to the primary SS with the body: Secondary SS CCA-ID, failover, SC CCA-ID.
 - (i) **[Required: SC, SS]** If the primary SS response is 200 (OK) response, then failover occurs per Step 2.a.1.
 - ii. **[Required: SS]** If the primary SS response to the SUBSCRIBE request (for the subscription refresh of step 2.a.2) is 481 (Subscription Does Not Exist), then the secondary SS shall consider its current subscription with the primary SS to be invalid and shall establish a new subscription with the primary SS. Upon completion of the secondary SS’s new subscription with the primary SS, the primary SS shall immediately establish a subscription with the secondary SS. Upon completion of the primary SS’s subscription with the secondary SS,

the secondary SS shall send a NOTIFY message to the primary SS with the body: Secondary SS CCA-ID, failover, SC CCA-ID.

- (i) **[Required: SS]** The primary SS shall respond with 200 (OK) response and the failover occurs per Step 2.a.1.
- (2) **[Required: SS]** If the OPTIONS request of Step 2 fails, then the secondary SS shall wait 5–10 seconds and shall send a second OPTIONS request to the primary SS.
 - (a) **[Required: SS]** If the second OPTIONS request also fails, then the primary SS is deemed unreachable from the secondary SS as well as from all other SSs. As the other SSs discover that the primary SS is inaccessible, they will begin sending UC SIP messages intended for the SCs served by the primary SS to the secondary SS instead. Failover is complete; STOP here.
 - (b) **[Required: SS]** If the second OPTIONS request succeeds, then the secondary SS shall send a NOTIFY message to the primary SS with a body that has the following content: Secondary SS CCA-ID, failover, SC CCA-ID.
 - i. **[Required: SS]** Upon receipt of the NOTIFY message from the secondary SS, the primary SS shall respond with a 200 (OK) response and forward all inbound UC SIP messages intended for the designated SC to the secondary SS. Failover is complete.

2.6.6.1 SSs Failover to Secondary SS

SCM-001420 [Required: SS] Each SS shall be configured with knowledge of every pair of SSs in the network that act as secondary (backup) SS for one another.

SCM-001430 [Required: SS] When an SS sends a defined configurable number of successive OPTIONS requests (default equals 2) to another SS (let's say SS B) (that is NOT its paired secondary SS) that either times out or receives a failure response—as opposed to 200 (OK) response (e.g., 408 Request Time-Out), 500 (Server Internal Error), 503 (Service Unavailable), or 504 (Server Time-Out), then:

- a. **[Required: SS]** The first SS shall send all INVITE requests corresponding to new call requests intended for SCs served by the failed SS to the paired secondary SS of the failed SS instead. The UC SIP requests shall include a route set composed of two Route headers, where the first Route header is the SIP URI for the SBC at the first SS, and the second Route header is the SIP URI for the SBC serving the paired secondary SS of the failed SS.
- b. **[Required: SS]** The first SS shall continue to send OPTIONS requests to the failed SS as per the requirements of [Section 2.6.3](#), Each SS Monitors All Other SSs in the Network. The OPTIONS requests include a route set composed of two Route headers, where the first Route header is the SIP URI for the first SS, and the second Route header is the SIP URI for the SBC serving the failed SS.

- c. **[Required: SS]** The first SS shall continue to send UC SIP messages associated with sessions established through the failed SS to the failed SS. The SIP requests shall include a route set composed of two Route headers, where the first Route header is the SIP URI for the SBC at the first SS, and the second Route header is the SIP URI for the SBC serving the paired secondary SS of the failed SS.
- d. **[Required: SBC]** If the first SS incorrectly attempts to forward a SIP request message to the secondary SS for a session that was established using the failed SS, then the SBC serving the secondary SS shall respond with a 481 (Call/Transaction Does Not Exist).

SCM-001440 [Required: SS] If the first SS receives a 200 (OK) response to an OPTIONS request from SS B before the configurable number of successive failures to the OPTIONS requests (default equals 2) has been reached, then no action is taken to failover to the paired SS. For example, using the default of two successive failures, if one OPTIONS request to the SS fails, then the next OPTIONS request receives a 200 (OK) response, no action is taken to failover to the secondary (backup) SS.

2.6.6.2 Failover to Secondary SS Triggered by Primary SS

SCM-001450 [Required: SS] When the primary SS sends to a served SC a defined configurable number of successive OPTIONS requests (default equals 3) for which there either is no response or a response other than 200 OK response (e.g., 408 (Request Time-Out), 500 (Server Internal Error), 503 (Service Unavailable), 504 (Server Time-Out)), then the following occurs:

- a. **[Required: SS]** The primary SS shall send a NOTIFY message to the secondary SS with the body: Primary CCA-ID, SCunreachable, SC CCA-ID
- b. **[Required: SS]** The secondary SS shall respond with a 200 (OK) response.
- c. **[Required: SS]** The secondary SS shall send a NOTIFY message to the SC with the body: Secondary CCA-ID, SCunreachable, SC CCA-ID
- d. **[Required: SC]** The SC shall respond with a 200 (OK) response and initiate SC failover per [Section 2.6.6](#), SC Failover to Secondary SS.

2.6.7 SC Failback to Primary SS

[Figure 2.6-4](#) depicts the basic call flow for SC failback to the primary SS from the secondary SS.

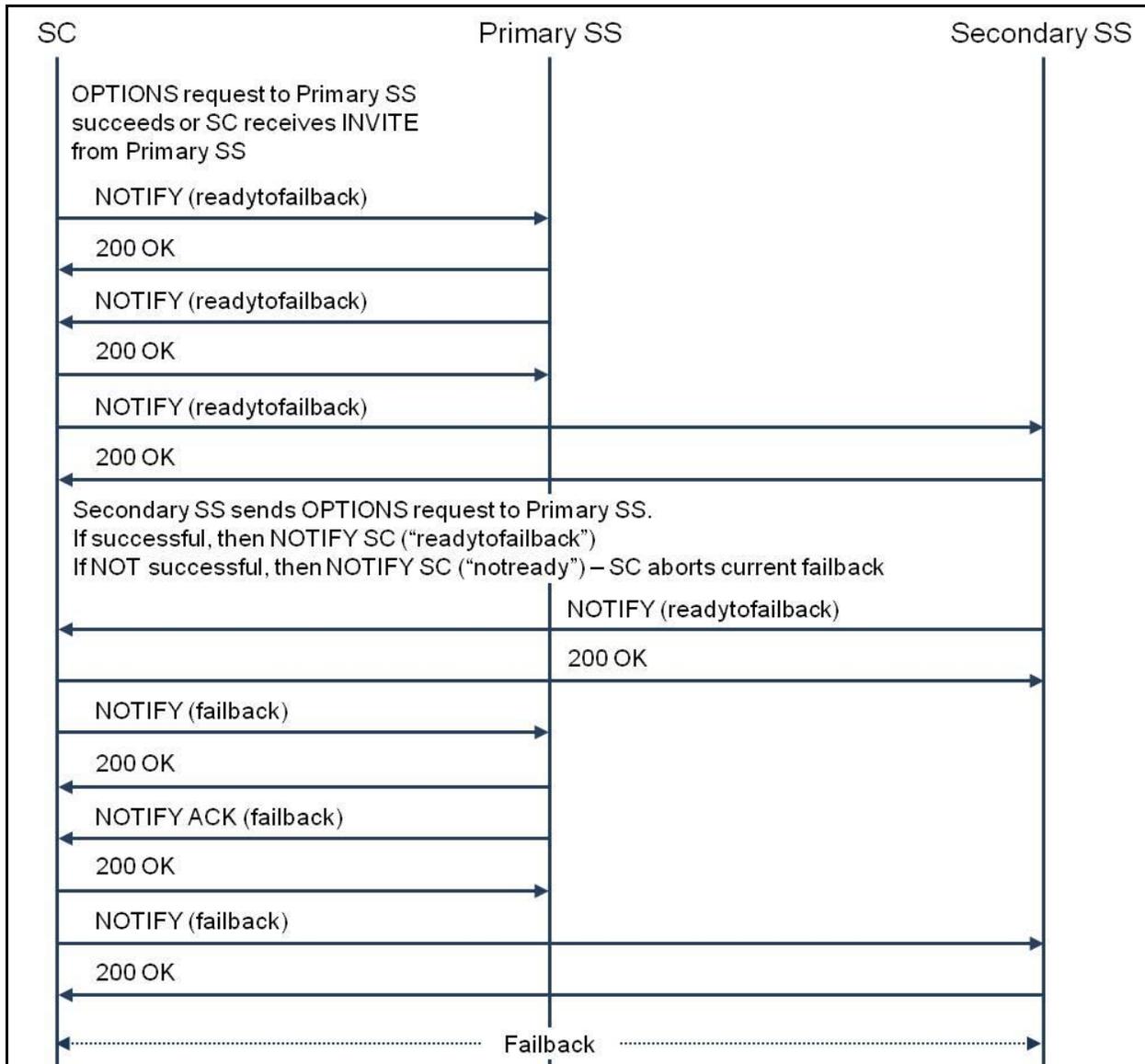


Figure 2.6-4. Call Flow Diagram for SC Failback Error Cases Not Included

SCM-001460 [Required: SC] Per [Section 2.6.6](#), SC Failover to Secondary SS, Step 1.a, upon successful SC failover to the secondary SS, the SC waits a configurable amount of time (default equals 30–60 minutes) before sending an OPTIONS request to the primary SS UNLESS the SC receives an inbound INVITE request from the primary SS .

- a. Step 1 **[Required: SC]** If the SC receives an inbound INVITE request from the primary SS, then the SC immediately sends an OPTIONS request to the primary SS per the requirements of [Section 2.6.1](#), SC Monitors Primary SS for Status.

NOTE: The SC does not complete inbound INVITE processing until the failback process has completed. It is possible that the INVITE message will time out.

- (1) [**Required: SC**] The OPTIONS requests sent by the SC shall include a route set composed of two Route headers, where the first Route header is the SIP URI for the SBC at the enclave, and the second Route header is the SIP URI for the SBC serving the primary SS.

SCM-001470 [**Required: SC**] When the SC receives a 200 (OK) response to an OPTIONS request from the primary SS, the SC shall send a NOTIFY message to the primary SS with the body: SC CCA-ID, readytofailback, SC CCA ID.

- a. Step 2 [**Required: SS**] Assuming the primary SS subscription with the SC is active, then the primary SS shall respond with a 200 (OK) response and send a NOTIFY message to the SC with the body: primary SS CCA-ID, readytofailback, SC CCA ID.
 - (1) [**Required: SC**] The SC responds with a 200 (OK) response and proceeds to Step 3.
 - (2) [**Required: SC**] If the primary SS responds to the SC's "readytofailback" NOTIFY message (of Step 2) with a 481 (Subscription Does Not Exist), then the SC shall initiate the subscription refresh process by refreshing its existing subscription with the secondary SS.
 - (a) [**Required: SC, SS**] If the SC's subscription refresh with the primary SS is successful, then the primary SS shall immediately refresh its subscription with the SC. Upon completion of the primary SS's subscription with the SC, the SC immediately sends a NOTIFY message to the primary SS with the body: SC CCA-ID, readytofailback, SC CCA-ID
 - i. [**Required: SC, SS**] If the primary SS responds with a 200 (OK) response, then proceed to Step 3.
 - ii. [**Required: SC**] If the NOTIFY message times out or if the primary SS does not respond with a 200 (OK) response, then the primary SS is not ready for failback and the SC shall return to Step 1.

NOTE: The SC again waits a configurable amount of time (30–60 minutes) before sending an OPTIONS request.

- (b) [**Required: SC, SS**] If the SC's SUBSCRIBE (for subscription refresh) (from Step 2.b) sent to the primary SS receives a 481 (Subscription Does Not Exist) response, then the SC shall consider its current subscription with the primary SS to be invalid and shall establish a new subscription with the primary SS. Upon completion of the SC's new subscription with the primary SS, the primary SS shall immediately establish a new subscription with the SC. Upon completion of the primary SS's subscription with the SC, the SC shall send a NOTIFY message to the primary SS with the body: SC CCA-ID, readytofailback, SC CCA-ID.
 - i. [**Required: SC, SS**] If the primary SS responds with a 200 (OK) response, then proceed to Step 3.

- ii. [**Required: SC**] If the primary SS does not respond with a 200 (OK) response, then the primary SS is not ready for failback and the SC shall return to Step 1.

NOTE: The SC again waits a configurable amount of time (30–60 minutes) before sending an OPTIONS request.

- (3) [**Required: SC**] If the SC's "readytofailback" NOTIFY message times out or if the primary SS does not respond with 200 (OK) response [or with a 481 (Subscription Does Not Exist)], then the primary SS is not ready for failback and the SC shall return to Step 1.

NOTE: The SC again waits a configurable amount of time (30–60 minutes) before sending an OPTIONS request.

b. Step 3.

- (1) [**Required: SS**] If the primary SS is ready to resume servicing the SC (or if the primary SS was unaware of the SC failover), then the primary SS sends a NOTIFY message to the SC with the body: Primary SS CCA-ID, readytofailback, SC CCA-ID.

(a) [**Required: SC**] The SC shall send a 200 (OK) response and proceed to Step 4.

- (2) [**Required: SC**] If the SC does NOT receive either a "readytofailback" NOTIFY message or a "notready" NOTIFY message from the primary SS within 60 seconds of receipt of the primary SS's 200 OK to the SC's "readytofailback" NOTIFY request, then the SC shall abort the failback procedure and return to Step 1.

NOTE: The SC again waits a configurable amount of time (30–60 minutes) before sending an OPTIONS request.

- (3) [**Required: SS**] If the primary SS is NOT ready to resume servicing the SC, then the primary SS shall send a NOTIFY message to the SC with the body:

Primary SS CCA-ID, notready, SC CCA-ID.

(a) [**Required: SC**] The SC sends a 200 (OK) response.

- (b) [**Required: SC**] If the triggering event for the failback had been receipt of an INVITE request from the primary SS and the primary SS sent a "notready" NOTIFY message, then after the SC sends the 200 (OK) response the SC shall immediately send a NOTIFY message to the primary SS with the body:

SC CCA-ID, failover, SC CCA-ID.

- i. [**Required: SS**] The primary SS sends a 200 (OK) response, and shall cease sending inbound UC SIP messages to the SC and instead shall forward the inbound UC SIP messages intended for the SC to the secondary SS.

- ii. [**Required: SC**] The SC returns to Step 1.

NOTE: The SC again waits a configurable amount of time (30–60 minutes) before sending an OPTIONS request.

- (c) If the triggering event for the failback had been a successful OPTIONS request sent by the SC to the primary SS, then:
 - i. **[Required: SC]** The SC returns to Step 1 whereby the SC again waits a configurable time interval (default equals 30–60 minutes) before sending an OPTIONS request to the primary SS unless the SC receives another inbound INVITE request from the primary SS.
- c. Step 4 **[Required: SC]** The SC shall send a NOTIFY to the secondary SS with body: SC CCA-ID, readytofailback, SC CCA-ID
 - (1) **[Required: SS]** The secondary SS shall respond to the NOTIFY message with a 200 (OK) response and send an OPTIONS request to the primary SS to confirm the primary SS is reachable at the SIP layer from the secondary SS.
 - (a) **[Required: SS]** If the secondary SS receives a 200 (OK) response to the OPTIONS request within 60 seconds, then upon receiving the 200 (OK) response the secondary SS shall immediately send a NOTIFY message to the SC with the body: Secondary SS CCA-ID, readytofailback, SC CCA-ID
 - i. **[Required: SC]** The SC sends a 200 OK response and goes to Step 5.
 - (b) **[Required: SS]** If the secondary SS does NOT receive a 200 (OK) response to the OPTIONS request (from step 4.1) within 60 seconds (i.e., the secondary SS either receives no response to the OPTIONS request or receives a failure response code from the primary SS), then the secondary SS sends a NOTIFY message to the SC with the body: Secondary SS CCA-ID, notready, SC CCA-ID
 - i. **[Required: SC]** The SC sends a 200 (OK) response and returns to Step 1 whereby the SC again waits a configurable time interval (default equals 30–60 minutes) before sending an OPTIONS request to the primary SS unless the SC receives another inbound INVITE request from the primary SS.
 - (c) **[Required: SC]** If the SC does NOT receive either a “readytofailback” NOTIFY message or a “notready” NOTIFY message from the secondary SS within 90 seconds of receipt of the secondary SS’s 200 (OK) response to the “readytofailback” NOTIFY message from the SC at step 4, then the SC shall abort the failback procedure and return to Step 1.
- NOTE: **[Required: SC]** If at any time during steps 1 to 4 the primary SS again becomes unreachable, then the SC aborts the failback process at that point and goes back to Step 1.
- d. Step 5 **[Required: SC]** The SC shall send a NOTIFY message to the primary SS with the body: SC CCA-ID, failback, SC CCA-ID.

- (1) [**Required: SS**] The primary SS shall send a 200 (OK) response and immediately sends a NOTIFY message to the SC with the body: Primary SS CCA-ID, ackfailback, SC CCA-ID
- (2) [**Required: SC**] The SC sends a 200 (OK) response and proceeds to Step 6.

NOTE: [**Required: SC**] If the SC does NOT receive an “ackfailback” NOTIFY message from the primary SS within 60 seconds of receipt of the 200 (OK) response to the “failback” NOTIFY message, then the SC shall abort the failback procedure and return to Step 1.

- e. Step 6 [**Required: SC**] Upon receipt of a timely “ackfailback” NOTIFY message from the primary SS, the SC shall send a NOTIFY message to the secondary SS with the body: SC CCA-ID, failback, SC CCA-ID

- (1) [**Required: SS**] The secondary SS shall send a 200 (OK) response.

NOTE: [**Required: SS**] If the NOTIFY message (of step 6) times out or the secondary SS does not respond with a 200 (OK) response, then the secondary SS shall resend the “failback” NOTIFY message every 30 seconds until the secondary SS responds with 200 (OK) response.

- (2) [**Required: SC**] Once the secondary SS responds to the “failback” NOTIFY message with a 200 (OK) response, then failback has officially occurred and the SC shall send the outbound INVITE requests corresponding to new call requests to the primary SS and shall continue to send the outbound UC SIP messages pertaining to existing calls that were established through the secondary SS to the secondary SS until those calls terminate normally.
- (3) [**Required: SS**] At this point, when the primary SS receives inbound INVITEs corresponding to new call requests intended for the SC, the primary SS shall send those inbound INVITEs to the SC.
- (4) [**Required: SS**] If, during the failover period, the primary SS had been receiving inbound INVITEs intended for the SC and forwarding those inbound INVITEs to the secondary SS, then the primary SS shall continue to send the inbound UC SIP messages related to the forwarded inbound INVITEs to the secondary SS until those calls terminate normally.
- (5) [**Required: SS**] At this point, when the secondary SS receives inbound INVITEs corresponding to new call requests intended for the SC, the secondary SS shall forward those inbound INVITEs to the primary SS.
- (6) [**Required: SS**] The secondary SS shall continue to send to the SC the inbound UC SIP messages pertaining to existing calls that were established during the failover period until those calls terminate normally.

- (7) **[Required: SC]** When the SC sends new INVITE requests (as well as the subsequent UC SIP requests for the new call requests) to destinations outside the enclave, then the new INVITE requests (and the subsequent UC SIP requests) shall include a route set composed of two Route headers, where the first Route header is the SIP URI for the SBC at the enclave, and the second Route header is the SIP URI for the SBC serving the primary SS.
- (8) **[Required: SC]** Upon failback, the SC continues monitoring the primary SS as set forth in [Section 2.6.1](#), SC Monitors Primary SS for Status.

2.6.7.1 SSs Failback to Primary SS

SCM-001480 [Required: SS] Per [Section 2.6.6.1](#), SSs Failover to Secondary SS, each SS (except for the paired SS) shall continue to send the OPTIONS requests described in [Section 2.6.3](#), Each SS Monitors All Other SSs in the Network, to the failed SS.

SCM-001490 [Required: SS] When an SS receives a 200 (OK) response to an OPTIONS request from a failed SS (i.e., now a newly recovering SS), then the SS shall send the INVITE requests corresponding to new call requests intended for SCs whose primary SS is the newly recovering SS to the newly recovering SS. The new INVITE requests shall include a route set composed of two Route headers, where the first Route header is the SIP URI for the originating SS, and the second Route header is the SIP URI for the SBC serving the newly recovering SS.

SCM-001500 [Required: SS] The SS shall continue to send UC SIP messages pertaining to existing calls that were established through the secondary SS to the secondary SS until those calls terminate normally.

2.6.7.2 SC Failback to Primary SS Triggered by Primary SS

SCM-001510 [Required: SS] The primary SS waits a configurable amount of time (default equals 30–60 minutes) before resuming the periodic OPTIONS request to the unreachable SC.

SCM-001520 [Required: SS] When the primary SS resumes sending the periodic requests to the unreachable SC and receives a 200 (OK) response to an OPTIONS request from the SC, the primary SS shall send a NOTIFY message to the SC with the body: Primary SS CCA-ID, SCreachable, SC CCA ID

SCM-001530 [Required: SC] The SC shall respond with 200 (OK) response and initiate SC failback per [Section 2.6.7](#), SC Failback to Primary SS.

2.6.7.3 Security Considerations

SCM-001540 [Required: SC] If the SC receives a SUBSCRIBE request from an EI that has an Event header with the event type failover, then the SC shall reject the SUBSCRIBE request with

a 403 (Forbidden) response, and the SC shall NOT forward the SUBSCRIBE to any other signaling platform.

2.6.8 SIP Event Package for Failover

2.6.8.1 Introduction

This section defines a failover event package for UC SIP signaling appliances using the Session Initiation Protocol (SIP) events framework, along with a data format used in subscriptions and notifications for this package. The failover package enables the following:

- SC to notify SSs of impending failover.
- SC to notify primary SS and secondary SS of intent to failback.
- Primary SS and secondary SS to notify SC as to their readiness to engage in failback.
- SC to notify primary SS of failback.
- Primary SS to acknowledge failback.
- Primary SS to notify secondary SS that an SC is unreachable and, in turn, secondary SS to notify SC that the primary SS cannot reach the SC.
- Primary SS to notify SC that the SC is again reachable from the primary SS.

2.6.8.2 Subscription

2.6.8.2.1 Subscription Creation

The SUBSCRIBE message shall have an Expires header whose value is not less than 1,209,600 seconds (14 days).

The Expires header of the 200 (OK) response shall have a value not less than 1,209,600 seconds (14 days).

2.6.8.2.1.1 Exponential Back-Off

If the subscription fails, the Subscriber implements a subscription establishment scheme using an exponential back-off starting at 30 minutes and doubling on each attempt until reaching 240 minutes (i.e., 30, 60, 120, 240). Thereafter the time interval between subscription establishment attempts stays at 240 minutes until the subscription is completed successfully.

2.6.8.2.2 Subscription Duration

The default expiration time for a subscription for the failover event package is not less than 1,209,600 seconds (14 days).

A SUBSCRIBE message shall be sent to refresh the subscription at between 864,000 (10 days) and 950,400 (11 days) so that the subscription does not lapse.

If the refresh attempt fails then the Subscriber implements the exponential back-off in [Section 2.6.4.2](#), Exponential Back-Off.

2.6.8.2.3 *NOTIFY Bodies*

According to RFC 3265 [1], the NOTIFY message will contain bodies that describe the state of the subscribed resource. The format for the body of the NOTIFY request is specified in Section 4, 2.6.8.8 NOTIFY Body Format.

2.6.8.3 *Notifier Processing of SUBSCRIBE Requests*

All SUBSCRIBE requests are sent over trusted Transport Control Protocol (TCP)/Transport Layer Security (TLS) connections between trusted and authenticated signaling platforms therefore no additional authentication mechanism is required.

2.6.8.4 *Notifier Generation of NOTIFY Requests*

Notifications shall be generated as follows:

- Upon completion of the establishment of a subscription or refresh of a subscription.
- By SC (to the secondary SS) upon SC decision to conduct failover.
- By the secondary SS (to the primary SS) in case of failover in which primary SS is reachable at the SIP layer by secondary SS.
- By SC (to the primary SS) when the SC is ready to failback.
- By the primary SS (to the SC) immediately in response to the SC notification of readiness to failback in order to indicate readiness – or not – of the primary SS to failback.
- By the SC (to the secondary SS) when the SC is ready to failback.
- By the secondary SS (to the SC) in response to the SC's notification of readiness to failback – secondary SS determines whether to indicate its readiness – or not- to failback.
- By the SC (to the primary SS) to notify the primary SS of failback.
- By the primary SS (to the SC) immediately in response to SC's notification of failback in order to acknowledge failback or to indicate primary SS has reverted to “notready” status.
- By the SC (to the secondary SS) to notify the secondary SS of failback.
- By the SC (to the primary SS) to notify the primary SS of failover when the SC is in failover state and the primary SS sends a new INVITE request to the SC intended for a served end instrument of the SC and the primary SS response to the SC's notification of readiness to failback is that the primary SS is not ready to serve the SC.

- By the primary SS (to the secondary SS) to notify secondary SS that the SC is unreachable from the primary SS.
- By the secondary SS (to the SC) to notify the SC that it is unreachable to the primary SS.
- By the primary SS (to the SC) to notify the SC that is again reachable from primary SS.

2.6.8.5 *Subscriber Processing of NOTIFY Requests*

The NOTIFY requests for the failover package specifically is used to provide the following information:

- The SC Notifier notifies SSs about its readiness state to conduct failover and failback.
- The SS Notifiers notify the SC and paired SS about its readiness state to process SC failover or failback.
- The SC Notifier notifies the SS that it is proceeding with failover, or announcing an intention to failback, or proceeding with failback.
- The SS Notifier acknowledges that failback notification of SC.
- The SS Notifier notifies the SC when the SC becomes unreachable from the SS and again becomes reachable from the SS.

2.6.8.6 *Handling of Forked Requests*

The SUBSCRIBE requests used for failover do not fork.

2.6.8.7 *Rate of Notifications*

Notifications are always generated in response to the establishment and refresh of relatively long-term subscriptions. Notifications are also generated by rare failover or failback events.

2.6.8.8 *NOTIFY Body Format*

The Multipurpose Internet Mail Extensions (MIME) content-type used in the NOTIFY body is as follows:

text/plain; charset=us-ascii

The Content-type header is:

Content-type: text/plain; charset=us-ascii

The NOTIFY body consists of three comma-separated elements. The first element is the CCA-ID of the generator of the NOTIFY request. The second element is the variable “failstate” that has one of the following eight values:

- ready.

- failover.
- readytofailback.
- notready.
- failback.
- ackfailback.
- SCunreachable.
- SCreachable.

The third element is the CCA-ID of the SC that is the intended beneficiary of the failover or failback process associated with the NOTIFY. In the case of the establishment or refresh of the subscriptions between the primary softswitch and the secondary softswitch then the third element consists of the reserved word “all.”

2.7 PRODUCT INTERFACE

2.7.1 Internal Interface

SCM-001550 [Required: PEI, UEI, SC (including the MG and Media Server), SS, SBC]

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

2.7.2 External Physical Interfaces Between Network Components

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

SCM-001560 [Required: SC, SS, SBC, CE Router, ASLAN, PEI, UEI] The physical interfaces between an SC (and its appliances), the SBC, the ASLAN switches/routers, and the CE-R shall be a 10/100/1000-T Mbps Ethernet interface. Whenever the physical interfaces use IEEE 802.3 Ethernet standards, they shall support auto-negotiation even when the IEEE 802.3 standard has it as optional. This applies to 10/100/1000-T Ethernet standards; i.e., IEEE, Ethernet Standard 802.3, 1993; or IEEE, Fast Ethernet Standard 802.3u, 1995; and IEEE, Gigabit Ethernet Standard 802.3ab, 1999.

2.7.3 Interfaces to Other Networks

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

2.7.3.1 Deployable Networks Interface

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

2.7.3.2 DISN Teleport Site Interface

SCM-001570 [Required] The Assured Services subsystem shall interface the Teleport sites on both a TDM basis and an IP basis. A T1.619a MG with PRI signaling will be used for T1 trunks to the Teleport sites. If the Teleport site contains an SC, then the interface will be via the DISN WAN for both the media and signaling, with the signaling being UC SIP (UC SIP 2013) between the Teleport SC and the UC SS.

2.7.3.3 PSTN Interface

SCM-001580 [Required] The Assured Services subsystem shall interface with the PSTN and host-nation PTTs via the MG interfaces as specified in [Section 2.16](#), Media Gateway.

2.7.3.4 Allied and Coalition Network Interface

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

2.7.4 DISA VVoIP EMS Interface

SCM-001590 [Required] The physical interface between the DISA VVoIP Electronic Message System (EMS) and the network components (i.e., SC, SS, SBC) is a 10/100-Mbps Ethernet interface. The interface will work in either of the two following modes using auto-negotiation: IEEE, Ethernet Standard 802.3, 1993; or IEEE, Fast Ethernet Standard 802.3u, 1995.

Local management traffic and VVoIP EMS management traffic are required to use separate physical Ethernet interfaces. Redundant VVoIP EMS physical Ethernet interfaces may be used but are not required. Redundant local management physical Ethernet interfaces may be used but are not required.

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

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

Signaling and bearer traffic may use the same physical Ethernet interface as local or VVoIP EMS management traffic, or it may use a separate physical Ethernet interface. If signaling and bearer traffic shares a physical Ethernet interface with local or VVoIP EMS management traffic, then the signaling and bearer traffic shall use a separate VLAN.

2.8 PRODUCT PHYSICAL, QUALITY, AND ENVIRONMENTAL FACTORS

2.8.1 Physical Characteristics

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

2.8.2 Product Quality Factors

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

2.8.2.1 Product Availability

SCM-001600 [Required: SC, SS] The assured services appliance shall have a hardware or software availability of [**Required: High Availability SC, SS**] 0.99999 (a nonavailability state of no more than 5 minutes per year) and [**Required: Medium Availability SC**] 0.9999 (a nonavailability state of no more than 53 minutes per year). The vendor shall provide an availability model for the appliance showing all calculations and showing how the overall availability will be met. [**Required: High Availability SC, SS**] The subsystem(s) shall have no single point of failure that can cause an outage of more than 96 voice and/or video subscribers. To meet the availability requirements, all subsystem(s) platforms that offer service to more than 96 voice and/or video subscribers shall have a modular chassis that provides, at a minimum, the following:

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

-
- b. **[Optional: Medium Availability SC]** Dual Processors/Swappable Sparing (Control Supervisors). The chassis shall support dual-active processors, or processor card automatic swappable sparing. Failure of any one processor or swappable processor cards shall not cause a loss of any ongoing functions within the chassis (e.g., no loss of active calls).
 - c. **[Optional: Medium Availability SC]** Termination Sparing. The chassis shall support an (N+1) sparing capability for available 10/100-Mbps Ethernet modules used to terminate an IP voice or video subscriber.
 - d. **[Optional: Medium Availability SC]** Redundancy Protocol. The routing equipment shall support a protocol that allows for dynamic rerouting of IP packets or Ethernet frames so that no single point of failure exists in the Assured Services subsystem.
 - e. **[Optional: Medium Availability SC]** No Single Failure Point. No single point shall exist in the subsystem that could cause the loss of voice and/or video service to more than 96 voice or video PEIs or UEIs.
 - f. **[Optional: Medium Availability SC]** Switch Fabric or Backplane Redundancy for Active Backplanes. Active switching platforms within the subsystem components shall support a redundant (1+1) switching fabric or backplane. The second fabric's backplane shall be in active standby so failure of the first backplane shall not cause the loss of any ongoing events within the platform.
 - g. Software Upgrades and Patches. Software upgrades and patches shall be able to be implemented without incurring any subsystem downtime.
 - h. Backup Power UPS Requirements. The components that compose the subsystem for F/FO users, I/P users, and R users shall meet the appropriate Section 7, Network Edge Infrastructure, switch type backup power UPS requirements (e.g., 8 hours for an SS and SC) for all devices including the PEIs and UEIs. If a base has an automatic UPS switchover 72-hour power capability that feeds all the voice and video equipment, including the PEIs and UEIs, then it naturally meets the 8-hour backup power requirement with no need to do anything special or extra at the SC or SS. Backup power is only required for as many hours as it will take the base to switch over to backup generator power, but the total combination of backup times shall not be less than 8 hours. **[Optional: Medium Availability SC]** The backup power requirement is a minimum of 1 hour.
 - i. No Loss of Active Sessions. In the event of component failure in an appliance subsystem(s), all active sessions shall not be disrupted (namely, the loss of established session connections requiring user redialing to reestablish), and the media path through the network shall be restored within 5 seconds. In addition, when the state information is lost for non-disrupted active sessions, the SRTP media streams will clear when both the called and calling parties hang up their EIs. All components used to implement redundancy shall be capable of handling the entire session processing load in the event

that its counterpart device fails. Signaling states during the establishment or disestablishment of a session need not be maintained or continued during the switch over to backup components. However, session establishment or disestablishment states shall be cleared to prevent anomalous conditions such as the EI continues to ring even though the session will not be established or disestablished during the device(s) switch over. When session establishment or disestablishment signaling states are lost when switching over to backup components, it is expected that the subscriber will be required to redial the called number.

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

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

2.8.2.2 *Maximum Downtimes*

SCM-001610 [Required: High Availability SC, SS, ASLAN] The performance parameters associated with the ASLAN, SS, and High Availability SC, when combined, shall meet the following maximum downtime requirements:

- a. IP (10/100 Ethernet) network links: 35 minutes per year.
- b. IP subscriber: 12 minutes per year.

SCM-001620 [Required: Medium Availability SC, SS, ASLAN] The performance parameters associated with the ASLAN, SS, and Medium Availability SC, when combined, shall meet the following maximum downtime requirements:

- a. IP (10/100 Ethernet) network links – 82 minutes per year.
- b. IP subscriber – 60 minutes per year.

2.8.3 **Environmental Conditions**

SCM-001630 [Required] Environmental conditions requirements are contained in Telcordia Technologies GR-63-CORE. This document identifies the minimum generic spatial and environmental criteria for all new telecommunications equipment systems used in a telecommunications network. Included with these equipment systems are associated cable distribution systems, distributing and interconnecting frames, power equipment, operations support systems, and cable entrance facilities. The detailed specifications of this section are those of best commercial practice and will be specified by the acquiring DOD organization.

2.8.4 Voice Service Quality

SCM-001640 [Required: PEI, UEI, IAD, TA, MG] For these VoIP devices, the voice quality shall have a Mean Opinion Score (MOS) of 4.0 (R-Factor equals 80) or better, as measured IAW the E-Model. Additionally, these devices shall not lose two or more consecutive packets in a minute and shall not lose more than seven voice packets (excluding signaling packets) in a 5-minute period. This only applies to devices that generate media and have a Network Interface Card (NIC).

2.9 END INSTRUMENTS

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

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

2.9.1 IP Voice End Instruments

2.9.1.1 Basic

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

SCM-001650 [Optional: Voice EI] DOD Common Access Card (CAC) reader. [See Section 4.2.3.5, Authentication Practices, item 1h(1), for SC and EI requirements on PKI and CAC authentication, and SC and EI requirements on Username and Personal Identification Number (PIN) authentication.]

SCM-001660 [Required: Voice EI] Display calling number. (See [Section 2.2.8](#), Calling Number Delivery, for SC and EI requirements on the Calling Number Delivery feature.)

SCM-001670 [Required: Voice EI] Display precedence level of the session.

SCM-001680 [Required: Voice EI] Use of DSCPs in signaling and media streams.

SCM-001690 [Required: Voice EI] Support for Dynamic Host Configuration Protocol (DHCP).

SCM-001700 [Required: Voice EI] For multiple line appearance, only two-appearance IP voice instruments are specified and they shall function as specified in [Section 2.9.7](#), Multiple Call Appearance Requirements for UC SIP EIs.

2.9.1.2 Tones and Announcements

SCM-001710 [Required: PEI, UEI, SC, SS] Tones and announcements, as required in [Section 2.9.1.2.1](#), UC Ringing Tones, Cadences, and Information Signals, and [Section 2.9.1.2.2](#), Announcements, shall be supported, except for the loss of the C2 announcement. These tones and announcements may be generated locally by the PEI or UEI on the command of the SC, or be generated on the command of the SC by an internal SC Media Server or an external Media Server connected to the ASLAN and passed as a media stream to the PEI or UEI. Regardless of how implemented, the Media Server is part of the SC SUT.

2.9.1.2.1 UC Ringing Tones, Cadences, and Information Signals

SCM-001720 [Required: PEI, UEI, TA, IAD, MG, SC, SS] The UC EIs and signaling appliances shall provide alerting (ringing) for precedence calls (i.e., PRIORITY and above) that is distinct from the alerting for ROUTINE calls.

SCM-001730 [Optional: PEI, UEI, TA, IAD, MG, SC, SS] The UC EIs and signaling appliances may implement the ringing tones and cadences shown in [Table 2.9-1](#), UC Ringing Tones and Cadences.

Table 2.9-1. UC Ringing Tones and Cadences

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

SCM-001740 [Required: UEI] The UEIs shall also be able to provide customized ring tones for incoming precedence calls through the use of pre-recorded audio files (e.g., MP3, WAV, WMA, OGG) that are stored in the UEIs. For example, an UEI may store one audio file for use with ringing on incoming PRIORITY calls, another file for use with ringing on incoming IMMEDIATE calls, another file for use with ringing on incoming FLASH calls, and so on. Different audio files can also be associated with different calling numbers when that calling

number is used on a Precedence calls (e.g., “This is an IMMEDIATE call from General John Smith.”).

SCM-001750 [Required: PEI, UEI, ATA, IAD, MG, SC, SS] The EIs and signaling appliances shall implement the UC information signals shown in [Table 2.9-2](#), UC Information Signals.

Table 2.9-2. UC Information Signals

SIGNAL	FREQUENCIES (HZ)	SINGLE TONE LEVEL	COMPOSITE LEVEL	INTERRUPT RATE	TONE ON	TONE OFF
Audible Ringback Precedence Call	440 + 480 (Mixed); +/- 0.5 % for each frequency	-19 dBm0, +/- 1.5 dB	-16 dBm0, +/- 1.5 dB	30 IPM (Based on an on/off cycle of 2 seconds +/- 200 ms, and 30 on/off cycles per minute)	1640 ms ; +/- 10%	360 ms; +/- 10%
Preemption Tone	440 + 620 (Mixed); +/- 0.5 % for each frequency	-19 dBm0, +/- 1.5 dB	-16 dBm0, +/- 1.5 dB		Steady on	
Call Waiting (Precedence Call)	440; +/- 0.5 %	-13 dBm0, +/- 1.5 dB		Continuous at 6 IPM (300 ms +/- 60 ms of CW tone, plus 9700 ms +/- 1940 ms of no CW tone; yields a nominal 10-second cycle which occurs 6 times per minute)	100 ± 20 ms, Three Bursts	9700 ms +/- 1940 ms
Conference Connect Tone	Vendor-provided ascending tones					
Conference Disconnect Tone	852 and 1336 (Alternated at 100 ms intervals); +/- 0.5 % for each frequency	-24 dBm0 +/- 1.5 dB		Steady on	2000 ms +/- 200 ms (per occurrence)	
Override Tone	440; +/- 0.5 percent	-13 dBm0, +/- 1.5 dB		Continuous at 6 IPM (2.5 sec +/- 0.25 sec of tone on, plus 7.5 sec +/- 0.75 sec of tone off; yields a nominal 10-second cycle which occurs 6 times per minute)	2000 ms +/- 200 ms (followed by) 500 ms +/- 50 ms on, and 7500 ms +/- 750 ms off	
Station Busy	480+620			0.5 sec on, 05. sec off (60 IPM)		
All Circuits Busy	480+620			0.25 sec on, 0.25 sec off (120 IPM)		
LEGEND						

SIGNAL	FREQUENCIES (HZ)	SINGLE TONE LEVEL	COMPOSITE LEVEL	INTERRUPT RATE	TONE ON	TONE OFF
CW: Call Waiting Hz: Hertz			IPM: Interruptions per Minute sec: second			

2.9.1.2.2 Announcements

SCM-001760 [Required: PEI, UEI, SC, SS] With the exception of the Precedence Access Limitation Announcement (PALA) and the Attendant Queue Announcement (ATQA), the announcements in [Table 2.9-3](#), Announcements, are required for all UC Appliances and EIs, and all announcements that are associated with a specific NM trunk group and/or code control implementation. Each announcement shall contain a location identification number to be provided by the Government. The appliance playing the announcement (or serving the EI that is playing the announcement) shall be identified by “Switch Name and Location.” Announcements shall be capable of being recorded and changed by Government operations and maintenance (O&M) personnel. Additional local messages may be added and optionally activated, deactivated, or modified via administrative or operational controls.

Table 2.9-3. Announcements

ANNOUNCEMENT CONDITION	ANNOUNCEMENT
An equal or higher precedence call is in progress	Blocked Precedence Announcement (BPA). “(Switch name and Location). Equal or higher precedence calls have prevented completion of your call. Please hang up and try again. This is a recording. (Switch name, location identification number, and Location).”
Unauthorized precedence level is attempted	Unauthorized Precedence Level Announcement (UPA). “(Switch name and Location). The precedence used is not authorized for your line. Please use an authorized precedence or ask your attendant for assistance. This is a recording. (Switch name, location identification number, and Location).”
No such service or Vacant Code	Vacant Code Announcement (VCA). “(Switch name and Location.) Your call cannot be completed as dialed. Please consult your directory and call again or ask your operator for assistance. This is a recording. (Switch name, location identification number, and Location).”
Operating or equipment problems encountered	Isolated Code Announcement (ICA). “(Switch name and Location). A service disruption has prevented the completion of your call. Please wait 30 minutes and try again. In case of emergency, call your operator. This is a recording. (Switch name, location identification number, and Location).”
Precedence Access Threshold (PAT) limitation	Precedence Access Limitation Announcement (PALA). “(Switch name and Location). Precedence access limitation has prevented the completion of your call. Please hang up and try again. This is a recording. (Switch name, location identification number, and Location).”
Busy station not equipped for preemption	Busy Not Equipped Announcement (BNEA). “(Switch name and Location). The number you have dialed is busy and not equipped for CW or preemption. Please hang up and try again. This is a recording. (Switch name, location identification number, and Location).”

ANNOUNCEMENT CONDITION	ANNOUNCEMENT												
Attendant Queue Announcement	Attendant Queue Announcement (ATQA). “This is the <site name> [multifunction, end office] switch. All attendants are busy now. Please remain on the line until an attendant becomes available or try your call later. This is a recording. <site name> [multifunction, end office] switch.”												
Loss of C2 Features	Loss of C2 Features Announcement (LOC2). “This is the (Switch name, location identification number, and Location). This call is leaving the DSN. This is a recording.”												
<p>LEGEND</p> <table border="0"> <tr> <td>ATQA: Attendant Queue Announcement</td> <td>ICA: Isolated Code Announcement</td> </tr> <tr> <td>BNEA: Busy Not Equipped Announcement</td> <td>LOC2: Loss of C2 Features</td> </tr> <tr> <td>BPA: Blocked Precedence Announcement</td> <td>PALA: Precedence Access Limitation Announcement</td> </tr> <tr> <td>C2: Command and Control</td> <td>UPA: Unauthorized Precedence Level Announcement</td> </tr> <tr> <td>CW: Call Waiting</td> <td>VCA: Vacant Code Announcement</td> </tr> <tr> <td>DSN: Defense Switched Network</td> <td></td> </tr> </table>		ATQA: Attendant Queue Announcement	ICA: Isolated Code Announcement	BNEA: Busy Not Equipped Announcement	LOC2: Loss of C2 Features	BPA: Blocked Precedence Announcement	PALA: Precedence Access Limitation Announcement	C2: Command and Control	UPA: Unauthorized Precedence Level Announcement	CW: Call Waiting	VCA: Vacant Code Announcement	DSN: Defense Switched Network	
ATQA: Attendant Queue Announcement	ICA: Isolated Code Announcement												
BNEA: Busy Not Equipped Announcement	LOC2: Loss of C2 Features												
BPA: Blocked Precedence Announcement	PALA: Precedence Access Limitation Announcement												
C2: Command and Control	UPA: Unauthorized Precedence Level Announcement												
CW: Call Waiting	VCA: Vacant Code Announcement												
DSN: Defense Switched Network													

SCM-001770 [Required: PEI, UEI, SC, SS] The ATQA is required for an SC SS, and for PEIs and UEIs served by SCs and SCs internal to SSs.

2.9.1.2.3 *Loss of C2 Features Announcement*

SCM-001780 [Optional: PEI, UEI, SC, SS] The LOC2 Features announcement only applies to calls placed via an SC MG or an SS MG to a non-MLPP PRI or CAS trunk and may be provided IAW the following:

- a. Play only for calls above the ROUTINE precedence level.
- b. Not required for locally originated calls to non-MLPP PRI or CAS trunks (e.g., PSTN).
- c. Required for VoIP calls received from the DISN WAN, or calls received from a base MLPP tie trunk via an MG that is destined to tandem via an SC MG or SS MG to a non-MLPP PRI or CAS trunk (assuming there is an available trunk to connect to). (NOTE: CAS interfaces are conditional for the SC MG and SS MG.)
- d. Play before ringback is provided to the caller.
- e. Play before cut-through to the non-MLPP trunk. This prevents ringback from interfering with the announcement.
- f. The announcement shall be played into the media stream at the MG point of departure from the DISN to the non-MLPP trunk.
- g. The LOC2 announcement is not signaled by UC SIP.

2.9.1.3 Audio Codecs, Voice Instruments

SCM-001790 [Required: PEI, UEI, SC MG, SS MG] The the origination and termination of a voice session using the following codecs shall be supported:

- a. ITU-T Recommendation G.711, to include both the μ -law and A-law algorithms.
- b. **[Optional: PEI, UEI]** ITU-T Recommendation G.723.1.
- c. ITU-T Recommendation G.729 or G.729A.
- d. **[Optional: PEI, UEI]** ITU-T Recommendation G.722.1.

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

Transcoding between low-bit-rate codecs like G.729 and higher-bit-rate codecs like G.711 may be performed in Deployed (Tactical) networks. When calls using this transcoding enter Fixed (Strategic) networks, these calls will appear in the Fixed networks as higher-bit-rate codec calls.

2.9.1.4 VoIP PEI or UEI Telephone Audio Performance

SCM-001800 [Required: PEI, UEI] Voice over IP PEIs or UEIs (i.e., handset, headset, and hands-free types) shall comply with Telecommunications Industry Association (TIA)-810-B, November 3, 2006.

2.9.1.5 Voice over IP Sampling Standard

SCM-001810 [Required: PEI, UEI] For Fixed-to-Fixed calls, the product shall use 20 ms as the default voice sample length, and as the basis for the voice payload packet size. For other call types, e.g., Fixed-to-Deployable calls, the product shall use different voice sample lengths and voice payload packet sizes, as negotiated during call setup via the Session Description Protocol (SDP).

2.9.1.6 Softphones

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

SC and SS support for softphones is optional.

SCM-001820 [Conditional: PEI, UEI, SC, SS] If a softphone is supported by an SC or SS, the softphone shall be conceptually identical to a traditional IP “hard” telephone and is required to

provide voice features and functionality provided by a traditional IP hard telephone, unless explicitly stated here within this paragraph. The softphone application in conjunction with a general-purpose computer, including its mouse (point and click) interaction, shall support, as a minimum, the following requirements:

- a. [Section 2.2](#), Voice Features and Capabilities.
- b. [Section 2.9.1.1](#), Basic.
- c. [Section 2.9.1.2](#), Tones and Announcements.
- d. [Section 2.9.1.3](#), Audio Codecs, Voice Instruments.
- e. [Section 2.9.1.4](#), VoIP PEI or UEI Telephone Audio Performance.
- f. [Section 2.9.1.5](#), Voice over IP Sampling Standard.
- g. [Section 2.9.4](#), Authentication to SC.
- h. [Section 2.9.5](#), End Instrument to ASLAN Interface.
- i. Section 6, Network Infrastructure End-to-End Performance. The softphone application shall be exempt from the performance (i.e., packet loss, jitter, latency) requirements specified in Section 6, Network Infrastructure End-to-End Performance; e.g., the PEI/UEI 50-ms latency for the G.711 codec.
- j. Section 6.3.2, VVoIP Differentiated Services Code Point.
- k. Section 4, Information Assurance.

SCM-001830 [Conditional: PEI, UEI] If an EI is a softphone, then it shall inhibit any screen saver or lock screen capability whenever the softphone application is active (i.e., user is on a call). This is to avoid the situation where the user needs to interact with the softphone application via the mouse or keyboard expeditiously (e.g., respond to a new call) but first needs to re-login.

2.9.1.7 DSCP Packet Marking

SCM-001840 [Required: PEI, UEI, SC, SS] As part of the session setup process, the SC controls what Differentiated Service Code Point (DSCP) to use in the subsequent session media stream packets. For inter-SC media sessions (across the WAN), and intra-SC media sessions (internal to the enclave), one of the following occurs:

- a. The PEI shall be commanded by the SC about which DSCP to insert in the session media stream packets.
- b. The PEI shall populate the DSCP marking on its own.
- c. The UEI shall populate the DSCP marking on its own.

SCM-001850 [Required: PEI, UEI, SC, SS] The exact DSCP method used by the implementer shall comply with Section 6, Network Infrastructure End-to-End Performance. The session's

media type (e.g., audio vs. video) and the session's precedence level (R, P, I, F, or FO) shall be used to determine the media stream DSCP for that session.

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

2.9.2 Analog and ISDN BRI Telephone Support

SCM-001860 [Required: SC] Analog instruments, including secure analog EIs, analog facsimile (fax) EIs, and analog modem EIs, shall be supported by the SC either by a Terminal Adapter, RJ-11 Plain Old Telephone Service (POTS) telephone to RJ-45 Ethernet interface (TA), or an Integrated Access Device (IAD), 4 or more ports of RJ-11 POTS telephone to one port of RJ-45 Ethernet interface.

- a. **[Required: TA]** The TA shall support G.711 standards.
- b. **[Optional: TA]** The TA may support V.150.1 Modem Relay and T.38 Fax Relay standards.
- c. **[Required: IAD]** The IAD shall support G.711 standards.
- d. **[Optional: IAD]** The IAD may support V.150.1 Modem Relay and T.38 Fax Relay standards.
- e. **[Required: EI, TA, IAD, SC, SS]** Analog telephones, when combined with a TA or IAD, together shall comply with TIA-810-B, November 3, 2006.

SCM-001870 [Required: MG Line Card] Analog instruments, including secure analog EIs, analog facsimile EIs, and analog modem EIs, shall be supported by the existing twisted-pair cable plant connected to line cards that are part of the SC MG.

- a. **[Required: MG Line Card]** The line card shall support G.711 standards.
- b. **[Optional: MG Line Card]** The line card may support V.150.1 Modem Relay and T.38 Fax Relay standards.
- c. **[Required: EI, MG Line Card, SC, SS]** Analog telephones, when connected to a line card, together shall comply with TIA-810-B, November 3, 2006.

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

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

- e. [**Optional: SC, SS**] The SC and SS may support analog facsimile EIs on analog TAs, IADs, and MG line cards, where the TAs, IADs, and MG line cards support the ITU-T Recommendation T.38 standard for Fax Relay.
- f. [**Optional: SC, SS**] The SC and SS may support analog modem EIs on analog TAs, IADs, and MG line cards, where the TAs, IADs, and MG line cards support the ITU-T Recommendation V.150.1 standard for Modem Relay.

2.9.2.1 ISDN BRI Telephone Support

SCM-001880 [**Optional: SC**] ISDN BRI EIs, including secure ISDN BRI EIs, may be supported by the SC.

SCM-001890 [**Conditional: SC**] If an SC supports ISDN BRI EIs, they shall be supported by one of the following:

- a. A BRI-capable TA that is connected to an Ethernet port.
- b. A BRI-capable IAD that is connected to an Ethernet port.
- c. The existing twisted-pair cable plant connected to a BRI-capable line card that is part of the SC MG.

SCM-001900 [**Conditional: SC, TA**] If a TA supports standard (nonsecure) ISDN BRI EIs, it shall support the ITU-T Recommendation G.711 standard.

SCM-001910 [**Conditional: SC, IAD**] If an IAD supports standard (nonsecure) ISDN BRI EIs, it shall support the ITU-T Recommendation G.711 standard.

SCM-001920 [**Conditional: SC, TA**] If a TA supports secure ISDN BRI EIs, it shall support both the ITU-T Recommendations G.711 and V.150.1 standards.

SCM-001930 [**Conditional: SC, IAD**] If an IAD supports secure ISDN BRI EIs, it shall support both the ITU-T Recommendations G.711 and V.150.1 standards.

SCM-001940 [**Conditional: SC MG**] If an MG line card supports standard (nonsecure) ISDN BRI EIs, the MG line card shall support the ITU-T Recommendation G.711 standard.

SCM-001950 [**Conditional: SC MG**] If an MG line card supports secure ISDN BRI EIs, it shall support both the ITU-T Recommendations G.711 and V.150.1 standards.

SCM-001960 [**Required: EI**] The ISDN BRI telephones when combined with a BRI-capable TA, BRI-capable IAD, or BRI-capable MG line card shall comply with TIA-810-B, November 3, 2006.

SCM-001970 [**Conditional: SC, TA, IAD, SC MG, EI**] If an SC, TA, IAD, or SC MG support ISDN BRI EIs (both standard and secure), the SC, TA, IAD, or SC MG shall support all the DSN ISDN BRI requirements in the following DSN sections:

- a. [Section 2.26.1.6](#), ISDN MLPP BRI.
- b. [Section 2.26.1.8](#), MLPP Interactions With Common Optional Features and Services.
- c. [Section 2.26.1.9](#), MLPP Interactions With Electronic Key Telephone Systems Features.
- d. [Section 2.26.2](#), Signaling.
- e. [Section 2.26.3](#), ISDN.

2.9.3 Video End Instrument

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

2.9.3.1 *Basic*

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

SCM-001980 [Optional: Video EI] DOD CAC card reader.

SCM-001990 [Required: Video EI] Automatic enabling of the video camera is not permitted after video session negotiation or acceptance. The called party must take a positive action to enable the camera.

SCM-002000 [Required: Video EI] Display calling number.

SCM-002010 [Optional: Video EI] Display precedence level of the session.

SCM-002020 [Optional: Video EI] Support for Multilevel Precedence and Preemption (MLPP) feature.

SCM-002030 [Required: Video EI] Support for DHCP.

2.9.3.2 *Display Messages, Tones, and Announcements*

SCM-002040 [Required: PEI, UEI, SC, SS] Tones and announcements, as appropriate for voice and video over IP, and as required, in [Section 2.9.1.2.1](#), UC Ringing Tones, Cadences, and Information Signals, and [Section 2.9.1.2.2](#), Announcements, shall be supported by the PEI and UEI, except for the loss of the C2 announcement. These tones and announcements may be generated locally by the PEI and UEI on the command of the SC, or generated on command of the SC by an internal SC Media Server or an external Media Server connected to the ASLAN, and passed as a media stream to the PEI and UEI. Regardless of how implemented, the Media Server is part of the SC SUT.

2.9.3.3 *Video Codecs (Including Associated Audio Codecs)*

SCM-002050 [Required: PEI, UEI] The product shall support the origination, maintenance, and termination of a video session using the following codecs: one G.xxx and one H.xxx shall be used to create and sustain a video session. (All video and audio capabilities in the PEI or UEI shall be sent to the terminating PEI or UEI for negotiation about which video and audio codec to use for the session.)

SCM-002060 [Required: PEI, UEI] Video PEIs and UEIs shall support, at a minimum, G.711 Pulse Code Modulation (PCM), where PCM has a static payload type value of 0 and a clock rate of 8000. The PCM shall support both the μ -law and A-law algorithms.

SCM-002070 [Optional: PEI, UEI] It is recommended that video PEIs and UEIs support other audio codecs in addition to G.711 PCM. Recommended audio codecs include the following:

- a. ITU-T Recommendation G.722, where G.722 has a static payload type value of 9 and a clock rate of 8000.
- b. ITU-T Recommendation G.722.1, where G.722.1 has the encoding name "G7221", a clock rate of 16000, and a standard bit rate of 24 Kbps or 32 Kbps.
- c. ITU-T Recommendation G.723.1, where G.723.1 has the encoding name "G723", a clock rate of 8000, and standard bit rates of 5.3 Kbps and 6.3 Kbps.
- d. ITU-T Recommendation G.729, where G.729 has the encoding name "G729", a clock rate of 8000, and a standard bit rate of 8 Kbps.
- e. ITU-T Recommendation G.729 Annex A (G.729A), where G.729A also has the encoding name "G729", a clock rate of 8000, and a standard bit rate of 8 Kbps.

SCM-002080 [Required: PEI, UEI] Video PEI and UEI shall support, at a minimum, the following video codecs:

- a. ITU-T Recommendation H.263-2000.
- b. ITU-T Recommendation H.264
- c. **[Optional]** ITU-T Recommendation H.264, Scalable Video Coding (SVC)
- d. **[Optional]** ITU-T Recommendation H.261

2.9.3.4 *Chg1-5.2.4.2 H.323 Video Teleconferencing*

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

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

SCM-002090 [Optional] The H.323 VTC system and end points should meet the the requirements of Federal Telecommunications Recommendation (FTR) 1080B-2002.

SCM-002100 [Optional] The H.323 VTC features and functions used in conjunction with IP network services should meet the requirements of H.323 in accordance with FTR 1080B-2002, and H.323 video EIs should meet the tagging requirements as specified in Section 7, Network Edge Infrastructure.

SCM-002110 [Required] A loss of any conferee on a multipoint H.323 videoconference shall not terminate or degrade the DSN service supporting H.323 VTC connections of any of the other conferees on the videoconference.

SCM-002120 [Optional] An audio add-on interface may be provided on H.323 VTC equipment in accordance with Section 3.7, Customer Premise Equipment.

SCM-002130 [Conditional] If an H.323VTC system or end point uses an integrated BRI interface to connect to the DSN, then it shall be in conformance with the requirements associated with a TA as described in Section 3.7, Customer Premise Equipment, and [Section 2.9.2.1](#), ISDN BRI Telephone Support.

SCM-002140 [Conditional] If a VTC system or end point uses a serial interface to another device, such as a cryptographic device or TA, for eventual connection to the DSN, it shall be in conformance with the requirements for that serial interface as described in FTR 1080B-2002.

SCM-002150 [Required] Physical, electrical, and software characteristics of a video teleconferencing unit (VTU) system or end point that is used in the DSN network shall not degrade, or impair, the serving DSN switch and its associated network operations.

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

2.9.4 Authentication to SC

SCM-002160 [Required: PEI, UEI, SC] The PEI and UEI shall each be capable of authenticating itself to its associated SC and vice versa IAW Section 4, Information Assurance.

2.9.5 End Instrument to ASLAN Interface

SCM-002170 [Required: PEI, UEI] The interface to the ASLAN shall be IAW Ethernet (IEEE 802.3) Local Area Network (LAN) technology. The 10-Mbps and 100-Mbps Fast Ethernet (IEEE 802.3u) shall be supported.

2.9.6 Operational Framework for UEIs and Video EIs

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

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

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

2.9.6.1 Requirements for Supporting UC SIP EIs

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

SCM-002180 [Required: SC, SS, UC SIP Voice EI, UC SIP Secure Voice EI, UC SIP Video EI] The UC SIP EIs (voice, secure voice, and video) shall follow all of the previous requirements for EIs (voice and video, with secure voice EIs following the previous requirements for voice EIs), except for those requirements that involve vendor-proprietary SC-to-EI signaling.

SCM-002190 [Required: SC, SS, UC SIP Voice EI, UC SIP Secure Voice EI, UC SIP Video EI] The SCs and UC SIP EIs (voice, secure voice, and video) shall support mutual authentication using UC SIP and TLS signaling instead of vendor-proprietary signaling. That is, each UC SIP EI shall authenticate itself with its serving SC using UC SIP and TLS signaling, and each SC shall authenticate itself with the UC SIP EIs that it serves using UC SIP and TLS signaling.

SCM-002200 [Required: SC, SS] The SC shall allow a single UC SIP EI to support voice, secure voice, and video capabilities. In this case, the SC shall support that EI using the combined requirements for a UC SIP voice EI, a UC SIP secure voice EI, and a UC SIP video EI, as given below. The SC shall also allow a single UC SIP EI to support the following subset of these three capabilities:

- a. Voice and Secure Voice.
- b. Voice and Video.

SCM-002210 [Optional: UC SIP Voice EI, UC SIP Secure Voice EI, UC SIP Video EI] A single UC SIP EI may support voice, secure voice, and video capabilities. In this case, the EI shall support those capabilities IAW the combined requirements for an UC SIP voice EI, an UC SIP secure voice EI, and an UC SIP video EI, as given in [Section 2.9.6.2](#), Requirements for UC SIP Voice EIs; [Section 2.9.6.3](#), Requirements for UC SIP Secure Voice EIs; and [Section 2.9.6.4](#), Requirements for UC SIP Video EIs.

SCM-002220 [Optional: UC SIP Voice EI, UC SIP Secure Voice EI] A single UC SIP EI may support both voice and secure voice capabilities. In this case, the EI shall support those capabilities IAW the combined requirements for an UC SIP voice EI and an UC SIP secure voice

EI, as given in [Section 2.9.6.2](#), Requirements for UC SIP Voice EIs, and [Section 2.9.6.3](#), Requirements for UC SIP Secure Voice EIs.

SCM-002230 [Optional: UC SIP Voice EI, UC SIP Video EI] A single UC SIP EI may support both Voice and Video capabilities. In this case, the EI shall support those capabilities IAW the combined requirements for an UC SIP voice EI and an UC SIP video EI, as given in [Section 2.9.6.2](#), Requirements for UC SIP Voice EIs, and [Section 2.9.6.4](#), Requirements for UC SIP Video EIs.

SCM-002240 [Required: UC SIP Secure Voice EI] A UC SIP secure voice EI shall also support the capabilities of a UC SIP Voice EI IAW the UC SIP voice EI requirements given in [Section 2.9.6.2](#), Requirements for UC SIP Voice EIs. The UC SIP secure voice EI shall support these capabilities for “voice communication in the clear” using the Audio media type and the G.7XX codecs.

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

2.9.6.2 Requirements for UC SIP Voice EIs

SCM-002250 [Required: SC, SS] The SCs shall support UC SIP voice EIs that use UC SIP for EI-to-SC signaling. The SCs shall support these UC SIP voice EIs using the UC SIP SC-to-UC SIP-EI interface defined in [Section 2.9.7](#), Multiple Call Appearance Requirements for UC SIP EIs, and in UC SIP 2013.

SCM-002260 [Required: UC SIP Voice EI] The UC SIP voice EIs shall support UC SIP for EI-to-SC signaling. These UC SIP voice EIs shall support the UC SIP SC-to-UC SIP-EI interface defined in [Section 2.9.7](#), Multiple Call Appearance Requirements for UC SIP EIs, and in UC SIP 2013.

SCM-002270 [Required: SC, SS, UC SIP Voice EI] The SCs and UC SIP Voice EIs shall support the following supplementary services for voice calls, consistent with [Section 2.2](#), Voice Features and Capabilities, using UC SIP signaling.

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

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

SCM-002280 [Required: SC, SS, UC SIP Voice EI] The SCs and UC SIP voice EIs shall support a mechanism to limit the total number of voice calls at that EI at any given time.

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

SCM-002290 [Required: SC, SS, UC SIP Voice EI] For UC SIP voice EIs, the voice call limit depends on the number of voice call appearances supported on the EI. The UC SIP voice EIs are required to support two voice call appearances for one DSN number in this document (per [Section 2.9.7](#), Multiple Call Appearance Requirements for UC SIP EIs). But one of these call appearances may not be used, because the SC is only configured to support one voice call appearance for one DSN number on this EI.

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

- a. When the SC is configured to support two call appearances on an UC SIP voice EI, the SC shall use a voice call limit of “Two” for that EI.
- b. When the SC is configured to support one call appearance on an UC SIP voice EI (even though the EI may support two call appearances), the SC shall use a voice call limit of “One” for that EI.

2.9.6.3 Requirements for UC SIP Secure Voice EIs

SCM-002300 [Required: SC, SS] The SCs shall support UC SIP secure voice EIs that use UC SIP for EI-to-SC signaling. The SCs shall support these UC SIP secure voice EIs using the UC SIP SC-to-UC SIP-EI interface defined in [Section 2.9.7](#), Multiple Call Appearance Requirements for UC SIP EIs, and in UC SIP 2013.

SCM-002310 [Required: UC SIP Secure Voice EI] UC SIP Secure Voice EIs shall support UC SIP for EI-to-SC signaling. These UC SIP secure voice EIs shall support the UC SIP SC-to-UC SIP-EI interface defined in [Section 2.9.7](#), Multiple Call Appearance Requirements for UC SIP EIs, and in UC SIP 2013.

SCM-002320 [Required: SC, SS] The SCs and SSs shall support the following supplementary services for voice calls on UC SIP secure voice EIs, consistent with [Section 2.2](#), Voice Features and Capabilities, using UC SIP signaling:

- a. Precedence Call Waiting [**Required**].
- b. Call Forwarding [**Required**].

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

SCM-002330 [Required: UC SIP Secure Voice EI] A UC SIP secure voice EI is not required to support any supplementary services for secure voice calls (calls using SCIP/modem relay media).

SCM-002340 [Required: UC SIP Secure Voice EI] A UC SIP secure voice EI shall be able to operate as an UC SIP voice EI for voice calls (calls using Audio media and not SCIP/modem relay media).

SCM-002350 [Required: UC SIP Secure Voice EI] A UC SIP secure voice EI shall be able to operate as an UC SIP voice EI for the portions of calls where Audio media is used (and SCIP/modem relay media is not used). This UC SIP secure voice EI requirement applies during the time before a call converts from Audio media to SCIP/modem relay media, and during the time after a call converts from SCIP/modem relay media back to Audio media. This requirement also applies to a call that never converts to SCIP/modem relay media, and uses Audio media for the lifetime of the call.

SCM-002360 [Required: UC SIP Secure Voice EI] A UC SIP Secure Voice EI shall not allow the end user to activate any supplementary services when a call on that EI is operating in “Secure Voice” mode, and SCIP/modem relay media is being used.

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

SCM-002370 [Required: UC SIP Secure Voice EI] Whenever the local end user returns the Secure Voice call to a Clear Voice call, or the remote end user returns the secure voice call to a clear voice call, the UC SIP secure voice EI shall return a “clear voice confirmation” indication (i.e., a locally generated tone and a visual display) to the local end user. This lets the local end user know that the call has returned from secure voice mode to clear voice mode. It also lets them know that they are no longer communicating in secure voice mode, and lets them know that they can activate supplementary services if desired.

SCM-002380 [Required: UC SIP Secure Voice EI] A UC SIP secure voice EI shall support supplementary services when all calls on that EI are operating in clear voice mode, and Audio media alone is being used.

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

SCM-002390 [Required: UC SIP Secure Voice EI] When operating as an UC SIP voice EI (i.e., all EI calls are in clear voice mode), a UC SIP secure voice EI shall support the following supplementary services for voice calls, consistent with [Section 2.2](#), Voice Features and Capabilities, using UC SIP signaling:

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

SCM-002400 [Required: UC SIP Secure Voice EI] When an UC SIP secure voice EI has a secure voice call active, the SC sends that EI a Precedence CW or ROUTINE CW indication, and the EI user attempts to place the secure voice call on hold and answer the waiting call, the EI shall send an error indication (tone and display) to the user as described previously. If the user converts the secure voice call back to a clear voice call, and then tries to place the clear voice call on hold and answer the waiting call, the EI shall accept the user's request and relay it to the SC.

SCM-002410 [Required: UC SIP Secure Voice EI] When an UC SIP secure voice EI has a secure voice call active, and the EI user attempts to activate Call Transfer by placing the secure voice call on hold and setting up another call, the EI shall send an error indication (tone and display) to the user as described previously. If the user converts the secure voice call back to a clear voice call, and then tries to activate Call Transfer by placing the clear voice call on hold and setting up another call, the EI shall accept the user's request and relay it to the SC.

SCM-002420 [Required: UC SIP Secure Voice EI] When an UC SIP secure voice EI has a secure voice call active, and the EI user attempts to activate Call Hold by placing the secure voice call on hold, the EI shall send an error indication (tone and display) to the user as described previously. If the user converts the secure voice call back to a clear voice call, and then tries to

activate Call Hold by placing the clear voice call on hold, the EI shall accept the user's request and relay it to the SC.

SCM-002430 [Required: UC SIP Secure Voice EI] When an UC SIP secure voice EI has a secure voice call active, and the EI user attempts to activate TWC by placing the secure voice call on hold and setting up another call, the EI shall send an error indication (tone and display) to the user as described previously. If the user converts the secure voice call back to a clear voice call, and then tries to activate TWC by placing the clear voice call on hold and setting up another call, the EI shall accept the user's request and relay it to the SC.

SCM-002440 [Required: UC SIP Secure Voice EI] When an UC SIP secure voice EI has a secure voice call active, and the SC sends that EI a Precedence CW or Routine CW indication and provides Calling Party ID and Precedence Level information within the CW indication, the UC SIP Secure Voice EI shall display both the Calling Party ID and Precedence Level information to the called user at the EI, as part of the CW indication that the EI delivers to the called user. (This gives the called users a basis for deciding whether to answer or ignore a "waiting" voice call when they have a secure voice call active on their EI. "Ignore," as used here, means that the user allows the call to be forwarded by the CFDA feature or deflected by the Precedence Call Diversion feature.)

2.9.6.4 Requirements for UC SIP Video EIs

SCM-002450 [Required: SC, SS] SCs shall support UC SIP Video EIs that use UC SIP for EI-to-SC signaling. The SCs shall support these UC SIP Video EIs using the UC SIP SC-to-UC SIP-EI interface defined in [Section 2.9.7](#), Multiple Call Appearance Requirements for UC SIP EIs, and in UC SIP 2013.

SCM-002460 [Required: UC SIP Video EI] The UC SIP Video EIs shall support UC SIP for EI-to-SC signaling. These UC SIP Video EIs shall support the UC SIP SC-to-UC SIP-EI interface defined in [Section 2.9.7](#), Multiple Call Appearance Requirements for UC SIP EIs, and in UC SIP 2013.

SCM-002470 [Optional: SC, SS, UC SIP Video EI] SCs, SSs, and UC SIP Video EIs may support the following supplementary services for video calls, as an extension of the requirement to support these services for voice calls in [Section 2.2](#), Voice Features and Capabilities:

- a. Precedence Call Waiting.
- b. Call Forwarding.
- c. Call Transfer.
- d. Call Hold.
- e. UC Conferencing.
- f. Three-Way Calling.

- g. Calling Number Delivery.
- h. Call Pickup.

SCM-002480 [Optional: SC, SS, UC SIP Video EI] SCs, SSs, and UC SIP Video EIs may support the following supplementary services for video calls:

- a. The SC and the UC SIP video EI may support the transmission of H.281 far-end camera control (FECC) messages when used in conjunction with video systems (e.g., MCUs and VTC bridges) that employ far-end camera control capabilities. The specific requirements for implementing this capability are provided in UC SIP 2013, Section 10.3.6.1, General H.224 Control Channel for Far-End Camera Control Messages, and in Section 10.3.6, FECC.
- b. The SC and the UC SIP Video EI may support (when used in multipoint conferences) the Binary Floor Control Protocol (BFCP) that uses a floor control server to manage the control of media streams that are shared resources (i.e., “floors”) as specified in RFC 4582. The specific requirements for implementing this capability are provided in Section 5.3.4.9.7.5, SDP Attributes for Binary Floor Control Protocol Streams.

SCM-002490 [Conditional: SC, SS, UC SIP Video EI] If SCs, SSs, and UC SIP Video EIs support the optional supplementary services noted above (within [Section 2.9.6.4](#)), they shall support them using UC SIP signaling.

SCM-002500 [Required: SC, SS, UC SIP Video EI] The SCs and UC SIP video EIs shall support a mechanism to limit the total number of video calls at that EI at any given time.

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

For UC SIP video EIs, the configured call limit for that EI shall be “one video call.” This is all that is required of UC SIP video EIs in the UCR.

SCM-002510 [Required: SC, SS, UC SIP Video EI] The SC and the UC SIP video EI shall support a mechanism to identify the amount of video call bandwidth (counted as Video Session Units) in use at that EI at any given time.

The SC and the UC SIP video EI shall keep track of the total amount of video call bandwidth (in VSU) in use at the UC SIP video EI at all times. (A 500-Kbps video call shall use one VSU of bandwidth, a 1-Mbps video call shall use two VSUs of bandwidth, a 2.5-Mbps video call shall use five VSU of bandwidth, and a 4.0-Mbps video call shall use eight VSUs of bandwidth.)

SCM-002520 [Required: SC, SS, UC SIP Video EI] The SC and the UC SIP video EI shall also support the conversion of a lower-bandwidth video call to a higher-bandwidth video call

(and vice-versa), using UC SIP re-INVITE messages on the SC-to-UC SIP-EI interface to signal the bandwidth change.

SCM-002530 [Required: SC, SS, UC SIP Video EI] The SC and the UC SIP video EI shall also support the conversion of a video call to a voice call (and vice-versa), using UC SIP re-INVITE messages on the SC-to-UC SIP-EI interface to signal the media change.

2.9.6.5 UC SIP Video EI Features

SCM-002540 [Conditional: UC SIP Video EI] If the UC SIP Video EI supports FECC based on the following:

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

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

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

SCM-002550 [Conditional: UC SIP Video EI] If the UC SIP Video EI supports BFCP based on the following:

- RFC 4582.
- RFC 4583.

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

- Section 5.3.4.9.7.5, SDP Attributes for Binary Floor Control Protocol Streams.

SCM-002560 [Conditional: UC SIP Video EI] If the UC SIP Video EI supports Video Channel Flow Control [VCFC] based on the following:

- RFC 4585.

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

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

SCM-002570 [Required: UC SIP Video EI] UC SIP Video EI shall support the following sections of RFC 4585:

- Section 3.1, Compound RTCP Feedback Packets.
- Section 3.2, Algorithm Outline.
- Section 3.3, Modes of Operation.

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

SCM-002580 [Conditional: UC SIP Video EI] If the UC SIP Video EI supports Video Channel Fast Update Requests (VCFURs) based on the following:

- RFC 5104.

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

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

SCM-002590 [Conditional: UC SIP Video EI] If the UC SIP Video EI supports VCFUR, Full Intra Request (FIR) payload-specific feedback message shall be used for implementing VCFUR.

2.9.7 Multiple Call Appearance Requirements for UC SIP EIs

2.9.7.1 Multiple Call Appearance Scenarios

The UC SIP 2013 document contains requirements on “Multiple Appearances” The first of these requirements is as follows:

“IP end instruments MUST be limited to two (2) appearances per DN and limited to, at most, two (2) DNs.”

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

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

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

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

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

2.9.7.2 Multiple Call Appearances – Specific Requirements

SCM-002600 [Required: UC SIP Voice EI, UC SIP Secure Voice EI] A UC SIP EI shall allow multiple call appearances of the same DN (10-digit DSN number) to be assigned to it. A UC SIP EI shall allow at least two appearances of the same DN to be assigned to it. This requirement does not apply to UC SIP Video EIs.

SCM-002610 [Required: UC SIP Voice EI, UC SIP Secure Voice EI] A UC SIP EI shall allow each call appearance of a DN to be used for voice and secure voice calls to and from that

DN. This requirement does not apply to UC SIP Video EIs. Dedication of call appearances on an EI to a particular call type (Voice, Secure Voice, or Video) is not a requirement.

SCM-002620 [Required: UC SIP Video EI] A UC SIP Video EI shall support one DN for video calls, and support one video call on that DN at a time. A UC SIP Video EI is not required to use a call appearance to support this single video call. A UC SIP Video EI that is also an UC SIP Voice EI (and supports voice calls and two voice call appearances) is not required to use either of its voice call appearances to support this video call.

SCM-002630 [Required: UC SIP Voice EI] A UC SIP Voice EI shall be able to support two simultaneous voice calls (media type equals Audio) using two call appearances of the same DN (10-digit DSN number).

SCM-002640 [Required: UC SIP Secure Voice EI] When operating as an UC SIP Voice EI (no Secure voice calls active), an UC SIP Secure Voice EI shall be able to support two simultaneous voice calls (media type equals Audio) using two call appearances of the same DN.

SCM-002650 [Required: UC SIP Secure Voice EI] When operating as an UC SIP Secure Voice EI (one Secure voice call active), an UC SIP Secure Voice EI shall be able to support one Secure voice call (media type equals modem relay) using one of its two call appearances. The EI may also support a voice call (media type equals Audio) on Hold using its other call appearance in this case.

SCM-002660 [Required: UC SIP Video EI] A UC SIP Video EI shall be able to support one video call (media type equals Video). If the UC SIP EI is also an UC SIP Voice EI or UC SIP Secure Voice EI, the EI is not required to use either of its voice call appearances to support the video call

SCM-002670 [Required: SC, SS, UC SIP Voice EI, UC SIP Secure Voice EI] The UC SIP EI and SC shall allow multiple media types to be requested (as part of SDP capability declaration) in the same EI-to-SC INVITE message.

SCM-002680 [Required: SC, SS, UC SIP Voice EI, UC SIP Secure Voice EI] The SC and UC SIP EI shall allow multiple media types to be requested (as part of SDP capability declaration) in the same SC-to-EI INVITE message.

SCM-002690 [Required: UC SIP Voice EI, UC SIP Secure Voice EI] A UC SIP EI shall only allow one voice call (voice or secure voice) to be associated with one call appearance at a time. An UC SIP EI shall not allow multiple calls (e.g., one active call and one held call) to be associated with the same call appearance at the same time.

SCM-002700 [Required: UC SIP Voice EI, UC SIP Secure Voice EI] A UC SIP EI shall allow multiple voice calls to be associated with itself, as long as each call is associated with one, and only one, call appearance on that UC SIP EI. A UC SIP EI shall allow each call associated with the EI to be in either an “active” state, a “held” state, or a “call in progress” state (a call in the process of being established).

SCM-002710 [Required: UC SIP Secure Voice EI] A UC SIP secure voice EI shall only allow one secure voice call (media equals modem relay) to be associated with the EI at a time, and allow that call to be associated with one call appearance on that EI. The UC SIP EI shall only allow this secure voice call to be in an “active” state, and not in a “held” state, or a “call in progress” state.

SCM-002720 [Required: UC SIP Secure Voice EI] When a secure voice call is active, the UC SIP secure voice EI shall also allow an additional voice call (media equals Audio) to be associated with the EI, and allow that call to be associated with the second call appearance on that EI. The UC SIP EI shall only allow this additional voice call to be in a “held” state or a “call in progress” state (a call in the process of being established), and not in an “active” state. For example, if the CW feature is assigned, the EI shall allow an active Secure voice call on one call appearance and an incoming “in progress” voice call on the other call appearance.

SCM-002730 [Required: UC SIP Voice EI, UC SIP Secure Voice EI] A UC SIP EI shall allow a call on a single call appearance to transition from one media type to another, using an in-band media message for a media change (like a V.150.1 modem relay SSE message). A UC SIP EI shall support transitions from voice media to secure voice media, and transitions from secure voice media to voice media.

2.9.7.3 Multiple Call Appearances – Interactions With Precedence Calls

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

SCM-002740 [Required: UC SIP Voice EI, UC SIP Secure Voice EI] When offering an incoming precedence call is offered on a multiple-call-appearance UC SIP EI, the EI shall do to the following:

- a. Play a precedence ringing tone for that call.
- b. Offer the call on the next available call appearance for the indicated DN.
- c. Provide a visual precedence level display to the end user.

SCM-002750 [Required: UC SIP Voice EI, UC SIP Secure Voice EI] The SC UC SIP EI shall then give the called user the option of either of the following:

- a. Placing the currently active call (on the currently active call appearance) on hold and picking up the incoming precedence call on the new call appearance.
- b. Ignoring the incoming precedence call on the new call appearance. “Ignoring,” as used here, means that the called user allows the call to be forwarded by the CFDA feature, or deflected by the Precedence Call Diversion feature.

SCM-002760 [Required: UC SIP Secure Voice EI] If the UC SIP EI is a secure voice EI and the currently active call is a secure voice call using modem relay media, the EI shall require the called user to convert the call back to a voice call using Audio media before placing it on hold. The UC SIP EI shall not allow a Secure voice call using modem relay media to be placed on hold.

SCM-002770 [Required: UC SIP Voice EI, UC SIP Secure Voice EI] The UC SIP voice EI shall offer subsequent incoming precedence calls to the end user, up to the total number of call appearances supported by the EI. For each additional incoming precedence call, the UC SIP EI shall offer the call as described previously, and allow the end user to place the existing active call on hold (if it is a voice call using Audio media) and answer the precedence call as described previously. This process of offering a new precedence call, placing an existing call on hold, and answering the precedence call shall remain the same until the UC SIP EI is saturated (i.e., all of its call appearances are in use).

SCM-002780 [Required: UC SIP Voice EI, UC SIP Secure Voice EI] When an UC SIP EI is saturated, and an incoming precedence call is made to that EI, the EI shall determine the lowest precedence call from all of the calls on all of the EI's call appearances (including those calls that are on hold), and shall preempt that call.

SCM-002790 [Required: UC SIP Voice EI, UC SIP Secure Voice EI] If this lowest precedence call is a call on hold, then the EI shall send a preemption tone to the remote party on the held call (the party on hold).

SCM-002800 [Required: UC SIP Voice EI, UC SIP Secure Voice EI] The UC SIP EI shall also send a preemption tone to the local party on this held call by playing this tone on the EI call appearance for this call.

SCM-002810 [Required: UC SIP Voice EI, UC SIP Secure Voice EI] After a preset period, the UC SIP EI shall clear this call on hold, and shall play a precedence ringing tone and provide a precedence level display on the call appearance where the held call has been cleared.

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

SCM-002820 [Required: UC SIP Voice EI, UC SIP Secure Voice EI] The UC SIP EI shall then give the called user the option of answering the call, or letting it forward to an alternate party (if CFDA is assigned), or letting it divert to an attendant (e.g., if Precedence Call Diversion is assigned).

SCM-002830 [Required: UC SIP Voice EI, UC SIP Secure Voice EI] If the lowest precedence call is not a call on hold, but instead is the active call at the EI, the UC SIP EI shall send a preemption tone to both the remote party and the local party on the active call (the local party on the active call appearance).

SCM-002840 [Required: UC SIP Voice EI, UC SIP Secure Voice EI] When the local party on the active call appearance goes “on hook,” the UC SIP EI shall offer the incoming precedence call to that party by playing a precedence ringing tone and providing a precedence level display on the call appearance where the active call has been cleared.

SCM-002850 [Required: UC SIP Voice EI, UC SIP Secure Voice EI] The UC SIP EI shall then give the called user the option of answering the call, or letting it forward to an alternate party (if CFDA is assigned), or letting it divert to an attendant (if Precedence Call Diversion is assigned).

SCM-002860 [Required: UC SIP Voice EI, UC SIP Secure Voice EI] In both of the previous cases (held call preempted and active call preempted), the UC SIP EI shall not preempt any of the other calls that are on hold (on any other the other call appearances), and shall allow the end user to retrieve any of those calls at any time.

SCM-002870 [Required: SC, SS, UC SIP Voice EI, UC SIP Secure Voice EI] In both previous cases above where the end user ignores the precedence call, and lets it either forward to an alternate party (via Call Forward Don’t Answer) or divert to an attendant (via Precedence Call Diversion), the SC and the UC SIP EI shall follow the requirements in [Section 2.2.1](#), Call Forwarding, that define the interaction between VVoIP precedence calls and CF.

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

SCM-002880 [Required: PEI, UEI, Secure UEI, TA with V.150.1, IAD with V.150.1] Whenever these types of IP EIs, TAs, or IADs use ITU-T Recommendation V.150.1, the following applies:

- a. ITU-T Recommendation V.150.1 provides for three states: audio, voiceband data (VBD), and modem relay. After call setup, inband signaling may be used to transition from one state to another. In addition, ITU-T Recommendation V.150.1 provides for the transition to FoIP using Fax Relay per ITU-T Recommendation T.38.
- b. When the product uses ITU-T Recommendation V.150.1 inband signaling to transition between audio, FoIP, modem relay, or VBD states or modes, the product shall continue to use the established session’s protocol [e.g., decimal 17 for User Datagram Protocol (UDP)] and port numbers so that the transition is transparent to the SBC.

2.9.9 UC Products With Non-Assured-Services Features

SCM-002890 [Conditional: All UC APL Products identified in the UCR Session Control and Auxiliary Services Sections] If the UC product has a component that provides Non-Assured-Services Features (Non-ASFs), and these Non-ASFs do not affect any of the product's Assured-Services Features (ASFs), then all voice or video sessions within the UC product with precedence above ROUTINE that are offered to a Non-ASF component (for example, a Non-

ASF End Instrument or Automatic Call Distributor) shall be diverted immediately to an attendant console station.

SCM-002900 [Optional: SC] The SC may support Non-Assured-Service EIs.

SCM-002910 [Conditional: SC] If the SC supports Non-Assured-Service EIs, then it shall support Assured-Service EIs that are included in the SC SUT.

2.9.10 ROUTINE-Only EIs

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

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

SCM-002920 [Conditional: SC] If an SC supports ROUTINE-only voice EIs, it shall also support voice EIs that fully support precedence and preemption.

SCM-002930 [Optional: SC] An SC may support ROUTINE-only video EIs without providing support for video EIs that fully support precedence and preemption.

SCM-002940 [Required: SC, ROEI] ROEIs shall not be able to originate precedence (i.e., PRIORITY and above) calls.

SCM-002950 [Required: SC] Precedence calls to ROUTINE-only EIs that are busy shall be diverted to an attendant.

SCM-002960 [Required: SC] Precedence calls to ROUTINE-only EIs that are not answered shall be diverted to an attendant.

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

SCM-002970 [Required: SC, ROEI] Sessions involving ROUTINE-only EIs affect ASAC Session Counts in the same way as sessions involving EIs that fully support precedence and preemption.

SCM-002980 [Required: SC, ROEI, non-RO EI] MLPP/PBAS requirements shall apply to non-ROUTINE only (RO) EIs in sessions involving both RO and non-RO EIs.

SCM-002990 [Optional: SC, ROEI] Preemption Tone may be provided to ROUTINE-only EIs on preempted sessions involving both ROUTINE-only and non-RO EIs.

SCM-003000 [Optional: ROEI] A ROUTINE-only EI may display the precedence level of the session on which it participates, but is not required to do so.

SCM-003010 [Optional: ROEI] A ROUTINE-only EI may support UC SIP signaling, but will be tested and certified as a PEI, with the precedence and preemption exceptions noted above in this section.

2.10 SESSION CONTROLLER

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

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

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

2.10.1 PBAS/ASAC

SCM-003020 [Required: SC] The SC shall meet all the requirements for Precedence-Based Assured Services (PBAS) and ASAC, as appropriate for VoIP and Video over IP services, as specified in [Section 2.26.1](#), Multilevel Precedence and Preemption and [Section 2.3](#), ASAC.

2.10.2 SC Signaling

SCM-003030 [Required: SC] The SC shall support UC SIP over IP for signaling to UC SIP End Instruments (UEI) and Softswitches (SS).

SCM-003040 [Optional: SC] The SC may support proprietary VVoIP signaling to interface with Proprietary End Instruments (PEI).

2.10.3 Session Controller Location Service

SCM-003050 [Required: SC] The SC shall support a Session Controller Location Service (SCLS) functionality that provides information on call routing and called address translation (where a called address is contained within the called SIP URI in the form of the called number). The CCA uses the routing information stored in the SCLS to route the following:

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

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

2.10.4 SC Management Function

SCM-003060 [Required: SC] The SC shall support the applicable Fault, Configuration, Accounting, Performance, and Security (FCAPS) management and audit log requirements provided in the following:

- [Section 2.19](#), Management of Network Appliances.
- [Section 2.20](#), Accounting Management.

2.10.5 SC-to-VVoIP EMS Interface

SCM-003070 [Required: SC] The SC shall provide an interface to the DISA VVoIP EMS. The interface consists of a 10/100-Mbps Ethernet connection as specified in [Section 2.7.4](#), DISA VVoIP EMS Interface.

2.10.6 SC Transport Interface Functions

SCM-003080 [Required: SC] The SC shall provide Transport Interface functions to interface with the ASLAN and its IP packet transport network. Examples of Transport Interface functions include the following:

- a. Network Layer functions: IP, IP security (IPSec).
- b. Transport Layer functions: IP Transport Protocols (TCP, UDP, TLS).
- c. LAN Protocols.

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

- Each PEI or UEI served by the SC.
- Each MG served by the SC (even though the MG may be physically connected to the CCA/MGC over an internal proprietary interface, instead of being connected logically to the CCA/MGC over the ASLAN).
- The CCA/IWF/MGC itself.
- The SBC (for SC, PEI, UEI, and MG communication with other SCs, SSs, PEIs, UEIs, and MGs over the DISN WAN).

2.10.7 Custom Line-Side Features Interference

SCM-003090 [Optional: SC] Vendors may implement unique custom features applicable to the line side of the SC.

SCM-003100 [Conditional: SC] If custom line-side features are implemented they shall not interfere with the Assured Services requirements.

2.10.8 Loop Avoidance for SCs

SCM-003110 [Required: SC] During the call establishment process, the product shall be capable of preventing or detecting and stopping hairpin routing loops over American National Standards Institute (ANSI) T1.619a and commercial PRI trunk groups (i.e., T1 PRI and E1 PRI) between a legacy switch (e.g., TDM EO) and an SC (see [Figure 2.10-1](#), Example of a Hairpin Routing Loop). The Loop Avoidance mechanism shall not block call requests that are legitimately redirected or forwarded between the two interconnected products. In the event that a routing loop is detected, the SC shall clear the call in the backwards direction, either sending a 404 (Not Found) response to a SIP originator, or an ISDN DISCONNECT message (from the MG) to a TDM originator. The SC shall provide a VCA to the caller in each case.

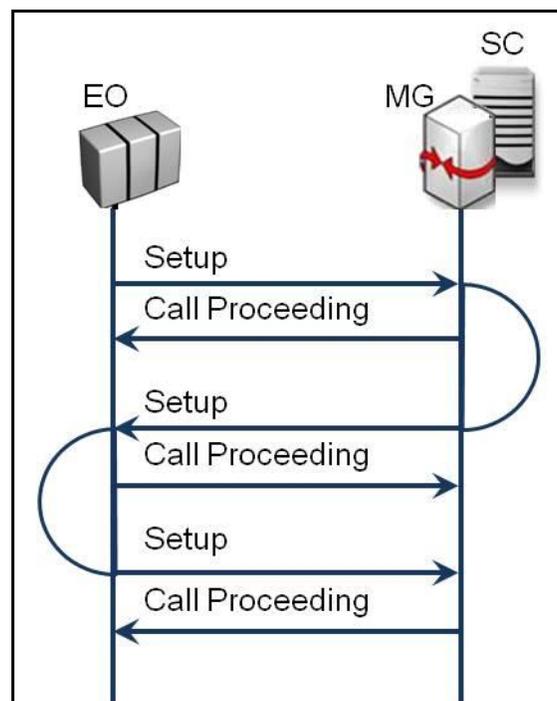


Figure 2.10-1. Example of a Hairpin Routing Loop

2.10.9 Local Session Controller Application

The requirements in this section are unique to the distributed application for the Session Controller.

2.10.9.1 Service Requirements Under Total Loss of WAN Transport Connectivity

SCM-003120 [Required: SC] In the event that a total loss of connectivity to the DISN WAN occurs, the SC shall provide the following functions:

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

2.11 UC SIP GATEWAYS

2.11.1 UC SIP TDM Gateway

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

[Table 2.11-1](#), Summary of UC SIP TDM Gateway Functions, provides a summary of UC SIP TDM Gateway functions.

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

FUNCTION	DESCRIPTION
Session Control and Signaling	Signaling interworking ANSI T1.619a PRI non-ANSI T1.619a PRI [Optional] UC SIP Call stateful, maintains local active session state knowledge (including precedence level)
Network Management	Provides traffic call information to and responds to traffic flow control commands from, an EMS
MGC	Required
MG	Interworking of B-channel PCM with SRTP/UDP/IP packets Generation and receipt/processing of SRTCP/UDP/IP packets Delivery of Q.931 messages Assignment of appropriate value to DSCP field when generating SRTP/UDP/IP packets
LEGEND	
UC SIP: Unified Capabilities Session Initiation Protocol	EMS: Electronic Message System
DSCP: Differentiated Services Code Point	PCM: Pulse Code Modulation
IP: Internet Protocol	PRI: Primary Rate Interface
ISDN: Integrated Services Digital Network	SRTCP: Secure Real-Time Transport Control Protocol
MG: Media Gateway	SRTP: Secure Real-Time Transport Protocol
MGC: Media Gateway Controller	UDP: User Datagram Protocol

FUNCTION	DESCRIPTION
	MLLP: Multilevel Precedence and Preemption

SCM-003130 [Required] The UC SIP TDM Gateway shall support the ANSI T1.619a PRI TDM interface.

SCM-003140 [Optional] The UC SIP TDM Gateway may support non-ANSI T1.619a PRI TDM interfaces.

2.11.1.1 UC SIP TDM Gateway Signaling

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

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

FUNCTIONAL COMPONENT	VOIP AND VIDEO SIGNALING INTERFACES	VOIP AND VIDEO SIGNALING PROTOCOLS
CCA	CCA (UC SIP TDM Gateway) – to – CCA (SS)	UC SIP over IP
CCA/MGC and MG	CCA (MGC) – to – MG	Internal interface to integrated MG functional component (used with ANSI T1.619a PRI trunks and optional non-ANSI T1.619a PRI trunks)
LEGEND		
CCA: Call Connection Agent	MG: Media Gateway	SS: Softswitch
IP: Internet Protocol	MGC: Media Gateway Controller	TDM: Time Division Multiplexing
MLPP: Multilevel Precedence and Preemption	PRI: Primary Rate Interface	UC SIP: Unified Capabilities Session Initiation Protocol

SCM-003150 [Required] The UC SIP TDM Gateway shall provide signal interworking between the connected TDM switch and the designated SS. The signaling protocol for interfacing with the SS shall be UC SIP over IP.

SCM-003160 [Required] When the UC SIP TDM Gateway receives a SETUP message from aANSI T1.619a PRI, the UC SIP TDM Gateway shall interwork the SETUP message to a UC SIP INVITE and forward the UC SIP INVITE to the SBC. The MLPP IE network identity digits, precedence level bits, and service domain shall be interworked into the Resource-Priority header's network domain subfield, r-priority field, and precedence domain subfield, respectively, consistent with UC SIP 2013.

The UC SIP TDM Gateway shall add a CCA-ID parameter to the Contact header.

The UC SIP TDM Gateway shall add a route set comprising two Route headers where the first Route header is the SIP URI for the SBC at the enclave, and the second Route header is the SIP URI for the SBC serving the SS.

SCM-003170 [Required] When the UC SIP TDM Gateway receives an UC SIP INVITE from the SS via the SBC intended for a ANSI T1.619a PRI, the UC SIP TDM Gateway shall interwork the INVITE to a SETUP message and forward the SETUP message on the D-channel.

SCM-003180 [Required] The UC SIP TDM Gateway shall interwork INVITEs received from the SBC to the TDM switch, even if all DS0s are currently in use.

2.11.1.2 SIP URI and Mapping of Telephone Number

SCM-003190 [Required] When the UC SIP TDM Gateway receives a call request over an ANSI T1.619a PRI then the UC SIP TDM Gateway shall map the telephony numbers received from the Q.931 SETUP message to SIP URIs IAW UC SIP 2013, Section 12.3, SIP URI and Mapping of Telephony Number into SIP URI, and Section 4.6, SIP URI and Mapping of Telephone Number into SIP URI.

2.11.1.3 UC SIP TDM Gateway Media

SCM-003200 [Required] The UC SIP TDM Gateway MG shall support the ITU-T Recommendation G.711 (μ -law and A-law) audio codec and shall perform A-law/ μ -law conversion when needed.

SCM-003210 [Required] The UC SIP TDM Gateway MG shall support RFC 4040 and the signaling for establishing the 64kbps unrestricted bearer per UC SIP 2013, Section 4.7, 64 Kbps Transparent Calls (Clear Channel).

SCM-003220 [Required] The UC SIP TDM Gateway MG shall support T.38 Fax Relay (see [Section 2.16.8.9](#), MG Support for Group 3 Fax Calls).

SCM-003230 [Required] The UC SIP TDM Gateway MG shall support the SCIP-216 subset of V.150.1 Modem Relay (see [Section 2.21.1](#), SCIP/V.150.1 Gateway) and the UC SIP signaling requirements in support of modem relay (See UC SIP 2013, Section 11.1, UC SIP Signaling Requirements in Support of Modem Relay-Capable Gateways).

2.11.1.4 Information Assurance

SCM-003240 [Required] The UC SIP TDM Gateway shall satisfy the Information Assurance requirements in Section 4, Information Assurance for a media gateway.

2.11.1.5 UC SIP TDM Gateway Management Function

SCM-003250 [Required] The CCA shall interact with the UC SIP TDM Gateway Management function by doing the following:

- a. Making changes to its configuration in response to commands from the Management function that requests these changes.
- b. Returning information to the Management function on its FCAPS, in response to commands from the Management function that requests this information.
- c. Sending information to the Management function on a periodic basis (e.g., on a set schedule), keeping the Management function up-to-date on CCA activity.

2.11.1.6 UC SIP TDM Gateway-to-EMS Interface

SCM-003260 [Required] The UC SIP TDM Gateway shall provide an interface to the DISA VVoIP EMS. The interface shall consist of a 10/100-Mbps Ethernet connection, as specified in [Section 2.7.4](#), DISA VVoIP EMS Interface.

2.11.2 UC SIP IP Gateway

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

The UC SIP IP Gateway is a VVoIP interworking appliance, and its purpose is to enable the interconnection and interoperation of proprietary IP-based UC signaling platforms and their associated IP EIs with the DISN UC system to support E2E voice and video sessions. The UC SIP IP Gateway directly interfaces with only one IP-based UC signaling platform, does NOT support interworking of TDM-based signaling platforms, and does NOT serve as a call manager for any TDM or IP EIs.

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

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

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

FUNCTION	DESCRIPTION
SCS	Verifies call request is consistent with SAC: Signaling interworking (proprietary to UC SIP; UC 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	
EMS: Electronic Message System	SCS: Session Control and Signaling

FUNCTION	DESCRIPTION
IP: Internet Protocol	SRTP: Secure Real-time Transport Protocol
IWF: Interworking Function	UC SIP: Unified Capabilities Session Initiation Protocol
NM: Network Management	UCR: Unified Capabilities Requirements
SAC: Session Admission Control	UDP: User Datagram Protocol

SCM-003270 [Required] The UC SIP IP Gateway shall implement call count thresholds for voice sessions and for video sessions in order to perform Session Admission Control (SAC). See [Section 2.11.3.4](#), Session Admission Control, for more details.

2.11.2.1 UC SIP IP Gateway Call Request Processing

SCM-003280 [Required] When the UC SIP IP Gateway receives a call request from the proprietary UC signaling platform then the UC SIP IP Gateway shall:

- a. Check the appropriate (voice or video) call count (and outbound call count in the case of directionalization) to determine whether there are available bandwidth resources to support the call request.
- b. If the new call request would not exceed the appropriate (voice or video) call count threshold (and outbound call count threshold) then the UC SIP IP Gateway interworks the call request by doing the following:
 - (1) Incrementing the call count (and outbound call count in the case of directionalization).
 - (2) Generating a “routine” level UC SIP INVITE that advertises equivalent capabilities to those specified in the received call request.
 - (3) Adding a CCA-ID parameter to the Contact header.
 - (4) Adding a route set comprising two Route headers where the first Route header is the SIP URI for the SBC at the enclave, and the second Route header is the SIP URI for the SBC serving the SS.
 - (5) Forwarding the INVITE message to the SBC at the enclave.

SCM-003290 [Required] If the appropriate (voice or video) call count (or outbound call count) is at threshold or the call request would cause the UC SIP IP Gateway to exceed the call count threshold (or outbound call count threshold) then the UC SIP IP Gateway shall reject the call.

NOTE: If the proprietary signaling interface is SIP, then the response message shall be 488 (Not Acceptable Here) and may include an optional Warning header field with warning code 370 (Insufficient Bandwidth).

2.11.2.2 SS Policing Requirements When Serving an UC SIP IP Gateway

SCM-003300 [Required: SS] The UC SIP IP Gateway only sends routine UC SIP INVITEs to the SS, and the SS shall apply the standard ASAC policing rules for outbound routine voice and video requests.

See UC SIP 2013, Requirements 7.2.8, 7.2.10, 7.2.11, and 7.2.12 for policing routine outbound telephony requests.

See UC SIP 2013, Requirements 7.3.9, 7.3.11, 7.3.12, and 7.3.13 for policing routine outbound video requests.

SCM-003310 [Required: SS] When a SS receives an initial “routine” UC SIP INVITE intended for forwarding to a served UC SIP IP Gateway, the SS shall apply the standard ASAC policing rules for inbound routine voice and video requests.

See UC SIP 2013, Requirements 7.2.13, 7.2.13.1, 7.2.13.3, 7.2.13.4, 7.2.13.5, 7.2.14, 7.2.14.1, 7.2.14.2, 7.2.14.5, 7.2.14.6, 7.2.14.7, 7.2.14.8, 7.2.14.9, 7.2.14.10, 7.2.15, 7.2.15.1, 7.2.15.3, 7.2.15.4, and 7.2.15.5 for policing inbound routine telephony requests.

See UC SIP 2013, Requirements 7.3.14, 7.3.14.1, 7.3.14.3, 7.3.14.4, 7.3.14.5, 7.3.14.6, 7.3.15, 7.3.15.1, 7.3.15.3, 7.3.15.4, 7.3.15.5, and 7.3.15.6 for policing inbound routine video requests.

SCM-003320 [Required: SS] When a SS receives an initial precedence UC SIP INVITE intended for forwarding to a served UC SIP IP Gateway, the SS shall implement one of the following two policing rules:

- a. **[Preferred]** Forward the UC SIP INVITE to the UC SIP IP Gateway and if the UC SIP IP Gateway responds with either a 1xx response code greater than 100 or a 2xx response and the call request would cause the appropriate (voice or video) call count threshold (or inbound call count threshold) to be exceeded then the SS:
 - (1) Sends a 488 (Not Acceptable Here) response code to the remote initiating party of the UC SIP INVITE that may include a Warning header field with warning code 370 (Insufficient Bandwidth).
 - (2) Sends a CANCEL request (in the case of a 1xx response code) or a BYE request (in the case of a 2xx response code) to the local UC SIP IP Gateway.

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

- b. **[Alternative]** (Standard ASAC Policing Rules for precedence call request) Forward the UC SIP INVITE to the UC SIP IP Gateway and if the UC SIP IP Gateway responds with either a 1xx response code greater than 100 or a 2xx response and the call request would cause the appropriate (voice or video) call count threshold (or inbound call count threshold) to be exceeded, then the SS applies the standard ASAC policing rules for a

precedence call request. That is, the SS preempts a ROUTINE or lesser precedence call by sending a BYE request with a reason header for preemption to the UC SIP IP Gateway. The UC SIP IP Gateway shall ignore the reason header for preemption, interwork the BYE to the proprietary UC signaling platform, and respond with a 200 (OK) response. The routine or lesser precedence call will be terminated and the SS will forward the 1xx response greater than 100 or the 2xx response to the precedence inbound call request over the UC WAN.

2.11.2.3 Chg1-5.3.2.7.5.3.1 UC SIP IP Gateway SCS

[Table 2.11-4](#), UC SIP IP Gateway support for VoIP and Video Signaling Interfaces, provides a complete list of the UC SIP IP Gateway signaling requirements. NOTE: the term proprietary signaling encompasses any vendor proprietary signaling, SIP, H.323, or other signaling protocol transported over IP that is not UC SIP.

Table 2.11-4. UC SIP IP Gateway Support for VoIP and Video Signaling Interfaces

FUNCTIONAL COMPONENT	VOIP AND VIDEO SIGNALING INTERFACES	VOIP AND VIDEO SIGNALING PROTOCOLS
CCA	CCA (UC SIP IP Gateway) – to – CCA (SS)	UC SIP over IP
CCA	CCA (UC SIP IP Gateway) – to – proprietary UC signaling platform	Proprietary signaling over IP
LEGEND		
CCA: Call Connection Agent		UC: Unified Capabilities
IP: Internet Protocol		UC SIP: Unified Capabilities Session Initiation Protocol
SS: Softswitch		VoIP: Voice over IP

2.11.2.3.1 Chg1-5.3.2.7.5.3.1.1 CCA Function

The CCA is part of the SCS functions and includes the IWF (signaling) function.

SCM-003330 [Required] The CCA IWF shall support the UC SIP consistent with the detailed UC SIP requirements in UC SIP 2013.

SCM-003340 [Required] The CCA IWF shall secure the UC SIP protocol using TLS, as described in Section 4, Information Assurance.

SCM-003350 [Required] The CCA IWF component of the UC SIP IP Gateway shall ensure that when the supplementary services enumerated in the UCR (i.e., Call Hold, Call Waiting, Precedence Call Waiting, Call Forwarding, Call Transfer) are performed by a served proprietary UC signaling platform that the UC SIP IP Gateway presents UCR-compliant call flows to the signaling appliances in the UC network per UC SIP 2013, Section 9.

2.11.2.3.2 Chg1-5.3.2.7.5.3.1.2 AS Precedence Capability Requirements and Resource Priority Header

SCM-003360 [Required] Whenever the UC SIP IP Gateway receives a proprietary signaling message from the proprietary UC signaling platform that translates it into an INVITE, UPDATE, or REFER request, then the UC SIP IP Gateway shall generate a Resource-Priority header having a ROUTINE priority level IAW UC SIP 2013, Section 6.1, Precedence Level Communicated over SIP Signaling.

SCM-003370 [Required] Whenever the UC SIP IP Gateway receives an INVITE, UPDATE, or REFER request from the SS via the SBC, then the UC SIP IP Gateway shall process the Resource-Priority header to distinguish a ROUTINE call from a precedence call.

SCM-003380 [Required] When an UC SIP IP Gateway receives an initial ROUTINE UC SIP INVITE (i.e., not a re-INVITE) from the SS (via the SBC), then the UC SIP IP Gateway shall:

- a. Check the appropriate (voice or video) call count (and inbound call count in the case of directionalization) to determine whether there are available bandwidth resources to support the call request.
- b. If the new call request would not exceed the appropriate (voice or video) call count threshold (and inbound call count threshold) then the UC SIP IP Gateway increments the appropriate (voice or video) call count (and inbound call count) and interworks the INVITE to the signaling protocol of the proprietary UC signaling platform.
- c. If the appropriate (voice or video) call count (or inbound call count) is at threshold or the call request would cause the UC SIP IP Gateway to exceed the appropriate (voice or video) call count threshold (or inbound call count threshold) then the UC SIP IP Gateway shall reject the call. NOTE: The response message is 488 (Not Acceptable Here) and may include a Warning header field with warning code 370 (Insufficient Bandwidth).

SCM-003390 [Required] The UC SIP IP Gateway shall support the following 2 methods for processing initial precedence UC SIP INVITEs received from the SS via the SBC and the choice of method shall be software configurable:

- a. Upon receipt of the initial precedence UC SIP INVITE request the UC SIP IP Gateway diverts the precedence INVITE to the attendant, or
- b. Upon receipt of the initial precedence UC SIP INVITE request the UC SIP IP Gateway determines whether the appropriate (voice or video) call count (or inbound call count in the case of directionalization) is at threshold or whether the call request would cause the UC SIP IP Gateway to exceed the appropriate (voice or video) call count threshold or inbound call count threshold:
 - (1) If the precedence UC SIP INVITE would cause the appropriate (voice or video) call count threshold (or inbound call count threshold) to be exceeded, then the precedence UC SIP INVITE is forwarded to the attendant.

NOTE: The UC SIP IP Gateway shall NOT conduct preemption on behalf of an inbound precedence UC SIP INVITE.

- (2) If the precedence UC SIP INVITE would NOT cause the appropriate call count threshold (or inbound call count threshold) to be exceeded, then the UC SIP IP Gateway treats the inbound precedence UC SIP INVITE request as if it were a routine inbound call request and increments the appropriate (voice or video) call count (and inbound call count) and interworks the INVITE to the signaling protocol of the proprietary UC signaling platform.

2.11.2.3.3 Chg1-5.3.2.7.5.3.1.3 SIP URI and Mapping of Telephone Number

SCM-003400 [Required] When the UC SIP IP Gateway receives a call request from the proprietary UC signaling platform, then the UC SIP IP Gateway shall map the telephony numbers received from the initial proprietary signaling message to SIP URIs IAW UC SIP 2013, Sections 12.3, SIP URI and Mapping of Telephony Number into SIP URI, and 4.6, SIP URI and Mapping of Telephone Number into SIP URI.

2.11.2.3.4 Chg1-5.3.2.7.5.3.1.4 Session Admission Control

SCM-003410 [Required] [Chg1-5.3.2.7.5.3.1.4.1] The UC SIP IP Gateway shall conduct SAC as detailed in this section in lieu of the ASAC required for SCs.

SCM-003420 [Optional] [Chg1-5.3.2.7.5.3.1.4.2] The UC SIP IP Gateway may support directionalization.

NOTE: Whenever the proprietary UC signaling platform supports directionalization, then directionalization will be performed in the proprietary UC signaling platform and not in the UC SIP IP Gateway.

SCM-003430 [Conditional] [Chg1-5.3.2.7.5.3.1.4.3] If the proprietary UC signaling platform does not support code blocking then the UC SIP IP Gateway shall support code blocking.

SCM-003440 [Required] [Chg1-5.3.2.7.5.3.1.4.4] The UC SIP IP Gateway shall support configuration of total voice call thresholds and total video call thresholds.

SCM-003450 [Optional] [Chg1-5.3.2.7.5.3.1.4.5] The UC SIP IP Gateway may support configuration of outbound voice call thresholds, inbound voice call thresholds, outbound video call thresholds, and inbound video call thresholds.

SCM-003460 [Required] [Chg1-5.3.2.7.5.3.1.4.6] Session Admission Control (SAC) refers to the enforcement of voice and video session thresholds whereby the UC SIP IP Gateway shall:

- a. Reject call requests received from the proprietary UC signaling platform that would exceed the appropriate (voice or video) call count threshold (or outbound call count threshold)

- b. Reject initial routine INVITES (i.e., not re-INVITES) received from the SS that would exceed the appropriate (voice or video) call count threshold (or inbound call count threshold).
- c. Per the requirement for precedence calls in [Section 2.11.2.3.2](#), either divert all precedence INVITES to the attendant, or divert the precedence INVITE to the attendant if the INVITE would cause the appropriate (voice or video) call count threshold (or inbound call count threshold) to be exceeded.

2.11.2.4 Chg1-5.3.2.7.5.3.2 UC SIP IP Gateway Media Interworking

SCM-003470 [Required] The UC SIP IP Gateway shall support the audio Codecs in [Section 2.9.1.3](#), Audio Codecs, Voice Instruments.

SCM-003480 [Required] The UC SIP IP Gateway shall comply with [Section 2.9.1.5](#), Voice over IP Sampling Standard, for the sampling rates.

SCM-003490 [Required] The UC SIP IP Gateway shall support the audio and video Codecs as specified in [Section 2.9.3.3](#), Video Codecs (Including Associated Audio Codecs).

SCM-003500 [Required] The voice media packets generated by the IP EIs served by the proprietary UC signaling platform that are intended for a destination outside the enclave shall be interworked by the UC SIP IP Gateway into UCR-compliant voice packets that shall be sent to the SBC.

SCM-003510 [Required: SBC] The enclave SBC shall send the UCR-compliant voice media packets received from the UC WAN and intended for the IP EIs served by the proprietary UC signaling platform to the UC SIP IP Gateway.

SCM-003520 [Required] The UC SIP IP Gateway shall interwork the UCR-compliant voice media packets received from the SBC into the proprietary voice media packets used by the IP EIs, and then the proprietary voice media packets shall be forwarded to the IP EIs.

SCM-003530 [Required] The video media packets generated by the IP EIs served by the proprietary UC signaling platform that are intended for a destination outside the enclave shall be interworked by the UC SIP IP Gateway into UCR-compliant video packets that shall be sent to the SBC.

SCM-003540 [Required: SBC] The enclave SBC shall send the UCR-compliant video media packets received from the UC WAN and intended for the IP EIs served by the proprietary UC signaling platform to the UC SIP IP Gateway.

SCM-003550 [Required] The UC SIP IP Gateway shall interwork the UCR-compliant video media packets received from the SBC into the proprietary video media packets employed by the IP EIs and then the proprietary video media packets shall be forwarded to the IP EIs.

2.11.2.5 Chg1-5.3.2.7.5.3.3 Information Assurance

SCM-003560 [Required] The UC SIP IP Gateway shall satisfy the Information Assurance requirements in Section 4, Information Assurance, for a media gateway.

2.11.2.6 UC SIP IP Gateway Management Function

SCM-003570 [Required] The CCA shall interact with the UC SIP IP Gateway Management function by doing the following:

- a. Making changes to its configuration in response to commands from the Management function that requests these changes.
- b. Returning information to the Management function on its FCAPS, in response to commands from the Management function that requests this information.
- c. Sending information to the Management function on a periodic basis (e.g., on a set schedule), keeping the Management function up-to-date on CCA activity.

2.11.2.7 UC SIP TDM Gateway-to-EMS Interface

SCM-003580 [Required] The UC SIP IP Gateway shall provide an interface to the DISA VVoIP EMS. The interface shall consist of a 10/100-Mbps Ethernet connection, as specified in [Section 2.7.4](#), DISA VVoIP EMS Interface.

2.11.3 UC SIP – H.323 Gateway

NOTE: Requirements in this section apply to either the UC SIP – H.323 Gateway or the Softswitch (SS) product. Requirements in this section that do not include an SS product qualifier are UC SIP – H.323 Gateway requirements.

The UC SIP – H.323 Gateway is a VVoIP interworking appliance, and its purpose is to enable the interconnection and interoperation of H.323 IP-based UC signaling platforms and their associated IP EIs with the DISN UC system to support E2E voice and video sessions.

The Government has adopted RFC 4123 – Session Initiation Protocol (SIP) – H.323 Interworking Requirements as the document which describes the requirements for the UC SIP – H.323 Gateway. Internet draft-agrawal-sip-h323-interworking-01.txt is cited as guidance to be used in implementing the UC SIP – H.323 Gateway. The following contents of this section are additional Government requirements.

NOTE: The UC SIP – H.323 Gateway is not an assured services appliance.

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

The UC SIP – H.323 Gateway provides interworking functions for the signaling and bearer planes (see [Table 2.11-5](#), Summary of UC SIP – H.323 Gateway Functions).

Table 2.11-5. Summary of UC SIP – H.323 Gateway Functions

FUNCTION	DESCRIPTION
SCS	Verifies call request is consistent with SAC: Signaling interworking (H.323 to UC SIP; UC 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	
EMS: Element Management System	SCS: Session Control and Signaling
IP: Internet Protocol	SRTP: Secure Real-time Transport Protocol
IWF: Interworking Function	UC SIP: Unified Capabilities Session Initiation Protocol
NM: Network Management	UCR: Unified Capabilities Requirements
SAC: Session Admission Control	UDP: User Datagram Protocol

SCM-003590 [Required] From a signaling perspective, the UC SIP – H.323 Gateway shall offer a UC SIP-compliant signaling interface that provides end-to-end signaling interoperability between the UC SIP – H.323 Gateway SUT and the UC SIP signaling appliances of the DISN UC WAN system.

From a media perspective, the UC SIP – H.323 Gateway shall offer a UCR-compliant bearer interface that provides E2E interoperability for voice and video media packets between the UC SIP – H.323 Gateway SUT and SBCs, IP EIs of SC SUTs, MGs, and UC SIP EIs. The UC SIP – H.323 Gateway shall interwork the voice and video media packets generated by the IP EIs served by the IP-based UC signaling platform and intended for a destination outside the H.323 system enclave to UCR-compliant SRTP/UDP packets having the appropriate DSCP. Similarly, UCR-compliant SRTP/UDP voice and video media packets received from the UC WAN and intended for the IP EIs served by the H.323 UC signaling platform shall be interworked by the UC SIP – H.323 Gateway into the H.323 media packets supported by the IP EIs.

SCM-003600 [Required] The UC SIP – H.323 Gateway shall implement call count thresholds for voice sessions and for video sessions in order to perform Session Admission Control (SAC). See [Section 2.11.3.6](#), Session Admission Control, for more details.

2.11.3.1 UC SIP – H.323 Gateway Call Request Processing

SCM-003610 [Required] ASF-2104210 When the UC SIP – H.323 Gateway receives a call request from the H.323 UC signaling platform then the UC SIP – H.323 Gateway shall:

- a. Check the appropriate (voice or video) call count (and outbound call count in the case of directionalization) to determine whether there are available bandwidth resources to support the call request.
- b. If the new call request would not exceed the appropriate (voice or video) call count threshold (and outbound call count threshold) then the UC SIP – H.323 Gateway interworks the call request by doing the following:
 - (1) Incrementing the call count (and outbound call count in the case of directionalization).
 - (2) Generating a “routine” level UC SIP INVITE that advertises equivalent capabilities to those specified in the received call request.
 - (3) Adding a CCA-ID parameter to the Contact header.
 - (4) Adding a route set comprising two Route headers where the first Route header is the SIP URI for the SBC at the enclave, and the second Route header is the SIP URI for the SBC serving the SS.
 - (5) Forwarding the INVITE message to the SBC at the enclave
- c. If the appropriate (voice or video) call count (or outbound call count) is at threshold or the call request would cause the UC SIP – H.323 Gateway to exceed the call count threshold (or outbound call count threshold) then the UC SIP – H.323 Gateway shall reject the call.

2.11.3.2 SS Policing Requirements When Serving a UC SIP – H.323 Gateway

SCM-003620 [Required: SS] ASF-2104310 The UC SIP – H.323 Gateway only sends routine UC SIP INVITEs to the SS, and the SS shall apply the standard ASAC policing rules for outbound routine voice and video requests.

See UC SIP 2013, Requirements 7.2.8, 7.2.10 through 7.2.12 for policing routine outbound telephony requests.

See UC SIP 2013, Requirements 7.3.9, 7.3.11 through 7.3.13 for policing routine outbound video requests.

SCM-003630 [Required: SS] ASF-2104320 When a SS receives an initial “routine” UC SIP INVITE request intended for forwarding to a served UC SIP – H.323 Gateway, the SS shall apply the standard ASAC policing rules for inbound routine voice and video requests.

See UC SIP 2013, Requirements 7.2.13, 7.2.13.1, 7.2.13.3 through 7.2.13.5, 7.2.14, 7.2.14.1, 7.2.14.2, 7.2.14.5 through 7.2.14.10, 7.2.15, 7.2.15.1, 7.2.15.3 through 7.2.15.5 for policing inbound routine telephony requests.

See UC SIP 2013, Requirements 7.3.14, 7.3.14.1, 7.3.14.3 through 7.3.14.6, 7.3.15, 7.3.15.1, 7.3.15.3 through 7.3.15.6 for policing inbound routine video requests.

SCM-003640 [Required: SS] [5.3.2.7.5.1.7] When a SS receives an initial precedence UC SIP INVITE request intended for forwarding to a served UC SIP – H.323 Gateway, the SS shall implement one of the following two policing rules:

- a. **[Preferred]** Forward the UC SIP INVITE to the UC SIP – H.323 Gateway and if the UC SIP – H.323 Gateway responds with either a 1xx response code greater than 100 or a 2xx response and the call request would cause the appropriate (voice or video) call count threshold (or inbound call count threshold) to be exceeded, then the SS:
 - (1) Sends a 488 (Not Acceptable Here) response code to the remote initiating party of the UC SIP INVITE that may include a Warning header field with warning code 370 (Insufficient Bandwidth).
 - (2) Sends a CANCEL request (in the case of a 1xx response code) or a BYE request (in the case of a 2xx response code) to the local UC SIP – H.323 Gateway.

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

- b. **[Alternative]** (Standard ASAC Policing Rules for precedence call request) Forward the UC SIP INVITE request to the UC SIP – H.323 Gateway and if the UC SIP – H.323 Gateway responds with either a 1xx response code greater than 100 or a 2xx response and the call request would cause the appropriate (voice or video) call count threshold (or inbound call count threshold) to be exceeded, then the SS applies the standard ASAC policing rules for a precedence call request. That is, the SS preempts a ROUTINE or lesser precedence call by sending a BYE request with a Reason header for preemption to the UC SIP – H.323 Gateway. The UC SIP – H.323 Gateway shall ignore the Reason header for preemption, interwork the BYE request to the H.323 UC signaling platform, and respond with a 200 (OK) response. The ROUTINE or lesser precedence call will be terminated and the SS will forward the 1xx response greater than 100 or the 2xx response to the precedence inbound call request over the UC WAN.

2.11.3.3 UC SIP – H.323 Gateway SCS

[Table 2.11-6](#), UC SIP – H.323 Gateway support for VoIP and Video Signaling Interfaces, provides a complete list of the UC SIP – H.323 Gateway signaling requirements.

Table 2.11-6. UC SIP – H.323 Gateway Support for VoIP and Video Signaling Interfaces

FUNCTIONAL COMPONENT	VOIP AND VIDEO SIGNALING INTERFACES	VOIP AND VIDEO SIGNALING PROTOCOLS
CCA	CCA (UC SIP – H.323 Gateway) – to – CCA (SS)	UC SIP over IP
CCA	CCA (UC SIP – H.323 Gateway) – to – H.323 UC signaling platform	Proprietary signaling over IP
LEGEND		

FUNCTIONAL COMPONENT	VOIP AND VIDEO SIGNALING INTERFACES	VOIP AND VIDEO SIGNALING PROTOCOLS
CCA: Call Connection Agent		UC: Unified Capabilities
IP: Internet Protocol		UC SIP: Unified Capabilities Session Initiation Protocol
SS: Softswitch		VoIP: Voice over IP

2.11.3.3.1 CCA Function

The CCA is part of the SCS functions and includes the IWF (signaling) function.

SCM-003650 [Required] The CCA IWF shall support the UC SIP consistent with the detailed UC SIP requirements in UC SIP 2013.

SCM-003660 [Required] The CCA IWF shall secure the UC SIP protocol using TLS, as described in Section 4, Information Assurance.

SCM-003670 [Required] The CCA IWF component of the UC SIP – H.323 Gateway shall ensure that when the supplementary services enumerated in the UCR (i.e., Call Hold, Call Waiting, Precedence Call Waiting, Call Forwarding, Call Transfer) are performed by a served H.323 UC signaling platform that the UC SIP – H.323 Gateway presents UCR-compliant call flows to the signaling appliances in the UC network per UC SIP 2013, Section 9.

2.11.3.4 AS Precedence Capability Requirements and Resource Priority Header

The UC SIP – H.323 Gateway does NOT conduct preemption.

SCM-003680 [Required] Whenever the UC SIP – H.323 Gateway receives a H.323 signaling message from the H.323 UC signaling platform that translates it into an INVITE, UPDATE, or REFER request, then the UC SIP – H.323 Gateway shall generate a Resource-Priority header having a ROUTINE priority level IAW UC SIP 2013, Section 6.1, Precedence Level Communicated Over SIP Signaling.

SCM-003690 [Required] Whenever the UC SIP – H.323 Gateway receives an INVITE, UPDATE, or REFER request from the SS via the SBC, then the UC SIP – H.323 Gateway shall process the Resource-Priority header to distinguish a ROUTINE call from a precedence call.

SCM-003700 [Required] ASF-2104220 When an UC SIP – H.323 Gateway receives an initial routine UC SIP INVITE (i.e., not a re-INVITE) from the SS (via the SBC), then the UC SIP – H.323 Gateway shall do the following:

- a. Check the appropriate (voice or video) call count (and inbound call count in the case of directionalization) to determine whether there are available bandwidth resources to support the call request.
- b. If the new call request would not exceed the appropriate (voice or video) call count threshold (and inbound call count threshold) then the UC SIP – H.323 Gateway

increments the appropriate (voice or video) call count (and inbound call count) and interworks the INVITE to H.323.

- c. If the appropriate (voice or video) call count (or inbound call count) is at threshold or the call request would cause the UC SIP – H.323 Gateway to exceed the appropriate (voice or video) call count threshold (or inbound call count threshold) then the UC SIP – H.323 Gateway shall reject the call.

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

SCM-003710 [Required] ASF-2104230 The UC SIP – H.323 Gateway shall support the following two methods for processing initial precedence UC SIP INVITEs received from the SS via the SBC and the choice of method shall be software configurable:

- a. Upon receipt of the initial precedence UC SIP INVITE request the UC SIP – H.323 Gateway diverts the precedence INVITE to the attendant, or
- b. Upon receipt of the initial precedence UC SIP INVITE request, the UC SIP – H.323 Gateway determines whether the appropriate (voice or video) call count (or inbound call count in the case of directionalization) is at threshold or whether the call request would cause the UC SIP – H.323 Gateway to exceed the appropriate (voice or video) call count threshold or inbound call count threshold:
 - (1) If the precedence UC SIP INVITE would cause the appropriate (voice or video) call count threshold (or inbound call count threshold) to be exceeded, then the precedence UC SIP INVITE is forwarded to the attendant.

NOTE: The UC SIP – H.323 Gateway shall NOT conduct preemption on behalf of an inbound precedence UC SIP INVITE.

- (2) If the precedence UC SIP INVITE would NOT cause the appropriate call count threshold (or inbound call count threshold) to be exceeded, then the UC SIP – H.323 Gateway treats the inbound precedence UC SIP INVITE request as if it were a routine inbound call request and increments the appropriate (voice or video) call count (and inbound call count) and interworks the INVITE to platform..

2.11.3.5 SIP URI and Mapping of Telephone Number

SCM-003720 [Required] When the UC SIP – H.323 Gateway receives a call request from the H.323 UC signaling platform, then the UC SIP – H.323 Gateway shall map the telephony numbers received from the initial H.323 signaling message to SIP URIs IAW UC SIP 2013, Sections 12.3, SIP URI and Mapping of Telephony Number into SIP URI, and 4.6, SIP URI and Mapping of Telephone Number into SIP URI.

2.11.3.6 *Session Admission Control*

SCM-003730 [Required] [2.10.4.4.1.4.1] The UC SIP – H.323 Gateway shall conduct SAC as detailed in this section in lieu of the ASAC required of SCs.

SCM-003740 [Optional] [2.10.4.4.1.4.2] The UC SIP – H.323 Gateway may support directionalization.

NOTE: Whenever the H.323 UC signaling platform supports Directionalization, then directionalization will be performed in the H.323 UC signaling platform and not in the UC SIP – H.323 Gateway.

SCM-003750 [Conditional] [2.10.4.4.1.4.3] If the H.323 UC signaling platform does not support code blocking then the UC SIP – H.323 Gateway shall support code blocking.

SCM-003760 [Required] [2.10.4.4.1.4.4] The UC SIP – H.323 Gateway shall support configuration of total voice call thresholds and total video call thresholds.

SCM-003770 [Optional] [2.10.4.4.1.4.5] The UC SIP – H.323 Gateway may support configuration of outbound voice call thresholds, inbound voice call thresholds, outbound video call thresholds, and inbound video call thresholds.

SCM-003780 [Required] [2.10.4.4.1.4.6] Session Admission Control (SAC) refers to the enforcement of voice and video session thresholds whereby the UC SIP – H.323 Gateway shall:

- a. Reject call requests received from the H.323 UC signaling platform that would exceed the appropriate [voice or video) call count threshold (or outbound call count threshold).
- b. Reject initial routine INVITEs (i.e., not re-INVITEs) received from the SS that would exceed the appropriate (voice or video) call count threshold (or inbound call count threshold).
- c. Per the requirement for precedence calls in [Section 2.11.2.3.2](#), either divert all precedence INVITEs to the attendant, or divert the precedence INVITE to the attendant if the INVITE would cause the appropriate (voice or video) call count threshold (or inbound call count threshold) to be exceeded.

2.11.3.7 *UC SIP – H.323 Gateway Media Interworking*

SCM-003790 [Required] The UC SIP – H.323 Gateway shall support the audio Codecs in [Section 2.9.1.3](#), Audio Codecs, Voice Instruments.

SCM-003800 [Required] The UC SIP – H.323 Gateway shall comply with [Section 2.9.1.5](#), Voice over IP Sampling Standard, for the sampling rates.

SCM-003810 [Required] The UC SIP – H.323 Gateway shall support the audio and video Codecs as specified in [Section 2.9.3.3](#), Video Codecs (Including Associated Audio Codecs).

SCM-003820 [Required] The voice media packets generated by the IP EIs served by the H.323 UC signaling platform that are intended for a destination outside the enclave shall be interworked by the UC SIP – H.323 Gateway into UCR-compliant voice packets that shall be sent to the SBC.

SCM-003830 [Required: SBC] The enclave SBC shall send the UCR-compliant voice media packets received from the UC WAN and intended for the IP EIs served by the H.323 UC signaling platform to the UC SIP – H.323 Gateway.

SCM-003840 [Required] The UC SIP – H.323 Gateway shall interwork the UCR-compliant voice media packets received from the SBC into the H.323 voice media packets used by the IP EIs, and then the H.323 voice media packets shall be forwarded to the IP EIs.

NOTE: The UCR does not specify the internal routing path of the voice media packets between the UC SIP – H.323 Gateway and the IP EIs.

SCM-003850 [Required] The video media packets generated by the IP EIs served by the H.323 UC signaling platform that are intended for a destination outside the enclave shall be interworked by the UC SIP – H.323 Gateway into UCR-compliant video packets that shall be sent to the SBC.

SCM-003860 [Required: SBC] The enclave SBC shall send the UCR-compliant video media packets received from the UC WAN and intended for the IP EIs served by the H.323 UC signaling platform to the UC SIP – H.323 Gateway.

SCM-003870 [Required] The UC SIP – H.323 Gateway shall interwork the UCR-compliant video media packets received from the SBC into the H.323 video media packets employed by the IP EIs and then the H.323 video media packets shall be forwarded to the IP EIs.

NOTE: The UCR does not specify the internal routing path of the video media packets between the UC SIP – H.323 Gateway and the IP EIs.

2.11.3.8 Information Assurance

SCM-003880 [Required] The UC SIP – H.323 Gateway shall satisfy the Information Assurance requirements in Section 4, Information Assurance, for a media gateway.

2.11.3.9 UC SIP – H.323 Gateway Management Function

SCM-003890 [Required] The UC SIP – H.323 Gateway Management Function shall support the applicable requirements in [Section 2.19](#), Management of Network Appliances:

2.11.3.10 UC SIP – H.323 Gateway-to-EMS Interface

SCM-003900 [Required] The UC SIP – H.323 Gateway shall provide an interface to the DISA NMS. The interface shall consist of a 10/100-Mbps Ethernet connection as specified in [Section 2.7.4](#), DISA VVoIP EMS Interface.

NOTE: The UC SIP – H.323 Gateway shall support one pair of Ethernet management interfaces where one management interface is for communication with a local EMS and one management interface is for communication with a remote EMS. In addition, the UC SIP – H.323 Gateway shall support at least one additional Ethernet interface for carrying signaling and media streams for VVoIP traffic.

2.11.3.11 Product Quality Factors

SCM-003910 [Required] The UC SIP – H.323 Gateway shall meet the product quality factors specified in [Section 2.8.2](#), Product Quality Factors.

2.12 ENTERPRISE UC SERVICES

2.12.1 Introduction

The Enterprise UC Services Architecture consists of both Centralized Enterprise Infrastructure products and Edge Infrastructure products. The Centralized Enterprise Infrastructure is composed of an Enterprise Session Controller (ESC), ESC-fronting SBC, Enterprise Hosted UC Services and Enterprise Remote Auxiliary Equipment (RAE). The Edge Infrastructure (at DOD Components' B/P/C/S locations) consists of End Instruments, Media Gateways, Enclave-fronting SBC, local Survivable Call Processing appliance (for Environments 1 and 2) and local RAE. 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). This section of the UCR assumes that the reader is familiar with the Enterprise UC Services architecture and concepts defined in UC Framework 2013.

2.12.2 Centralized Enterprise Infrastructure

2.12.2.1 Enterprise Session Controller (ESC)

2.12.2.1.1 General

SCM-003920 [Required] The ESC shall support the SC requirements defined in [Section 2.10](#), Session Controller (subject to the modifications and additions set forth in this subsection).

SCM-003930 [Required] The ESC shall support centralized, integrated voice, video and data session management on behalf of served IP end instruments (EIs) that are located at different enclaves (i.e., B/P/C/S sites) within the associated ESA.

SCM-003940 [Required] The ESC shall be capable of autonomously providing session management for all intra-ESA voice and video sessions (where both the caller and called party reside within the ESA).

SCM-003950 [Required] The ESC shall be capable of interoperating with other ESCs and SCs using UC SIP as defined in the UC SIP 2013.

SCM-003960 [Required] For sessions where either the calling party or called party is served by an SC or another ESC (external to the ESA), the ESC shall comply with the UC two-tier, hierarchical session routing policy.

SCM-003970 [Required] The ESC shall have an availability of at least 99.999%.

SCM-003980 [Required] The ESC shall meet the IPv6 requirements defined in Section 5 of the UCR.

SCM-003990 [Required] The ESC shall support the DSCP marking requirements defined in Section 6, Network Infrastructure End-to-End Performance.

SCM-004000 [Required] Signaling, bearer, and Operations, Administration, Maintenance, and Provisioning (OAM&P) protocol traffic exchanged between the centralized Enterprise Services infrastructure and the Edge infrastructure shall be capable of traversing DOD Component enclave and Enterprise Information Assurance (IA) accreditation boundaries using protocols that are approved by the Ports, Protocols, and Service Management (PPSM) Category Assurance List (CAL).

SCM-004010 [Required] The ESC shall support an interface to a Local RTS Routing Database (LRDB) to support database (DB) queries and DB responses in support of the Commercial Cost Avoidance feature as defined in Section 3, Auxiliary Services.

SCM-004020 [Required] The ESC shall support an interface to a Master RTS Routing Database (MRDB) in order to support the DB update capability as defined in Section 3, Auxiliary Services.

SCM-004030 [Required] Each time an end user/EI registers for service with the ESC, the ESC shall determine the served enclave where the originating EI resides. This information shall permit the ESC to correctly associate a served enclave with every inbound (EI-to-ESC) or outbound (ESC-to-EI) call leg. Such an association is essential to the correct execution of services such as ASAC, Commercial Access, and Precedence Call Diversion. The precise mechanism for determining the enclave from which the registration request originated is left up to the vendor's discretion.

2.12.2.1.2 *Support for End Instruments (EIs)*

SCM-004040 [Required] The ESC shall support EI session management functions defined for the SC in [Section 2.10](#), Session Controller (subject to the modifications and additions set forth in this subsection).

SCM-004050 [Required] The ESC shall offer hardware based voice, video and videophone EIs.

SCM-004060 [Required] The ESC shall offer soft clients that provide access to integrated UC services from a common user interface. In performing this function, the ESC shall comply with the softphone requirements defined in [Section 2.9.1.6](#), Softphones.

SCM-004070 [Required] The ESC shall support an UC SIP “ESC-to-EI” signaling interface in support of UC SIP EIs (UEIs) as defined in this section and the UC SIP 2013.

NOTE: The ESC solution is not required to include UEIs.

SCM-004080 [Conditional] If the ESC supports Proprietary EIs (PEIs), then the vendor proprietary “ESC-to-EI” signaling interface shall comply with the PEI signaling requirements as defined in [Section 2.9.1](#), IP Voice End Instruments (subject to the modifications and additions set forth in this subsection).

SCM-004090 [Required] The ESC shall centrally provide registrar functionality for all of its served EIs.

SCM-004100 [Required] The ESC shall be capable of supporting up to 50,000 served EIs and must have a migration plan to support up to one million EIs.

2.12.2.1.3 *Centralized Configuration and OAM&P*

SCM-004110 [Required] The ESC shall provide a centralized configuration service that permits served Edge Infrastructure products (EIs, MGs, SBCs, DSCs and SSPs) to securely retrieve/download configuration files. The signaling and transport used to initiate and complete the retrieval and download of configuration files must be able to traverse DOD Component enclave and Enterprise IA accreditation boundaries using protocols that are approved by the PPSM CAL.

SCM-004120 [Required] The ESC shall enable centralized management and distribution of firmware/software updates directly to Edge Infrastructure products (including EIs, SBCs, MGs, DSCs and SSPs). The signaling and transport used to initiate and complete the distribution of firmware/software updates must be able to traverse DOD Component enclave and Enterprise IA accreditation boundaries using protocols that are approved by the PPSM CAL.

SCM-004130 [Required] The ESC shall provide an integrated management framework that enables the provisioning, administration, management, accounting and monitoring of all centralized Enterprise Services components (i.e., ESC, ESC-fronting SBC, and Enterprise

Hosted UC Services) and all Edge Infrastructure components within the ESA (including EIs, Enclave-fronting SBCs, MGs, DSCs and SSPs).

SCM-004140 [Required] The ESC shall permit local enclave administrators at served B/P/C/S locations to have secure, restricted access to the provisioning capabilities of the ESC for the purpose of provisioning local moves, adds and changes (MACs). Enclave administrative access privileges to the ESC's centralized provisioning capabilities shall be restricted to the extent that the local administrators can only see and make provisioning changes that affect their local user community.

NOTE: The local administrator must be able to provision local moves, adds and changes without having root/super user access to ESC system management.

2.12.2.1.4 *Commercial Access*

SCM-004150 [Required] The ESC shall centrally provide Media Gateway Control (MGC) functionality as defined in this section. In performing this function, the ESC shall be capable of routing commercial calls to a media gateway (MG) that resides in the same local enclave as the call originator. In the execution of this capability, the ESC shall leverage end user/EI-to-enclave association data determined at the time of end user/EI registration as described in [Section 2.12.2.1.1](#).

SCM-004160 [Required] The ESC shall be capable of using UC SIP to route commercial calls to the SS. To disambiguate an E.164 telephony number from a 10-digit DSN number within the UC SIP Request URI, the ESC shall strip away any prefix digits and shall add the leading "+" character to the commercial numbers which shall be composed of the country code (CC) and national specific numbers.

NOTE: The SS is responsible for routing commercial traffic to an SBC at a DOD Internet Access Point (IAP) in order to interface with a Voice Internet Service Provider (ISP) carrier.

SCM-004170 [Required] The ESC shall permit the provisioning of a Commercial Access Route on a per DOD Component Enclave-basis. Commercial Access Route provisioning data shall dictate whether a commercial call is routed to a media gateway that resides in the same local enclave as the call originator or to the SS.

2.12.2.1.5 *ASAC*

SCM-004180 [Required] The ESC shall support the ASAC requirements for the SC related to voice and video session management as defined in this section and the UC SIP 2013 (subject to the modifications and additions set forth in this subsection).

SCM-004190 [Required] To regulate IP access link utilization, the ESC shall manage a separate voice and video budget for each of its served enclaves.

SCM-004200 [Required] The ESC shall provide the capability for the system administrator to configure a separate voice and video budget for each enclave.

SCM-004210 [Required] In the execution of centralized line-side ASAC enforcement, the ESC shall be capable of assigning calls to or from a served EI to the correct ASAC budget. In the execution of this capability, the ESC shall leverage end user/EI-to-enclave association data determined at the time of end user/EI registration as described in [Section 2.12.2.1.1](#).

SCM-004220 [Required] To enable the correct execution of ASAC, the ESC shall be able to differentiate between intra-enclave calls (which will not consume IP access link bandwidth) and inter-enclave calls (which will consume IP access link bandwidths):

- a. The ESC shall increment the corresponding ASAC budget based upon each inter-enclave session origination.
- b. The ESC shall, likewise, decrement the corresponding ASAC budgets based upon each inter-enclave session termination.
- c. The ESC shall not increment or decrement ASAC budgets based upon intra-enclave session originations or terminations.

SCM-004230 [Required] The ESC shall be capable of supporting up to 500 ASAC budgets across the ESA.

SCM-004240 [Required] With regards to the management of voice and video call counts across IP access links internal to the ESA, the ESC shall not be subject to ASAC policing by the SS.

NOTE: The ESC autonomously manages (without the involvement of the SS) intra-ESA voice and video sessions. Because the SS is not involved in the session management of intra-ESA voice and video sessions, it is not able to maintain an accurate accounting of voice and video call counts across IP access links internal to the ESA. As a result the SS is not in a position to police ASAC compliance across these IP access links which are internal to ESA.

2.12.2.2 Enterprise Hosted UC Services

2.12.2.2.1 UC Audio and Video Conferencing

SCM-004250 [Optional] The ESC shall centrally provide UC audio and video conferencing by means of a collocated UC audio and video conference system.

NOTE: Support for UC audio and video conferencing by the ESC is categorized as an Optional capability. However, if the ESC does include support for UC audio and video conferencing, the system must comply with the following requirements.

SCM-004260 [Optional] The ESC shall be in the signaling path for all signaling messages exchanged between EIs served by the ESC and the associated audio and video conference system.

SCM-004270 [Optional] The conference system is not required to understand or act upon call precedence or to support the preemption of participants or conferences.

SCM-004280 [Optional] The conference system shall provide a “service portal” for end user access to UC conferencing services, features, and capabilities.

SCM-004290 [Optional] The conference system shall provide notification of participants joining and leaving a conference and provide an end-of-conference warning to all participants.

SCM-004300 [Optional] The conference system shall provide the following conferencing chair control functionality:

- a. Voice-activated switching.
- b. Continuous presence.
- c. Mute and unmute all conference participants.
- d. Enable/disable extension of a conference.
- e. Capability to “force disconnect” select participants from a conference.

SCM-004310 [Optional] A video conference system shall be capable of accepting audio-only participants into a conference call.

SCM-004320 [Optional] Audio conference systems shall support the following audio codes: G.711, G.722, G.722.1, G.723.1, G.728, G.729A.

SCM-004330 [Optional] Video conference systems shall support the following audio codecs: G.711, G.722, G.722.1, G.723.1, G.728, G.729A and video codecs: H.263-200 and H.264.

SCM-004340 [Optional] The conference system shall provide a Reservationless, Meet-Me Audio Conference service.

SCM-004350 [Optional] The conference system shall provide an Ad hoc Audio Conference service.

SCM-004360 [Optional] The conference solution shall provide a Scheduled Audio Conference service.

SCM-004370 [Optional] The conference solution shall provide Preset Conferencing capabilities.

2.12.2.2.2 *Announcements and Music on Hold*

SCM-004380 [Required] The ESC shall be capable of centrally providing announcements for served EIs without a noticeable degradation in the quality of the audio transmission. The delivery of the announcement shall not be adversely impacted by traversing Enterprise or DOD Component IA accreditation boundaries (using protocols that are approved by the PPSM CAL) or by WAN transport impairments (e.g., delay, packet loss).

SCM-004390 [Required] The ESC shall centrally provide the set of announcements required of an SC as defined in this section.

SCM-004400 [Conditional] If the ESC provides music-on-hold capabilities, the music-on-hold shall be implemented as defined in UC SIP 2013.

2.12.2.2.3 *Enterprise E911 Call Management*

SCM-004410 [Required] The ESC shall support an integrated E911 Management capability that enables EI location information to be provided to the local emergency response dispatch center (e.g., an off-base or on-base PSAP) that is associated with each enclave within the ESA.

SCM-004420 [Required] For each enclave served by the ESC, the integrated E911 Management capability shall support the generation of enclave-specific Private Switch/Automatic Location Information (PS/ALI) database records that maps Emergency Response Locations (ERLs) to corresponding Emergency Location Identification Numbers (ELINs) as described in Section 3, Auxiliary Services.

NOTE: The DOD Component enclave administrator is responsible for establishing/defining ERLs across a particular B/P/C/S location. This information must be reliably provided to the system administrator for the E911 management capability associated with the ESC.

SCM-004430 [Required] After the individual PS/ALI database records have been generated, the integrated E911 Management solution shall be capable of exporting the enclave-specific PS/ALI record to the ALI database provider associated with the local off-base or on-base PSAP that is geographically responsible for the 911 caller. The integrated E911 Management solution shall be capable of exporting the enclave-specific PS/ALI records using the file formats defined in Section 3, Auxiliary Services.

SCM-004440 [Required] The provisioning capabilities associated with the ESC's integrated 911 Management solution shall permit the manual association of an end user/EI to an ERL based upon the physical location of the end user/EI at the time of end user/EI provisioning.

SCM-004450 [Optional] During the end user/EI registration process, the ESC shall prompt the user to establish/update their location leveraging the display capabilities of the associated softphone or hardphone:

- a. The end user shall have the option of selecting from a list of locations that is presented to the end user via the user interface associated with the softphone or hardphone. Additionally, the end user should be permitted to select their last location or select from a list of “favorites.”
- b. Once the location has been selected by the end user, the integrated E911 management capability shall have the capability to map the location selected by the end user to an associated ERL.

SCM-004460 [Required] Based on available end user/EI-to-ERL association data, the integrated E911 management capabilities shall permit the ESC to dynamically determine the correct ELIN to associate with each EI that originates a 911 emergency call.

SCM-004470 [Required] If the integrated E911 management capability cannot determine the physical location of the EI originating the 911 call (i.e., it does not have specific EI-to-ERL association data for the EI that is originating the 911 call), it shall assign an enclave-specific “default ERL” to the call based on EI-to-enclave association data the ESC established during the EI registration process (see [Section 2.12.2.1.1](#)). The integrated E911 management solution shall be capable of generating and exporting ALI database records for the default ERL and the associated ELIN. The ALI record associated with the default ERL shall include:

- a. The address associated with the main Listed Directory Number (LDN) for the associated B/P/C/S location.
- b. An explicit notification that the caller’s detailed location is not known and that a default routing of the emergency call has occurred.
- c. Contact information for on-site emergency personnel.

SCM-004480 [Required] Using ISDN PRI trunks off a media gateway in the same enclave as the 911 caller, the ESC shall route the emergency call to the regional 911 network provider who is responsible for routing the emergency call to the PSAP that is geographically responsible for the 911 caller.

SCM-004490 [Required] Prior to sending the call to the 911 network provider, the ESC’s MGC capability shall substitute the appropriate ELIN number in place of the original Calling Party Number in the ISDN PRI setup message as described in Section 3 of the UCR. The ELIN will enable the proper routing of the call and location identification at the appropriate PSAP.

SCM-004500 [Required] The ESC shall be capable of routing a “911 PSAP call back” to the EI that originated the 911 call. In the process of substituting the original Calling Party Number with an ELIN, the ESC shall temporarily cache the telephone number of the EI from which the 911 call was made (indexed against the corresponding ELIN). In the event that the PSAP dispatcher calls back using the ELIN, the ESC shall use the cached telephone number to route the “call back” to the EI that initiated the 911 call.

2.12.2.2.4 Voicemail and Unified Messaging

SCM-004510 [Required] The ESC shall provide a voicemail capability inherent to the solution or be configurable to interface with the Microsoft Unified Messaging (MS-UM) Voicemail solution as its voicemail platform.

SCM-004520 [Required] The ESC shall provide a mechanism that allows for Voicemail messages to be accessed via the Microsoft Outlook Email Client.

SCM-004530 [Conditional] If the ESC interfaces with a MS-UM Server within Microsoft Exchange Server 2010 Suite, it shall follow the requirements as stated in [Section 2.12.2.2.4.1](#). Else, the ESC shall support EWS APIs to interface with the Microsoft Client Access Server (CAS) to provide UM functionalities as described in [Section 2.12.2.2.4.2](#).

2.12.2.2.4.1 ESC Requirements for Interfacing With Microsoft Unified Messaging (MS-UM) Voicemail Server

SCM-004540 [Required] The ESC shall support the capability to forward unanswered or diverted calls to a UC SIP enabled MS-UM appliance capable of traversing DOD Components IA accreditation boundaries in accordance with Facility Security Office (FSO) and PPSM policy.

SCM-004550 [Required] The ESC shall support the capability to signal SIP with TLS to a SIP enabled MS-UM appliance using TCP port 5061.

SCM-004560 [Required] The ESC shall support SRTP for delivery and encryption of media when interfacing with a SIP enabled MS-UM appliance.

SCM-004570 [Required] The ESC shall support SIP Diversion as specified in historic RFC 5806; in particular, the ESC shall recognize warning code 302 “Moved Temporarily” to redirect the message to the MS-UM worker process using media channels TCP ports 5065 or 5066.

SCM-004580 [Required] The ESC shall wait until the ACK message is sent for the 200 OK messages before media exchange can begin as MS-UM does not support early media.

SCM-004590 [Conditional] If the IP address of the “To:” header does not match the MS-UM IP Gateway object IP address or if the extension does not match a MS-UM pilot number listed in a MS-UM hunt group, then the ESC shall support SIP Diversion as specified in historic RFC 5806; in particular, the ESC shall recognize warning code 302 “Moved Temporarily” to anticipate repackaging a second SIP Invite in order for the MS-UM appliance to be able to recognize the proper voicemail box.

SCM-004600 [Required] The ESC shall support local certificate stores to enable TLS communications.

SCM-004610 [Required] The ESC shall support mutual TLS authentication and negotiation to establish sessions with MS-UM.

SCM-004620 [Required] The ESC shall support seamless integration of email and voicemail messages into a single Outlook Client.

SCM-004630 [Required] The ESC shall support synchronization of the Message-Waiting Indicator (MWI) on the end user's phone based on user interaction (i.e., Play, Delete, Read) with voicemails in the Outlook Client.

SCM-004640 [Required] The ESC shall support configuration for at least two independent paths for redundancy to help ensure voicemails can always be sent to the MS-UM Appliance in case of outage or offline maintenance.

SCM-004650 [Required] The ESC shall support configuration with a primary and backup MS-UM servers.

SCM-004660 [Required] The ESC shall support verification and notification that the primary MS-UM server is down.

SCM-004670 [Required] The ESC shall support verification and notification that the backup MS-UM server is operational and is currently handling calls when the link to the primary server is down.

SCM-004680 [Required] The ESC shall support mutual synchronization of voicemail and email message status (i.e., "read"/"unread") between Outlook and the EI and shall reciprocate seamlessly between the EI and Outlook.

SCM-004690 [Required] The ESC shall have the capability to support E.164 or Alpha-Numeric "UserInfo" resource identifiers to be passed to MS-UM for processing as subscriber extensions.

2.12.2.2.4.2 ESC Requirements for Interfacing With to Exchange Web Services Application Programming Interface

SCM-004700 [Required] The ESC shall support Exchange Web Services (EWS) Application Programming Interface (API) integration with Microsoft Exchange 2010. This includes support of the Simple Object Access Protocol (SOAP) and XML based EWS operations which provide the messaging framework for integration between the ESC and the Exchange server.

SCM-004710 [Required] The ESC shall support Active Directory Integration with Microsoft Exchange 2010.

SCM-004720 [Required] The ESC shall support integration with the Microsoft Exchange 2010 Client Access Server (CAS) which is responsible for interfacing the different Exchange server roles with the ESC.

SCM-004730 [Required] The ESC shall use EWS to support mutual synchronization of voicemail and email message status (i.e., "read"/"unread") between Outlook and the EI and reciprocate seamlessly between the EI and Outlook.

SCM-004740 [Required] The ESC shall use EWS to support synchronization of the Message-Waiting Indicator (MWI) on the end user's phone based on user interaction with voicemails in the Outlook Client.

SCM-004750 [Required] The ESC shall use EWS to provide a Voicemail Form window which is embedded within the Outlook Client.

SCM-004760 [Required] The Voicemail Form shall provide the following options:

- a. Clearly delineates a Voice Message from an Email Message.
- b. Embeds Windows Media Player Controls with the following functional buttons: Stop, Play, Pause, Progress Bar, Volume Bar, Previous, Next and Mute.
- c. Assimilates the look and feel of the Outlook interface.

SCM-004770 [Optional] The ESC shall use EWS to provide the Play-on-Phone Feature, which enables users to send a request to the MS-UM server, via the Voicemail Form, to play a selected voice message on their phone or send the voice message to another telephone number they specify.

SCM-004780 [Optional] The ESC shall use EWS to provide the Voicemail Preview (Speech-to-Text) feature; which enables users to view the text transcription of the actual voice mail message as was left by a caller.

SCM-004790 [Optional] The ESC shall use EWS to provide the Outlook Voice Access (Text-to-Speech) feature; which enables subscribers to retrieve e-mail messages from their individual mailbox using an analog, digital, or mobile telephone.

2.12.2.2.5 IM/Chat/Presence Federation

SCM-004800 [Required] The ESC shall support secure Extensible Messaging and Presence Protocol (XMPP) server-to-server federation (i.e., server-to-server interoperability) in support of near real-time, text-based messaging (including instant messaging, group chat, and the exchange of presence) in accordance with the UC XMPP 2013.

SCM-004810 [Required] The ESC shall have a migration path to federate with the IM/Chat/Presence services of Defense Connection Online (DCO) in accordance with the server-to-server interface requirements defined in the UC XMPP 2013.

SCM-004820 [Required] In support of IM/Chat/Presence services within the ESA, the ESC shall provide secure client-to-server connections to served EIs. The client-to-server protocol from the ESC to the EI may be either XMPP or vendor proprietary (e.g., a vendor specific implementation of SIP/SIMPLE).

SCM-004830 [Conditional] If vendor proprietary, client-to-server protocols are used, the proprietary protocols shall be able to federate with native XMPP servers through the use of an

XMPP gateway implementation that provides the bidirectional translation between XMPP and the proprietary protocol as defined in the UC XMPP 2013.

2.12.2.2.6 *Enterprise Directory Services*

This section provides requirements for Enterprise Directory Services (EDS), provided by Enterprise Session Controllers (ESCs) and UC Video Conference Bridges for Enterprise UC end users.

The term “UC Video Conference Bridge,” as used in this section, has the same meaning as “UC Audio and Video Conferencing System,” as specified in Section 3.4, UC Audio and Video Conference System.

Acronyms used in this section are as follows:

- AD LDS: Active Directory Lightweight Directory Services.
- DMDC: Defense Manpower Data Center (part of OSD, not DISA).
- EASF: Enterprise Applications and Services Forest.
- IDMI: IdSS Machine Interface.
- IdSS: Identity Synchronization Service.

2.12.2.2.6.1 EDS Client

SCM-004840 [Required: Voice EI with EDS Client, Video EI with EDS Client] The EDS Client application shall support an interface to the EDS Gateway. This interface shall support transmission of directory queries in the Client-to-Gateway direction, and transmission of directory query responses in the Gateway-to-Client direction.

NOTE: The protocol used on this interface is up to the EDS Client (EI) and EDS Gateway (ESC or Conference Bridge) supplier.

SCM-004850 [Required: Voice EI with EDS Client, Video EI with EDS Client] The EDS Client shall be able to authenticate itself with the EDS Gateway using a set of EDS Authentication Credentials that are stored in the EDS Client and signaled to the EDS Gateway before an EDS directory query is sent.

- a. At a minimum, the EDS Client shall support the storage and signaling of a Username and Password as EDS Authentication Credentials. In this case, the Username and Password should be unique to that EDS Client, and should not be shared with other EDS Clients on Voice EIs and Video EIs served by that EDS Gateway.

SCM-004860 [Required: Voice EI with EDS Client, Video EI with EDS Client] The EDS Client shall be able to generate directory queries containing the following IdSS directory attributes. The query may include all or some of the following attributes:

- First Name.
- Middle Initials.
- Last Name.
- Organization Name (e.g., AR, AF, NV, MC, DOD, CIV).
- Department Name (e.g., Unit name).
- DOD SIP URI (e.g., sip:FirstName.MiddleInitials.LastName.civ@uc.mil).
- E-mail address.
- Business phone number.
- Mobile phone number.
- Rank.
- Office.

SCM-004870 [Optional: Voice EI with EDS Client, Video EI with EDS Client] The EDS Client shall also be able to generate directory queries containing the following additional IdSS directory attributes. The query may include all or some of the following attributes:

- LDAP Distinguished Name.
- Company Name (e.g., COCOM name, MAJCOM name).
- Display Name (e.g., “Captain John A Smith USAF ACC”).
- Fax number.
- Job Title.
- Alias (Mail Nickname).
- Country / Region.
- Address.
- City.
- State.
- Zip Code.

SCM-004880 [Required: Voice EI with EDS Client, Video EI with EDS Client] The EDS Client shall be capable of accepting EDS query responses from the EDS Gateway, and displaying those query responses to the EI end user. The attributes are as follows:

- LDAP Distinguished Name.
- First Name.
- Middle Initials.
- Last Name.
- Organization Name (e.g., AR, AF, NV, MC, DOD, CIV).
- Company Name (e.g., COCOM name, MAJCOM name).
- Rank.
- Office.
- Display Name (e.g., “Captain John A Smith USAF ACC”).
- Job Title.
- Alias (Mail Nickname).
- Country / Region.

-
- Department Name (e.g., Unit name).
 - E-mail address.
 - Business phone number.
 - Mobile phone number.
 - Fax number.
 - DOD SIP URI (e.g., sip:FirstName.MiddleInitials.LastName.civ@uc.mil).
 - Address.
 - City.
 - State.
 - Zip Code.

SCM-004890 [Required: Voice EI with EDS Client, Video EI with EDS Client] The EDS Client shall also be capable of accepting any attribute from the EDS Gateway in an EDS query response, and displaying that attribute in the EDS query response to the EI end user, without deleting or removing that attribute from the EDS query response.

NOTE: In other words, the set of attributes that the EDS Client displays to the EI end user should be limited by the set of attributes that the EDS Gateway returns to the EDS Client, and should not be limited by the set of required IdSS directory attributes listed in the previous requirement.

SCM-004900 [Required: Voice EI with EDS Client] The EDS Client on the Voice EI shall allow the EI end user to review the query responses returned by the EDS Gateway, and set up a Voice call to a target DOD end user by 1) selecting that end user's data record from the set of responses received, and 2) selecting the called address (DSN number, commercial wireline number, commercial mobile number, or DOD SIP URI) from that record. The Voice EI shall then use that record and address to place a VoIP call to the target DOD end user.

SCM-004910 [Required: Video EI with EDS Client] The EDS Client on the Video EI shall allow the EI end user to review the query responses returned by the EDS Gateway, and set up a Video call to a target DOD end user by 1) selecting that end user's data record from the set of responses received, and 2) selecting the called address (DSN number or DOD SIP URI) from that record. The Video EI shall then use that record and address to place a Video call to the target DOD end user.

2.12.2.2.6.2 EDS Gateway

SCM-004920 [Required: ESC with EDS Gateway, UC Video Conference Bridge with EDS Gateway] The EDS Gateway shall support interfaces to EDS Clients on both Voice EIs and Video EIs.

- a. Each of these interfaces shall support transmission of directory queries in the Client-to-Gateway direction, and transmission of directory query responses in the Gateway-to-Client direction.

NOTE: The protocol used on these interfaces is up to the EDS Client (EI) and EDS Gateway (ESC or Conference Bridge) supplier. For example, the LDAP-based Active Directory protocol can be used, or another protocol like Hypertext Transfer Protocol Secure (HTTPS)/XML/SOAP can be used instead. In the latter case, the format of the queries and responses exchanged within the SOAP messages is up to the supplier.

SCM-004930 [Required: ESC with EDS Gateway, UC Video Conference Bridge with EDS Gateway] The EDS Gateway shall require each EDS Client to authenticate itself with the EDS Gateway, before accepting EDS queries from that EDS Client, or returning EDS query responses to that EDS Client.

- a. The EDS Gateway shall require each EDS Client to authenticate using a set of EDS Authentication Credentials that are stored in the EDS Gateway and signaled by the EDS Client before an EDS directory query is sent. At a minimum, the EDS Gateway shall support the storage and signaling of a Username and Password as EDS Authentication Credentials. In this case, the Username and Password should be unique to each EDS Client, and should not be shared with other EDS Clients on other Voice EIs and Video EIs served by that EDS Gateway.

SCM-004940 [Required: ESC with EDS Gateway, UC Video Conference Bridge with EDS Gateway] The EDS Gateway shall be able to accept and process directory queries from EDS Clients containing the following IdSS directory attributes. The query may include all or some of the following attributes:

- First Name.
- Middle Initials.
- Last Name.
- Organization Name (e.g., AR, AF, NV, MC, DOD, CIV).
- Department Name (e.g., Unit name).
- DOD SIP URI (e.g., sip:FirstName.MiddleInitials.LastName.OrgName@uc.mil).
- E-mail address.
- Business phone number.
- Mobile phone number.
- Rank.
- Office.

SCM-004950 [Optional: ESC with EDS Gateway, UC Video Conference Bridge with EDS Gateway] The EDS Gateway shall also be able to accept and process directory queries from EDS Clients containing the following additional IdSS directory attributes. The query may include all or some of the following attributes:

- LDAP Distinguished Name.
- Company Name (e.g., COCOM name,
- Country / Region.
- Address.

MAJCOM name).

- Display Name (e.g., “Captain John A Smith • City. USAF ACC”).
- Fax number. • State.
- Job Title. • Zip Code.
- Alias (Mail Nickname).

SCM-004960 [Required: ESC with EDS Gateway, UC Video Conference Bridge with EDS Gateway] The EDS Gateway shall be able to authenticate itself with the UC AD-LDS Server, using AD Authentication Credentials that are stored in the EDS Gateway and signaled to the AD-LDS Server before an AD directory query is sent. At a minimum, the EDS Gateway shall support the storage and signaling of a Username and Password as AD Authentication Credentials. In this case, the Username and Password should be unique to that EDS Gateway, and should not be shared with other EDS Gateways on other ESCs and Video Conference Bridges that are served by that AD-LDS Server.

SCM-004970 [Required: ESC with EDS Gateway, UC Video Conference Bridge with EDS Gateway] Upon receipt of an EDS directory query from an EDS Client, the EDS Gateway shall convert this EDS query to a Microsoft Active Directory query, and send this AD query on to the UC AD-LDS Server that serves the ESC or Video Conference Bridge.

- a. The EDS Gateway shall include all of the EDS query attributes signaled by the EDS Client in the AD query that it sends to the UC AD-LDS Server.
- b. The EDS Gateway shall use its own Authentication Credentials to authenticate itself with the UC AD-LDS Server before sending the AD query; it should not use any EDS Client Authentication Credentials for that purpose.

SCM-004980 [Required: ESC with EDS Gateway, UC Video Conference Bridge with EDS Gateway] Upon receipt of an AD query response from the UC AD-LDS Server, the EDS Gateway shall convert this AD query response to an EDS query response that is compatible with the EDS Client (e.g., an HTTPS/XML/SOAP query response, if the EDS Client supports HTTPS/XML/SOAP instead of Active Directory). The EDS Gateway shall then send this EDS query response on to the EDS Client on the Voice EI or Video EI that originally sent the EDS query to the Gateway.

- a. The EDS Gateway shall include all of the query response components (both user records and user record attributes) in the AD response that it received from the UC AD-LDS server, in the EDS query response that it sends on to the EDS Client.

SCM-004990 [Required: ESC with EDS Gateway, UC Video Conference Bridge with EDS Gateway] The EDS Gateway shall be capable of accepting AD query responses from the UC AD LDS Server that contain the following IdSS directory attributes:

a. The EDS Gateway shall also be capable of sending EDS query responses to the EDS Client that contain the following IdSS directory attributes.

- LDAP Distinguished Name.
- Rank.
- First Name.
- Office.
- Middle Initials.
- Display Name (e.g., “Captain John A Smith USAF ACC”)
- Last Name.
- Job Title.
- Organization Name (e.g., AR, AF, NV, MC, DOD, CIV).
- Alias (Mail Nickname).
- Company Name (e.g., COCOM name, MAJCOM name).
- Country / Region.
- Department Name (e.g., Unit name).
- Address.
- E-mail address.
- City.
- Business phone number.
- State.
- Mobile phone number.
- Zip Code.
- Fax number.
- DOD SIP URI (e.g., sip:FirstName.MiddleInitials.LastName.civ@uc.mil).

SCM-005000 [Required: ESC with EDS Gateway, UC Video Conference Bridge with EDS Gateway] The EDS Gateway shall also be capable of accepting any AD attribute from the UC AD-LDS Server in an AD query response, and sending that attribute on to the EDS Client in the corresponding EDS query response, without deleting or removing that attribute from the EDS query response.

NOTE: In other words, the set of attributes that the EDS Gateway returns to the EDS Client should be limited by the set of AD attributes that the UC AD-LDS Server returns to the EDS Gateway, and should not be limited by the set of required IdSS directory attributes listed in the previous requirement.

2.12.2.2.7 *Enterprise Accounting Management*

SCM-005010 [Required] The ESC shall centrally support the minimum set of requirements to capture basic call information for accounting purposes as defined in this section.

2.12.2.2.8 *Precedence Call Diversion*

SCM-005020 [Required] The ESC shall provide a default diversion of all unanswered calls above ROUTINE precedence to a designated DN (e.g., an attendant console) as defined in this

section. The designated DN shall be a DN associated with an EI (e.g., an attendant console) in the same enclave as the original called party.

2.12.3 Edge Infrastructure

2.12.3.1 End Instruments

2.12.3.1.1 Proprietary End Instrument (PEI)

SCM-005030 [Conditional] If a PEI is served by the ESC, the PEI shall comply with the PEI requirements defined in [Section 2.9.1.6](#), Softphones (subject to the modifications and additions set forth in this subsection).

SCM-005040 [Conditional] If a PEI is served by the ESC, the proprietary signaling exchanged between the PEI and the ESC shall be capable of traversing DOD Component enclave and Enterprise IA accreditation boundaries using protocols that are approved by the PPSM CAL.

SCM-005050 [Conditional] If a PEI is served by the ESC and the PEI is relying upon the enclave-fronting SBC to facilitate the traversal of the enclave IA accreditation boundary, the PEI shall comply with the following:

- a. As a part of the normal startup and configuration process, the PEI shall obtain the IPv4 address and IPv6 address of the local enclave-fronting SBC.
- b. The PEI shall establish a secure persistent connection (TLS or equivalent) with the enclave-fronting SBC.
- c. The PEI shall send and receive all signaling messages over the TLS or equivalent connection with the enclave-fronting SBC.

NOTE: The requirement above is not intended to exclude the alternative of PEIs being served by the ESC which do NOT rely upon the enclave-fronting SBC to facilitate the traversal of the enclave IA accreditation boundary.

SCM-005060 [Conditional] If a PEI is served by the ESC and the PEI is not relying upon the enclave-fronting SBC to facilitate the traversal of the enclave IA accreditation boundary, then the signaling traffic and bearer traffic associated with the PEI must be capable of traversing the enclave IA accreditation boundary via the data firewall using protocols that are approved by the PPSM CAL and in a manner acceptable to the FSO.

SCM-005070 [Conditional] If a PEI is being served by the ESC and access to the ESC is interrupted, then the PEI shall failover to a survivable call processing appliance within the local enclave (Environments 1 and 2).

- a. When access to the ESC is restored, the PEI shall failback and re-register with the ESC.

2.12.3.1.2 UC SIP End Instrument (UEI)

SCM-005080 [Required] The UEIs shall comply with UEI requirements in this section and the UC SIP 2013 (subject to the modifications and additions set forth in this subsection).

SCM-005090 [Required] As a part of the normal startup and configuration process, UEIs shall obtain the IPv4 address and IPv6 address of their enclave-fronting SBC.

SCM-005100 [Required] UEIs served by the ESC shall establish a persistent TLS connection with the enclave-fronting SBC.

SCM-005110 [Required] UEIs served by the ESC shall send and receive all UC SIP messages over the TLS connection with the enclave-fronting SBC (i.e., the enclave-fronting SBC serves as the outbound and inbound proxy for all SIP signaling including REGISTER requests).

SCM-005120 [Required] In the event that access to the serving ESC is interrupted, the UEI shall failover to a survivable call processing instance within the local enclave.

- a. When access to the ESC is restored, the UEI shall be capable of discovering the service restoration and of subsequently re-registering with the ESC.

2.12.3.2 Media Gateway

SCM-005130 [Required] Media gateways (MGs) that reside at DOD Component enclaves within the ESA shall support the Media Gateway requirements defined in this section (subject to the modifications and additions set forth in this subsection).

SCM-005140 [Required] The MG shall be capable of securely registering with and sending/receiving control signaling to and from the MGC component of the ESC. Registration messages and control signaling sent or received by the MG shall be capable of traversing DOD Component enclave and Enterprise IA accreditation boundaries using protocols that are approved by the PPSM CAL.

SCM-005150 [Required] In the event that access to the serving ESC is interrupted, the MG shall failover to a survivable call processing appliance within the local enclave.

- a. When access to the ESC is restored, the MG shall failback to the ESC.

2.12.3.3 COOP

2.12.3.3.1 Environment Types

DOD Components shall determine the appropriate Mission Environment Type for each B/P/C/S site in line with the mission being performed at each respective location. A site's Mission Environment Type dictates the Continuity of Operations (COOP) requirements (i.e., the requirement for locally provided UC services when access to the ESC is interrupted) for that

location. The COOP requirements in turn dictate the technical solution components that must be deployed at each location.

SCM-005160 [Required] During normal operating conditions, end users at Environment 1, 2, or 3 locations shall all have access to the full complement of UC services provided by the centralized ESC and the associated Enterprise hosted applications and services.

2.12.3.3.1.1 Environment 1: Mission Critical (B/P/C/S)

SCM-005170 [Required] When access to the ESC is interrupted, an Environment 1 location shall have access to a minimum essential set of locally-provided UC services. The minimum essential set of locally-provided UC services shall include the following:

- a. Intra-base precedence calling capability.
- b. Audio conferencing (sized per customer requirements).
- c. Video point-to-point.
- d. Local-user presence, IM, and chat.
- e. E911 services.
- f. PSTN/DSN access via local media gateway (sized per customer requirements).

2.12.3.3.1.2 Environment 2: Mission and Combat Support (B/P/C/S)

SCM-005180 [Required] When access to the ESC is interrupted, an Environment 2 location shall have access to locally provided voice services. Locally-provided voice services shall include the following:

- a. Basic intra-base calling capability (ROUTINE service only).
- b. PSTN and E911 access via local media gateway (sized per customer requirements).

2.12.3.3.1.3 Environment 3: Non Mission Critical Locations (B/P/C/S)

SCM-005190 [Required] When access to the ESC is interrupted, an Environment 3 location requires no survivable, locally provided UC services. In this case, PSTN, E911 and other services shall be provided by other means (e.g., cellular).

2.12.3.3.2 *Survivable Call Processing*

2.12.3.3.2.1 Discretionary Session Controller (DSC)

SCM-005200 [Required] The Discretionary Session Controller (DSC) shall support the COOP requirements of Environment 1 sites (see [Section 2.12.3.3.1.1](#)). When access to the ESC is interrupted, the DSC shall locally provide the following UC services:

-
- a. Intra-base precedence calling capability with TLS (or equivalent) for signaling and SRTP for bearer.
 - b. Audio conferencing with support for Preset conference services (sized per customer requirements).
 - c. Video point-to-point.
 - d. Local-user presence, IM, and chat.
 - e. E911 services.
 - f. PSTN/DSN access via local media gateway (sized per customer requirements).

NOTE: A DSC is not intended to provide the full suite of capabilities required of an SC.

SCM-005210 [Required] The DSC shall provide local registrar functionality to EIs and MGs during the period of the ESC outage.

SCM-005220 [Required] The DSC shall provide MGC functionality to local MGs during the period of the ESC outage.

NOTE: A DSC will normally be deployed in a simplex configuration (without full server redundancy). However, the vendor must also support a redundant DSC configuration option for select Environment Type 1 locations that stipulate a need for that kind of system/platform redundancy.

2.12.3.3.2.2 Survivable Session Processor (SSP)

SCM-005230 [Required] The Survivable Session Processor (SSP) shall support the COOP requirements of Environment 2 sites (see [Section 2.12.3.3.1.2](#)). When access to the ESC is interrupted, the SSP shall locally provide the following voice services:

- a. Basic intra-base calling capability (ROUTINE service only) with TLS (or equivalent) for signaling and SRTP for bearer.
- b. PSTN and E911 access via local media gateway (sized per customer requirements).

SCM-005240 [Required] The SSP shall provide local registrar functionality to EIs and MGs during the period of the ESC outage.

SCM-005250 [Required] The SSP shall provide MGC functionality to local MGs during the period of the ESC outage.

2.12.4 Session Border Controller (SBC)

2.12.4.1 General SBC Functionality

SCM-005260 [Required] SBCs deployed within the Enterprise UC Services architecture shall support SBC functionality defined in this section (subject to the modifications and additions set forth in this subsection).

2.12.4.2 Enclave-Fronting SBC Functionality

SCM-005270 [Required] The enclave-fronting SBC shall be able to differentiate an intra-enclave VVoIP sessions from an inter-enclave VVoIP sessions. For inter-enclave VVoIP sessions routed through the enclave-fronting SBC, the enclave-fronting SBC shall perform the bidirectional anchoring of the associated media as defined in this section. For all intra-enclave VVoIP sessions, the enclave-fronting SBC shall not perform the bidirectional anchoring of the associated media.

2.12.4.2.1 Enclave-Fronting SBC Support of UEIs

SCM-005280 [Required] To enable full topology hiding [Network Address Translation (NAT)] of signaling and bearer traffic, the enclave-fronting SBC shall function as the outbound and inbound signaling proxy for signaling traffic exchanged between UEIs at a served enclave and the ESC.

SCM-005290 [Required] For the routing of UC SIP signaling traffic exchanged between UEIs and the ESC, the enclave-fronting SBC shall be capable of maintaining a persistent TLS connection with every served UEI within the enclave and the ESC-fronting SBC.

SCM-005300 [Required] The enclave-fronting SBC shall function as a registration proxy for all UEIs located within the associated enclave:

- a. When a served UEI sends a UC SIP REGISTER request to the enclave-fronting SBC, the enclave-fronting SBC shall replace the IP address and port value contained in the Contact header of the REGISTER message (i.e., the inside-address/port) with an IP address and port value associated with a WAN-facing interface on the enclave-fronting SBC (i.e., the outside-address/port).
- b. For the life of the registration, the enclave-fronting SBC shall maintain a binding between the inside-address/port and outside-address/port.
- c. When the enclave-fronting SBC receives an inbound SIP request/response where the embedded address (e.g., in the Request URI or Via header) matches a particular outside-address/port, the enclave-fronting SBC shall replace the outside-address/port value with the original inside-address/port value and shall forward the request to the associated UEI.

2.12.4.2.2 *Enclave-fronting SBC Support of PEIs*

SCM-005310 [Conditional] If served PEIs are relying upon the enclave-fronting SBC to facilitate the traversal of the enclave IA accreditation boundary, the enclave-fronting SBC shall function as a VVoIP aware firewall for vendor proprietary signaling exchanged between PEIs and the ESC. The enclave-fronting SBC shall maintain a secure, persistent connection (TLS or equivalent) with each served PEI within the enclave and with the ESC-fronting SBC.

SCM-005320 [Conditional] If served PEIs are relying upon the enclave-fronting SBC to facilitate the traversal of the enclave IA accreditation boundary, the enclave-fronting SBC shall function as a Application-Layer Gateway (ALG) capable of performing the bidirectional mapping of embedded inside-addresses/port values (within the signaling stream) to an outside-address/port value associated with a WAN-facing interface on the enclave-fronting SBC.

NOTE: The requirements above are not intended to exclude the alternative of PEIs being served by the ESC which do NOT rely upon the enclave-fronting SBC to facilitate the traversal of the enclave IA accreditation boundary.

2.12.4.3 *ESC-fronting SBC Functionality*

SCM-005330 [Required] The ESC-fronting SBC shall be inserted into the signaling plane between the ESC and enclave-fronting SBCs within the ESA.

SCM-005340 [Required] For the routing of UC SIP signaling exchanged between UEIs and the ESC, the ESC-fronting SBC shall maintain a persistent TLS connection with the ESC and with the enclave-fronting SBC at each UEI-hosting enclave within the ESA.

SCM-005350 [Conditional] If served PEIs are relying upon the ESC-fronting SBC to facilitate the traversal of the Enterprise IA accreditation boundary, the ESC-fronting SBC shall maintain a secure, persistent connection (TLS or equivalent) with the ESC and the enclave-fronting SBC at each PEI-hosting enclave within the ESA.

SCM-005360 [Required] The ESC-fronting SBC shall perform media anchoring on media streams to or from Enterprise media resources which are co-located with the ESC (e.g., an Enterprise conference bridge or an announcement server).

SCM-005370 [Required] With the exception of media streams to or from media resources co-located with the ESC (e.g., an Enterprise conference bridge or an announcement server), the ESC-fronting SBC shall NOT conduct media anchoring.

SCM-005380 [Required] The ESC-fronting SBC shall be a High Available SBC as defined in this section.

2.13 NETWORK-LEVEL SOFTSWITCH

SSNetwork-level SSs are backbone devices that provide long-haul signaling between local service enclaves and act as an UC SIP B2BUA within the UC framework. It provides the equivalent functionality of a commercial SS.

Support for the functionality of an internal SC is optional.

SCM-005390 [Required: SS] The SS product shall provide the following functional components, IAW the applicable requirements in the sections referenced:

- a. **[Required]** [Section 2.13.1](#), Softswitch Location Server.
- b. **[Optional]** [Section 2.10](#), Session Controller.
- c. **[Required]** [Section 2.14](#), Call Connection Agent, including the CCA-associated IWF that applies to both the SS and the **[Optional]** SC functionality, if deployed.
- d. **[Required]** [Section 2.15.10](#), CCA Interactions With Service Control Functions, that addresses media servers.
- e. **[Required]** [Section 2.3.2](#), ASAC Requirements for the SS Related to Voice, and [Section 2.3.3](#), ASAC Requirements for the SC and the SS Related to Video Services. These sections address WAN-level ASAC policing requirements.
- f. **[Required]** [Section 2.26.1](#), Multilevel Precedence and Preemption, as appropriate for VoIP and Video over IP services.
- g. **[Required]** [Section 2.2.8](#), Calling Number Delivery
- h. **[Required]** [Section 2.16](#), Media Gateway, including MG and MGC requirements as well as ISDN T1.619a PRI and commercial PRI trunking interfaces. The MGC may connect via the DISN WAN to remotely located MGs.
- i. **[Required]** [Section 2.19](#), Management of Network Appliances.
- j. **[Required]** [Section 2.20](#), Accounting Management.
- k. **[Required]** [Section 2.10.6](#), SC Transport Interface Functions, that addresses the IP Transport Interface functions.
- l. **[Required]** [Section 2.8.2](#), Product Quality Factors.
- m. **[Required]** UC SIP 2013.
- n. **[Required]** Section 4, Information Assurance, for SS, MG, and **[Optional]** SC.
- o. **[Optional]** The MG of the SS shall support an OC-3 physical interface for transport of multiplexed PRI trunk groups between 1) the SS and MFSs in the DISA TDM network, and 2) the SS and EOs in the commercial TDM network (in the case where the SS contains an SC, and the SC end users need access to the commercial TDM network). The OC-3 physical interface shall support multiplexing of both T1-based T1.619A PRI trunk

groups and T1-based commercial PRI trunk groups (e.g., NI-2 PRI trunk groups in the United States). The OC-3 multiplexing of E1-based Q.955.3 PRI trunk groups and E1-based commercial PRI trunk groups (e.g., ETSI PRI Trunk Groups in Europe) is not required.

NOTE:

- The SS MG is only required to support ISDN T1.619A PRI trunks to a Multifunction Switch (MFS). If the optional SC is supported, the SS MG also needs to support commercial PRI trunks to the local PSTN (or to an adjacent MFS that has its own commercial PRI trunks to the local PSTN).
- The SS MG(s) may be remotely located from the MGC within the CCA of the SS.
- The SS does not need to implement an ASLAN; it can use a proprietary switched Ethernet LAN for interconnecting its components within itself, and to the CE-R via an SBC.

NOTE: The only connections required between the SS MG and the MFS are ISDN T1.619A PRI and commercial PRI, IAW ANSI Standards T1.619-1992 and T1.619a-1994, plus the U.S. National ISDN documents, which include the NFAS feature. Support for the NFAS feature of the ANSI Standards is a Conditional requirement for T1.619A PRIs and a Requirement for U.S. commercial PRIs.

2.13.1 Softswitch Location Server

The Softswitch Location Service (SSLS) provides global location services and supports call routing where the called address points to a global destination (i.e., outside the SS) rather than a local destination (i.e., within the SS). A called address is contained within a SIP URI in the form of a called number. [Section 2.15.7](#), CCA Interactions With Softswitch Location Service, describes how the CCA uses routing information stored in the SSLS to route calls between SS EIs and the following:

- SCs served by the SS.
- Other SSs.
- DOD TDM networks.
- Allied TDM networks.
- Coalition TDM networks.
- PSTN (CONUS and Global).

However, when an optional, internal SC is deployed with the SS, the SS uses the routing information stored in its SCLS to do the following:

- Route internal calls from one SS PEI or UEI to another.

- Route incoming calls to local SS PEIs or UEIs from the following:
 - An SC.
 - Another SS.
 - A DOD TDM network.
 - An allied or coalition TDM network.
 - The PSTN (CONUS and Global).

2.13.2 SS Signaling Interfaces

SCM-005400 [Required: SS] The SS shall support UC SIP signaling for IP communication with other SSs and SCs.

SCM-005410 [Required: SS] The SS shall support PRI signaling for TDM communication with other systems.

SCM-005420 [Optional: SS MG] The SS MG shall support CAS signaling as required by local implementations.

2.13.3 Network Management System Interface

SCM-005430 [Required: SS] The SS-to-NMS interface shall be an Ethernet connection as specified in [Section 2.7.4](#), DISA VVoIP EMS Interface.

2.14 CALL CONNECTION AGENT

2.14.1 Introduction

This section provides GRs for the CCA function in the SC and SS.

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

The CCA described in the following requirements is part of the SCS functions, and includes both the IWF and the MGC.

SCM-005440 [Required: SC, SS] A CCA in an SS or SC shall be able to support multiple MGs on a single ASLAN.

SCM-005450 [Required: SC, SS] A CCA in an SS or SC shall be able to support multiple MGs on multiple ASLANs, where those ASLANs are interconnected to form a Metropolitan Area Network (MAN) or Community of Interest Network (COIN). In this arrangement, it is expected that the set of ASLANs forming the MAN or COIN will meet the single-ASLAN performance requirements in Section 7, Network Edge Infrastructure. In this case, the SC shall support

sessions between an MG on one ASLAN and an PEI, UEI, MG, or SBC on another ASLAN, as long as both ASLANs are part of the same MAN or COIN.

SCM-005460 [Required: SC, SS] A CCA in an SS or SC shall be able to support MGs at multiple physical locations. In some deployments, an SC in one location will serve ASLANs and EIs at distant locations, where both locations are part of the same regional MAN or COIN. In these cases, each distant ASLAN may want to have its own gateway to the local PSTN. In these cases, the SC shall support MGs at multiple locations over MAN or COIN infrastructures that meet the ASLAN performance requirements in the UCR.

2.14.2 Functional

2.14.2.1 CCA IWF Component

The IWF within the CCA does the following:

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

SCM-005470 [Required: SC, SS] The CCA IWF shall support the following VoIP and TDM signaling protocols:

- a. UC SIP.
- b. **[Optional: SC]** Proprietary VoIP (for PEIs on the EI-SC interface; this is optional and may include supplier-specific SIP, supplier-specific H.323, and other supplier-proprietary protocols).
- c. North American ISDN PRI, including MLPP.
- d. **[Optional: SC, SS]** European or other foreign ISDN PRI, including MLPP.
- e. Facility Associated Signaling (FAS) shall be supported for T1.619A PRIs.
- f. **[Optional: SC, SS]** Non-Facility Associated Signaling (NFAS) may be supported for T1.619A PRIs.
- g. Both FAS and NFAS are required for commercial PSTN PRIs, for access to the U.S. PSTN.
- h. **[Optional: SC, SS]** CAS, including MLPP.

2.14.2.2 CCA MGC Component

SCM-005480 [Required: SC, SS] The CCA MGC component shall support the following trunks:

- a. **[Required: SC, SS]** Support for DOD ISDN trunks.

- b. [**Optional: SC, SS**] Support for CAS trunks.

The MGC within the CCA does the following:

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

The MGC and the MG that it controls are considered Optional – Deployable for the SC.

2.14.3 Role of the CCA in Network Appliances

The role of the CCA is to provide session control for all VoIP sessions and Video over IP sessions that are originated by or terminated by EIs on the SC. These VoIP and Video sessions can be established using either UC SIP or a proprietary VoIP protocol.

The CCA takes on the role of a SIP B2BUA in the traditional SIP architecture.

The CCA takes on the role of a SIP Registrar for all EIs, MGs, and SBCs served by the SC, allowing EIs, MGs, and SBCs to register their SIP URIs (i.e., Addresses of Record) and current IP addresses with the CCA. The CCA is responsible for maintaining a SIP URI-to-IP-address “binding” for each PEI, UEI, MG, and SBC that is active on the SC at any time.

The CCA is responsible for providing call control and feature control for all VoIP and Video-over-IP calls and features that the SC provides. All VoIP and Video-over-IP calls that are originated by or answered by SC PEI and UEI end users are controlled by the CCA. All VoIP and Video-over-IP features that are provided to SC PEI and UEI end users, on either a per-call basis, a per-feature-request basis, or an all-calls basis, are controlled by the CCA.

In the current DISN design for an SC, the CCA includes an IWF and an MGC, and the MGC controls all the TDM interfaces served by the MG (ISDN PRI trunks, and CAS trunks). This section reviews the role of the CCA in the SC and SS reference models, and covers the role of the CCA, IWF, and MGC in each case.

2.14.4 CCA-IWF Signaling Protocol Support

This section describes the requirements for the CCA Signaling Protocol IWF to support the various VoIP and TDM signaling protocols used in the SC and SS. In summary, the role of the IWF within the CCA is to support all the VoIP and TDM signaling protocols that are used by the EIs, MGs, and SBCs, and interwork all these various signaling protocols with one another.

2.14.4.1 CCA-IWF Support for UC SIP

SCM-005490 [Required: SC, SS] The CCA IWF shall support the UC SIP protocol consistent with the detailed UC SIP protocol requirements in UC SIP 2013.

SCM-005500 [Required: SC, SS] The CCA IWF shall use the UC SIP protocol on SC-SS and SS-SS sessions.

SCM-005510 [Required: SC, SS] When the CCA IWF uses the UC SIP protocol over the Access Segment between the SBC and the DISN WAN, or over the DISN WAN itself, the CCA IWF shall secure the UC SIP protocol using TLS, as described in Section 4, Information Assurance.

2.14.4.2 CCA-IWF Support for PRI, via MG

SCM-005520 [Required: SC, SS] The CCA IWF shall support the U.S./National ISDN version of the ISDN PRI protocol, consistent with the detailed ISDN PRI protocol requirements in the following DOD and ANSI documents:

- a. [Section 2.26.3](#), ISDN, including [Table 2.26-12](#), PRI Access, Call Control, and Signaling, and [Table 2.26-13](#), PRI Features.
 - (1) The “MFS” column in these tables shall apply to the SS.
 - (2) The “PBX1” and “PBX2” columns in these tables shall apply to the SC.
- b. [Section 2.26.1](#), Multilevel Precedence and Preemption, including:
 - (1) [Section 2.26.2.3](#), Line Signaling.
 - (2) [Section 2.26.1.7](#), ISDN MLPP PRI.
- c. ANSI T1.619-1992 (R2005).
- d. ANSI T1.619a-1994 (R1999).
 - (1) Facility Associated Signaling is required for T1.619A PRIs, and NFAS is optional for T1.619A PRIs.
 - (2) Both FAS and NFAS are required for commercial PSTN PRIs, for access to the U.S. PSTN.

SCM-005530 [ETSI PRI: Required – Other Foreign PRIs: Optional] The appliance supplier (i.e., SC or SS supplier) has the option of supporting one or more foreign versions of the ISDN PRI protocol on its product. As used here, the term “Foreign version of ISDN PRI protocol” means the version of the PRI protocol that is used in the PSTN of a foreign country.

If an appliance supplier supports a foreign version of the ISDN PRI protocol on its product, the CCA IWF in that product shall support that foreign version of the ISDN PRI protocol consistent with the PRI protocol standards that are used in the PSTN of that foreign country.

Examples of these standards follow:

- ETSI standards on the use of ISDN PRI in European countries (and other countries that also support ETSI PRI standards).
- Japanese Telecommunication Technology Committee (TTC) and South Korean Telecommunication Technology Association (TTA) standards on the use of ISDN PRI in Japan and South Korea, respectively.
- ITU-T standards on the use of ISDN PRI worldwide (in countries that only support ITU-T standards).

NOTE: The ISDN-PRI/UC SIP interworking requirements in this document only apply to the U.S. version of ISDN PRI. The ISDN-PRI/UC SIP interworking requirements for foreign versions of ISDN PRI (e.g., European, Japanese, South Korean) are outside the scope of this document.

NOTE: Support for ETSI PRI is required when the SC or SS is used in the European Theater or in other OCONUS ETSI-compliant countries.

SCM-005540 [ETSI PRI: Required] When used in the European Theater and in other OCONUS ETSI-compliant countries, the CCA IWF shall support the ITU-T Recommendation Q.955.3 MLPP extensions to the ITU-T ISDN PRI protocol, consistent with the UCR and ITU-T Recommendation Q.955.3.

SCM-005550 [Required: SC, SS] The CCA IWF shall support reception of ISDN PRI messages from the MG and transmission of ISDN PRI messages to the MG.

SCM-005560 [Required: SC, SS] The CCA IWF shall be able to determine the ISDN PRI (and its D-Channel signaling link) that an incoming PRI message was received on, when processing an incoming PRI message from the MG.

SCM-005570 [Required: SC, SS] The CCA IWF shall be able to identify the ISDN PRI (and its D Channel signaling link) that an outgoing PRI message will be sent on, when generating an outgoing PRI message to the MG.

SCM-005580 [Required: SC, SS] The CCA IWF shall be able to support multiple ISDN PRIs (and their D Channel signaling links) at the MG, where each PRI is connected to a different PRI end point (e.g., to a different DOD PBX, DOD TDM switch, SS, SC, PSTN PBX, or PSTN TDM switch).

SCM-005590 [Required: SC, SS] The CCA IWF shall be able to differentiate between the individual ISDN PRIs (and their D-Channel signaling links) at the MG. The CCA IWF shall know, as part of its configuration data, which DOD PBX, DOD TDM switch, SS, SC, PSTN PBX, or PSTN TDM switch each ISDN PRI (and its D-Channel signaling link) is connected to.

SCM-005600 [Required: SC, SS] In conjunction with the MG, the CCA IWF shall support ISDN PRIs (and D-Channel signaling links) to the following:

- a. TDM PBXs and switches in the DOD network (This includes the TDM EO and Tandem components of the local SS, in the SS CCA/MG case).
- b. SSs and SCs in the DOD network.
- c. TDM PBXs and switches in the U.S. PSTN.
- d. TDM PBXs and switches in allied and coalition partner networks (when those networks support U.S. “National ISDN” PRI).

SCM-005610 [Required: SC, SS] The CCA IWF shall support the full set of ISDN MLPP requirements in ANSI T1.619 and ANSI T1.619a, including the following from ANSI T1.619:

- a. Precedence level.
- b. Cause.
- c. Notification Indicator.
- d. Signal.
- e. Call Identity.
- f. Information elements in ISDN PRI messages, on ISDN PRIs to do the following:
 - (1) TDM PBXs in the DOD TDM network.
 - (2) TDM switches in the DOD TDM network.
 - (3) SSs in the DOD network.
 - (4) SCs in the DOD network.

SCM-005620 [Required: SC, SS] The CCA IWF shall not support any of the ISDN MLPP requirements in ANSI T1.619 and ANSI T1.619a, on ISDN PRIs to TDM PBXs and switches in the U.S. PSTN.

In other words, the MLPP feature and its associated ISDN PRI signaling shall be supported on ISDN PRIs from the CCA/MG to PBXs and switches in the DOD TDM network (or to appliances in the network), but shall not be supported on ISDN PRIs from the CCA/MG to PBXs and switches in the U.S. PSTN.

SCM-005630 [Required: SC, SS] On ISDN PRIs from the CCA/MG to TDM PBXs and switches in allied and coalition partners (where those networks support U.S. “National ISDN” PRI), the CCA IWF shall support a DOD-user-configurable per-PRI option that allows the PRI to support or not support the ANSI T1.619/619a PRI MLPP feature on calls to and from that PRI.

SCM-005640 [ETSI PRI: Required – Other Foreign PRIs: Optional] When the appliance supplier supports a foreign ISDN PRI on its product, consistent with the PRI protocol standards

used in the PSTN of that foreign country, the CCA IWF (along with the MG) shall support ISDN PRIs and D Channel signaling links to the following:

- a. TDM PBXs and switches in the PSTN in that foreign country.
- b. TDM PBXs and switches in allied and coalition partner networks (where those networks support the ISDN PRI used in the home country of the allied or coalition partner).

Support for ETSI PRI is required when the SC or SS is used in the European Theater or in other OCONUS ETSI-compliant countries.

SCM-005650 [Required: SC, SS] The CCA IWF shall be able to associate individual PRI configuration data with each individual PRI served by the MG and the CCA. The CCA IWF shall not require groups of PRIs served by the MG and the CCA to share “common” PRI configuration data.

2.14.4.3 CCA-IWF Support for CAS Trunks, via MG

SCM-005660 [Optional] The CCA IWF (with the MG) may support the U.S. version of CAS trunks and trunk signaling, consistent with the CAS trunk and trunk signaling requirements in the following sections:

- a. [Section 2.26.2](#), Signaling, including the following:
 - (1) [Section 2.26.2.4](#), Trunk Supervisory Signaling.
 - (2) [Section 2.26.2.5](#), Control Signaling.
 - (3) [Section 2.26.2.6](#), Alerting Signals and Tones.
- b. [Section 2.26.1](#), Multilevel Precedence and Preemption, including:
 - (1) [Section 2.26.1.4.1](#), Channel-Associated Signaling.

SCM-005670 [Optional] The appliance supplier (i.e., SC or SS supplier) has the option of supporting one or more foreign versions of CAS trunks and trunk signaling on its product. As used here, the term “foreign version of CAS trunks and trunk signaling,” means the version of CAS trunks and trunk signaling used in the PSTN of a foreign country.

If an appliance supplier supports a foreign version of CAS trunks and trunk signaling on its product, the CCA IWF shall support the version of CAS trunks and trunk signaling used in the PSTN of a foreign country, consistent with the CAS trunk standards used in the PSTN of that foreign country. Examples of these standards include the following:

- a. ETSI standards on the use of CAS trunks in European countries (and other countries that also support ETSI CAS trunk standards).
- b. Japanese TTC and South Korean TTA standards on the use of CAS trunks in Japan and South Korea, respectively.

- c. ITU-T standards on the use of CAS trunks worldwide (in countries that only support ITU-T standards).

NOTE: The CAS trunk/UC SIP interworking requirements in this document only apply to the U.S. version of CAS trunks. The CAS trunk/UC SIP interworking requirements for foreign versions of CAS trunks (i.e., European, Japanese, South Korean) are outside the scope of this document.

SCM-005680 [Conditional] If CAS trunks and trunk signaling are supported, the CCA IWF shall support reception of CAS signaling sequences (i.e., Supervisory, Control, and Alerting) from the MG, and transmission of CAS signaling sequences to the MG.

SCM-005690 [Conditional] If CAS trunks and trunk signaling are supported, the CCA IWF shall be able to determine the MG CAS trunk and CAS trunk group that an incoming CAS signaling sequence was received on when processing an incoming CAS signaling sequence from the MG.

SCM-005700 [Conditional] If CAS trunks and trunk signaling are supported, the CCA IWF shall be able to identify the MG CAS trunk and CAS trunk group that an outgoing CAS signaling sequence will be sent on when generating an outgoing CAS signaling sequence to the MG.

SCM-005710 [Conditional] If CAS trunks and trunk signaling are supported, the CCA IWF shall be able to support multiple CAS trunk groups at the MG, where each CAS trunk group is connected to a different end point (e.g., to a different DOD PBX, DOD TDM switch, SS, SC, PSTN PBX, or PSTN TDM switch).

SCM-005720 [Conditional] If CAS trunks and trunk signaling are supported, the CCA IWF shall be able to differentiate between the individual CAS trunk groups at the MG. The CCA IWF shall know, as part of its configuration data, which DOD PBX, DOD TDM switch, SS, SC, PSTN PBX, or PSTN TDM switch each CAS trunk group is connected to.

SCM-005730 [Conditional] If CAS trunks and trunk signaling are supported, the CCA IWF shall, in conjunction with the MG, support CAS trunk groups to the following:

- a. TDM PBXs and switches in the DOD TDM network.
- b. SSs and SCs in the DISN.
- c. TDM PBXs and switches in the U.S. PSTN.
- d. TDM PBXs and switches in allied and coalition networks (where those networks support U.S. CAS trunk groups).

SCM-005740 [Conditional] If CAS trunks and trunk signaling are supported, the CCA IWF shall support the MLPP signaling requirements for CAS trunk groups in [Section 2.26.1.4.1](#), Channel-Associated Signaling. This MLPP signaling support shall include the following four cases:

- a. Answered call, Trunk to be reused.
- b. Unanswered call, Trunk to be reused.
- c. Answered call, Trunk not to be reused.
- d. Unanswered call, Trunk not to be reused.

SCM-005750 [Conditional] If CAS trunks and trunk signaling are supported, when the IWF is the appliance sending the preemption request over the CAS trunk group, the CCA IWF shall generate the measured supervisory signal (preemption signal) causing trunk circuit disconnect, with the following four variations:

- a. Answered call, Trunk to be reused.
- b. Unanswered call, Trunk to be reused.
- c. Answered call, Trunk not to be reused.
- d. Unanswered call, Trunk not to be reused.

SCM-005760 [Conditional] If CAS trunks and trunk signaling are supported, when the IWF is the appliance receiving the preemption signal over the CAS trunk group, the CCA IWF shall be able to receive and act on the measured supervisory signal (preemption signal) causing trunk circuit disconnect, with the following four variations:

- a. Answered call, Trunk to be reused.
- b. Unanswered call, Trunk to be reused.
- c. Answered call, Trunk not to be reused.
- d. Unanswered call, Trunk not to be reused.

SCM-005770 [Conditional] If CAS trunks and trunk signaling are supported, when the IWF is the appliance receiving the preemption request over the CAS trunk group, the CCA IWF shall generate the Preempt warning tone to the CCA-served party on the preempted call (e.g., a VoIP EI served by the CCA that is active on the preempted call).

SCM-005780 [Conditional] If CAS trunks and trunk signaling are supported, when the IWF is the appliance receiving the preemption request over the CAS trunk group, the CCA IWF shall detect the Returned disconnect signal from the CCA-served party on the preempted call, and remove the Preempt warning tone from the party after this detection.

SCM-005790 [Conditional] If CAS trunks and trunk signaling are supported, the CCA IWF shall support the CAS MLPP signaling as described earlier on CAS trunk groups to:

- a. TDM PBXs and switches in the DOD TDM network (This includes the TDM EO and Tandem components of the local SS, in the SS CCA/MG case).
- b. SSs and SCs in the DISN.

SCM-005800 [Conditional] If CAS trunks and trunk signaling are supported, the CCA IWF shall not use the CAS MLPP signaling described earlier on CAS trunk groups to TDM PBXs and switches in the U.S. PSTN.

In other words, the MLPP feature and its associated CAS signaling shall be supported on CAS trunk groups from the CCA/MG to PBXs and switches in the DOD TDM network (or to appliances in the network), but shall not be supported on CAS trunk groups from the CCA/MG to PBXs and switches in the U.S. PSTN.

SCM-005810 [Conditional] If CAS trunks and trunk signaling are supported, the CCA IWF shall support a DOD-user-configurable per-CAS trunk group option on CAS trunk groups from the CCA/MG to TDM PBXs, and in allied and coalition partners (where those networks support U.S. CAS trunks), that allows the CAS trunk group to either:

- a. Support the CAS MLPP feature on calls to and from that trunk group, or
- b. Not support the CAS MLPP feature on calls to and from that trunk group.

When the “Support” option is configured, the CCA IWF shall support the CAS MLPP feature for allied and coalition partner calls on that trunk group.

When the “Not Support” option is configured, the CCA IWF shall not support the CAS MLPP feature for allied and coalition partner calls on that trunk group.

SCM-005820 [Conditional] If CAS trunks and trunk signaling are supported, when the appliance supplier supports foreign CAS trunk groups on its product, the CCA IWF, along with the MG, shall support CAS trunk groups to the following:

- a. TDM PBXs and switches in the PSTN in a foreign country.
- b. TDM PBXs and switches in allied and coalition partner networks (where those networks support the CAS trunk groups used in the home country of the allied or coalition partner).

SCM-005830 [Conditional] If CAS trunks and trunk signaling are supported, the CCA IWF shall be able to associate individual CAS trunk group configuration data with each individual CAS trunk group served by the MG and the CCA. The CCA IWF shall not require groups of CAS trunk groups served by the MG and the CCA to share “common” CAS trunk group configuration data.

SCM-005840 [Conditional] If CAS trunks and trunk signaling are supported, the CCA IWF shall know the identity of the CAS device at the far end of each CAS trunk group, as part of CAS trunk group configuration data. Specifically, the CCA IWF shall know the following:

- a. The identity of each interconnected TDM PBX and switch in the TDM portion of the network (This includes the TDM EO and Tandem components of the local SS, in the SS CCA/MG case.)
- b. The identity of each interconnected SS and SC in the DISN.

- c. The identity of each interconnected TDM PBX and switch in the U.S. PSTN.
- d. The identity of each interconnected TDM PBX and switch in each allied and coalition partner network (when that network supports U.S. CAS trunk groups).

SCM-005850 [Conditional] If CAS trunks and trunk signaling are supported, when the appliance supplier supports foreign CAS trunk groups on its product, the CCA IWF shall know, as part of CAS trunk group configuration data, the identity of the foreign CAS device at the far end of each foreign CAS trunk group. Specifically, the CCA IWF shall know:

- a. The identity of each interconnected TDM PBX and switch in the foreign PSTN.
- b. The identity of each interconnected TDM switch in the foreign PSTN.
- c. The identity of each interconnected TDM PBX and switch in each allied and coalition partner network (when that network supports the foreign CAS trunk group of the allied or coalition partner's home country).

NOTE: These "foreign" CAS trunk group requirements are included to support DOD users in interconnecting their SSs and SCs with the networks of foreign PSTNs, U.S. Allies, and U.S. Coalition Partners using CAS trunk groups. Detailed requirements for support of foreign CAS trunk groups are outside the scope of this document.

2.14.4.4 CCA-IWF Support for PEI and UEI Signaling Protocols

SCM-005860 [Required: SC, SS] The CCA IWF shall support supplier-proprietary Voice and Video EIs and their associated proprietary EI signaling protocols. Proprietary EI signaling protocols, which may include a supplier's version of SIP or H.323, are permitted.

SCM-005870 [Required] The CCA IWF shall support the following Voice and Video EIs, and their associated EI signaling protocols:

- a. [Optional] Voice and Video SIP EIs.
- b. [Optional] Voice and Video H.323 EIs.
- c. Voice and Video UC SIP EIs.

SCM-005880 [Conditional] If the CCA IWF supports Voice and Video SIP EIs, the IWF shall support these EIs using the set of IETF SIP and SDP RFCs listed in UC SIP 2013.

SCM-005890 [Conditional] If the CCA IWF supports Voice and Video H.323 EIs, the IWF shall support these EIs using ITU-T Recommendation H.323.

NOTE: An SC or SS ASLAN may support two different types of Voice and Video H.323 EIs:

- a. H.323 EIs that are served by an H.323 Gatekeeper, which is completely separate from the CCA and its IWF.

- b. H.323 EIs that are served by the CCA and its IWF (where the CCA IWF is, effectively, an H.323 Gatekeeper for these EIs).

In the first case, the H.323 EIs are completely independent of the CCA, MG and SBC. It is possible in this case for an H.323 EI on the local ASLAN to set up an H.323 Voice or Video call with another H.323 EI on a remote ASLAN (located elsewhere on the DISN WAN), without using any UC SIP, and without affecting any of the UC SIP Voice or Video budgets that are used at SCs or SSs.

This first case is an “H.323 Overlay Network” case and is outside the scope of this document.

In the second case, the H.323 EIs are dependent on the CCA, MG, and SBC for interworking with TDM voice networks, for interworking with UC SIP, and for gaining access to the DISN WAN. When an H.323 EI on the local ASLAN makes an H.323 Voice or Video call to another H.323 EI on a remote ASLAN in this case, the “calling SC” does H.323/UC SIP protocol conversion, the called SC does UC SIP/H.323 protocol conversion, and the call is treated as an UC SIP session (with resulting Voice or Video budget impacts) between the calling SC, the called SC, and any intermediate SSs.

This second case, while unusual, is an “H.323/UC SIP Interworking” case, and is within the scope of this document, with one major qualification. The CCA and IWF’s use of UC SIP in this interworking case is within the section’s scope. The details on how the suppliers’ CCA and IWF perform the protocol interworking between EI H.323 and CCA UC SIP are outside this section’s scope.

SCM-005900 [Required] When the CCA IWF supports Voice and Video UC SIP EIs, the IWF shall support these EIs using the set of UC SIP protocol requirements in UC SIP 2013.

2.14.4.5 CCA-IWF Support for VoIP and TDM Protocol Interworking

Per [Section 2.14.2.1](#), CCA IWF Component, the role of the IWF within the CCA is to support all the VoIP and TDM signaling protocols that the appliance supports for PEIs, UEIs, MGs, and SBCs, and interwork all these various signaling protocols with one another.

The requirements in this section support the IWF’s interworking of the various VoIP and TDM signaling protocols together. [Table 2.14-1](#), Full IWF Interworking Capabilities for VoIP and TDM Protocols, summarizes the various interworking capabilities that the appliance is required to support.

Table 2.14-1. Full IWF Interworking Capabilities for VoIP and TDM Protocols

IWF Input Protocol	IWF Output Protocol					
	UC SIP (to a UEI)	UC SIP (to an SBC)	PV		ISDN PRI	CAS
UC SIP (from a UEI)	No interworking needed	Required	Required if PV is supported		Required	Optional

IWF Input Protocol	IWF Output Protocol					
	UC SIP (to a UEI)	UC SIP (to an SBC)	PV		ISDN PRI	CAS
UC SIP (from an SBC)	Required	No interworking needed	Required if PV is supported		Required	Optional
PV	Required if PV is supported	Required if PV is supported	No interworking needed		Required if PV is supported	Optional
						Optional
ISDN PRI	Required	Required	Required if PV is supported		No interworking needed	Optional
CAS	Optional	Optional	Optional		Optional	No interworking needed
LEGEND CAS: Channel-Associated Signaling DOD: Department of Defense ISDN: Integrated Services Digital Network PRI: Primary Rate Interface PV: Proprietary VoIP SBC: Session Boundary Controller SS: Softswitch UC SIP: Unified Capabilities Session Initiation Protocol UCR: Unified Capabilities Requirements UEI: UC SIP End Instrument						

SCM-005910 [Required] When they are present in the network appliance, the CCA IWF shall interwork the protocols for the following cases, which shall include support for both Voice and Video UEIs, unless noted otherwise:

- a. UC SIP protocol via UC SIP UEIs with the suppliers' proprietary VoIP EI protocol.
- b. UC SIP protocol via UC SIP UEIs with the U.S. ISDN PRI protocol.
- c. **[Required: ETSI PRI – Optional: Other Foreign PRIs]** UC SIP protocol via UC SIP UEIs with the appropriate foreign ISDN PRI protocol.
- d. **[Optional]** UC SIP protocol via UC SIP UEIs with the U.S. CAS trunk protocol.
- e. **[Optional]** UC SIP protocol via UC SIP UEIs with the appropriate foreign CAS trunk protocol.

SCM-005920 [Required] When they are present in the network appliance, the CCA IWF shall interwork the protocols for the following cases, which shall include support for both VoIP and Video PEIs, unless noted otherwise:

- a. **[Conditional: SC, SS]** Proprietary VoIP EI protocol with the DOD CCS7 protocol.
- b. Proprietary VoIP EI protocol with the U.S. ISDN PRI protocol.

- c. **[Required: ETSI PRI – Optional: Other Foreign PRI]** Proprietary VoIP EI protocol with the appropriate foreign ISDN PRI protocol.
- d. **[Optional]** Proprietary VoIP EI protocol with the U.S. CAS trunk protocol.
- e. **[Optional]** Proprietary VoIP EI protocol with the appropriate foreign CAS trunk protocol.

SCM-005930 [Required] When they are present in the network appliance, the CCA IWF shall interwork the protocols for the following cases, which shall include both VoIP and Video PEIs, unless noted otherwise:

- a. UC SIP protocol via SBCs with the suppliers' Proprietary VoIP EI protocol.
- b. UC SIP protocol via SBCs with the U.S. ISDN PRI protocol.
- c. **[Required: ETSI PRI – Optional: Other Foreign PRI]** UC SIP protocol via SBCs with the appropriate foreign ISDN PRI protocol.
- d. **[Optional]** UC SIP protocol via SBCs with the U.S. CAS trunk protocol.
- e. **[Optional]** UC SIP protocol via SBCs with the appropriate foreign CAS trunk protocol.

2.14.5 CCA Preservation of Call Ringing State During Failure Conditions

SCM-005940 [Required: SC, SS, SS] The CCA in the SC and SS shall not allow UC SIP sessions that have reached the ringing state (i.e., a UC SIP 180 (Ringing) message or 183 (Session Progress) has been sent from the called party to the calling party, and the calling party is receiving an audible ringing tone) to fail when an internal failure occurs within the CCA. (As used here, "internal failure" includes cases where one component of the CCA fails, and a failover occurs within the CCA so that a second redundant component is brought into service to replace the first failed component.) Instead, the CCA shall ensure that the "call ringing state" is preserved (rather than dropped) at both the calling party interface (where audible ringing tone is being returned to the caller) and the called party interface (where incoming call alerting is being provided to the called party).

2.15 CCA INTERACTION WITH NETWORK APPLIANCES AND FUNCTIONS

This section specifies how the CCA interacts with network appliances and appliance functions. These other appliance functions include the following:

- ASAC.
- Service Control functions.
- NM (FCAPS and audit logs).
- Transport Interface functions.

- SBC (not part of the SC, but part of the local assured services domain).

2.15.1 CCA Interactions With Transport Interface Functions

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

- Network Layer functions: IP and IPsec.
- Transport Layer functions: TCP, UDP, Stream Control Transmission Protocol (SCTP), TLS.
- LAN protocols.

SCM-005950 [Required] The CCA shall support assignment of the following items to itself:

- a. Only one CCA IP address (this one IP address may be implemented in the CCA as either a single logical IP address or a single physical IP address).
- b. A CCA FQDN that maps to that IP address.
- c. A CCA SIP URI that uses that CCA FQDN as its domain name, and maps to the “SIP B2BUA” function within the CCA itself.

SCM-005960 [Required] The CCA shall support assignment of the following items to each SIP and UC SIP PEI and UEI on the Appliance LAN:

- a. Only one PEI or UEI IP address.
- b. A PEI or UEI FQDN that maps to that IP address.
- c. A PEI or UEI SIP URI that uses that PEI or UEI FQDN as its domain name, and maps to the “SIP User Agent” function within the PEI or UEI.

SCM-005970 [Required] The CCA shall support assignment of the following items to each MG on the Appliance LAN:

- a. Only one MG IP address (this one IP address may be implemented in the MG as either a single logical IP address or a single physical IP address).
- b. An MG FQDN that maps to that IP address.
- c. An MG SIP URI that uses that MG FQDN as its domain name, and maps to the “UC Signaling and Media End Point” function within the MG.

SCM-005980 [Required] The CCA shall support assignment of the following items to the SBC:

- a. Only one SBC IP address (this one IP address may be implemented in the SBC as either a single logical IP address or a single physical IP address).
- b. An SBC FQDN that maps to that IP address.

- c. An SBC SIP URI that uses that SBC FQDN as its domain name, and maps to the “SIP B2BUA” function within the SBC.

2.15.2 CCA Interactions With the SBC

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

High-level CCA requirements for interacting with an SBC are as follows:

SCM-005990 [Required] When directing VoIP sessions to other network appliances providing voice and video services across the DISN, the CCA shall direct these VoIP sessions to the SBC, so that the SBC can process them before directing them to the network appliances on the DISN WAN.

SCM-006000 [Required] The CCA shall direct VoIP sessions to other network appliances through the SBC in the following cases:

- a. When the CCA is part of an SC and is directing VoIP sessions to an SS on the DISN WAN, which is the “primary” or “backup” SS for that SC.
- b. When the CCA is part of an SS and is directing VoIP sessions to an SC on the DISN WAN, which is a “subtended” SC for that SS.
- c. When the CCA is part of an SS and is directing VoIP sessions to another SS on the DISN WAN.

SCM-006010 [Required] When accepting VoIP sessions from other network appliances on the DISN, the CCA shall accept these VoIP sessions from the SBC, because the SBC relays them from the network appliances on the DISN WAN.

SCM-006020 [Required] The CCA shall accept VoIP sessions from other network appliances through the SBC in the following cases:

- a. When the CCA is part of an SC and is accepting VoIP sessions from an SS on the DISN WAN, which is the “primary” or “backup” SS for that SC.
- b. When the CCA is part of an SS and is accepting VoIP sessions from an SC on the DISN WAN, which is a “subtended” SC for that SS.
- c. When the CCA is part of an SS and is accepting VoIP sessions from another SS on the DISN WAN.

2.15.3 CCA Support for Admission Control

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

SCM-006030 [Required] The SC and SS CCA shall meet all the requirements in [Section 2.3](#), ASAC.

SCM-006040 [Required] The SC and SS CCA shall meet all the requirements in [Section 2.26.1](#), Multilevel Precedence and Preemption.

SCM-006050 [Required] The SC and SS CCA shall meet all the requirements in UC SIP 2013, Section 7, Policing of Call Count Thresholds.

2.15.4 CCA Support for User Features and Services

The User Features and Services (UFS) Server is responsible for providing features and services to VoIP and Video PEIs/UEIs on an SC or SS, where the CCA alone cannot provide the feature or service.

SCM-006060 [Required] The CCA within a network appliance shall support the operation of the following features and capabilities, as listed in [Table 2.2-1](#), Assured Services Product Features and Capabilities:

- a. The CCA shall generate a redirecting number each time it forwards a VoIP or Video session request as part of a CF feature.
- b. The CCA supports the ability to direct VoIP and Video sessions and session requests to the UFS Server, so that the UFS Server can apply an Appliance VoIP or Video feature, when use of that feature is required by the calling party, the called party, or the appliance itself.

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

2.15.5 CCA Support for Information Assurance

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

SCM-006070 [Required] The CCA shall relay received SIP and TLS authentication credentials and encryption key information from sending end systems (i.e., users, PEIs, UEIs, and SBCs) to the Information Assurance function to support the Information Assurance function's user, PEI, UEI, and SBC authentication capabilities, and its PEI, UEI, and SBC signaling stream encryption capabilities.

SCM-006080 [Required: MG] The CCA MGC shall relay received H.248 and IPSec (or proprietary-protocol-equivalent) authentication credentials and encryption key information from MGs to the Information Assurance function to support the Information Assurance function's MG authentication capabilities, and its MG signaling stream encryption capabilities.

SCM-006090 [Required] The CCA shall relay authentication credentials received in a SIP or UC SIP REGISTER message from an PEI, UEI, or SBC to the Information Assurance function so the Information Assurance function can validate those credentials and allow that PEI, UEI, or SBC to register with the appliance.

SCM-006100 [Optional] The CCA MGC shall relay authentication credentials received with an H.248 message in an IPSec packet from an MG to the Information Assurance function so the Information Assurance function can validate those credentials and allow that MG to register with the appliance.

SCM-006110 [Required] The CCA shall relay TLS encryption key information received from a PEI or UEI to the Information Assurance function so the Information Assurance function can verify that this encryption key information can be used on the signaling streams for voice or video sessions to/from that PEI or UEI.

SCM-006120 [Required] The CCA shall relay TLS encryption key information received from an SBC to the Information Assurance function so the Information Assurance function can verify that this encryption key information can be used on the signaling streams for the Voice or Video sessions to/from that SBC.

SCM-006130 [Required] The CCA within the appliance shall support all Information Assurance Appliance requirements in Section 4, Information Assurance, which involve the appliance's SCS functions and the appliance's MGC.

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

2.15.6 CCA Interactions With Session Controller Location Service

The Session Controller Location Service (SCLS) provides information on called address translation in response to call routing queries from the CCA.

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

2.15.7 CCA Interactions With Softswitch Location Service

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

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

2.15.8 CCA Interactions With End Instrument(s)

The CCA in the SS or SC needs to interact with VoIP PEIs and UEIs served by that SS or SC. The VoIP interface between the PEI and the SS or SC is left up to the network appliance supplier. The VoIP interface between the UEI and the SS or SC is UC SIP.

The following requirements on VoIP EIs are part of the CCA requirements for the SS or SC:

SCM-006140 [Required] The CCA shall support supplier-proprietary Voice and Video EIs, using EI-CCA protocols that are proprietary to the SC or SS supplier.

SCM-006150 [Required] The CCA shall support the following Voice and Video EIs and their associated EI signaling protocols:

- a. [Optional] SIP Voice and Video EIs.
- b. [Optional] H.323 Voice and Video EIs.
- c. UC SIP Voice and Video EIs.

SCM-006160 [Conditional] If the CCA IWF supports H.323 Voice and Video EIs, the IWF shall support these EIs using ITU-T Recommendation H.323.

NOTE: An SC or SS ASLAN may support two different types of H.323 EIs:

- a. “H.323 Overlay Network”: H.323 EIs that are served by an H.323 Gatekeeper, which is completely separate from the CCA.
- b. “H.323/UC SIP Interworking”: H.323 EIs that are served by the CCA (where the CCA is effectively an H.323 Gatekeeper for these EIs).

The first case is outside the scope of this section.

The second case is within the scope of this section, with one qualification. The CCA’s use of UC SIP is within the section’s scope, but the details on how the suppliers’ CCA performs the protocol interworking between EI H.323 and CCA UC SIP are outside this section’s scope.

SCM-006170 [Required] When the CCA IWF supports UC SIP Voice and Video UEIs, the IWF shall support these UEIs using the set of UC SIP protocol requirements in [Section 2.9.6](#), Operational Framework for UEIs and Video Codecs, and UC SIP 2013.

2.15.9 CCA Support for Assured Services Voice and Video

SCM-006180 [Required] The Appliance CCA shall support both assured Voice and Video services. The CCA shall support both assured Voice and assured Video sessions, and shall support these sessions from both VoIP EIs and Video EIs, as described in [Section 2.15.8](#), CCA Interactions With End Instrument(s).

SCM-006190 [Required] The Appliance CCA shall support common procedures and protocol for VoIP and Video session control, with the following clarifications and exceptions:

- a. The CCA is required to be able to support “single-rate” TDM video (i.e., 64-Kbps TDM video calls) at MG trunk groups that are controlled by the CCA.
- b. The CCA is not required to be able to support “multi-rate” TDM video (i.e., Nx64-Kbps TDM video calls, where N runs from 2 to 24) at MG trunk groups that are controlled by the CCA.

The CCA is not required to support protocol interworking between TDM video calls and the following:

- IP video sessions that originate from or terminate on local Video EIs that are served by the CCA.
- IP video sessions that originate from or terminate on remote Video EIs, that reach the CCA via the SBC, the DISN WAN, and remote appliances.

SCM-006200 [Required] The Appliance CCA shall support common procedures and protocol for feature control, for the features and capabilities given in [Table 2.2-1](#), Assured Services Product Features and Capabilities.

SCM-006210 [Required] On calls to and from Proprietary VoIP and Proprietary Video EIs, the CCA shall use the appropriate parameters within the appliance supplier’s Proprietary protocol messages to differentiate Proprietary VoIP sessions from Proprietary Video sessions.

SCM-006220 [Conditional] If H.323 EIs are supported on calls to and from H.323 EIs, the CCA shall use the appropriate parameters within the H.323 protocol messages to differentiate H.323 VoIP sessions from H.323 Video sessions.

SCM-006230 [Required] When UC SIP EIs are supported on calls to and from UC SIP EIs, the CCA shall use the SDP message bodies in UC SIP INVITE, UPDATE, REFER, and Acknowledgement (ACK) messages, as well as the SDP message bodies in UC SIP 200 (OK) responses and earlier 1xx provisional responses, to differentiate UC SIP Voice sessions from UC SIP Video sessions.

The CCA’s use of these SDP bodies for VoIP and Video differentiation shall follow the detailed SDP requirements for VoIP and Video in UC SIP 2013.

SCM-006240 [Required] The CCA shall track VoIP sessions against corresponding Appliance VoIP budgets, and shall separately track Video sessions against corresponding Video budgets. The CCA shall maintain the Appliance’s VoIP budgets separate from the Appliance’s Video budget. The CCA shall perform this separate tracking of Appliance VoIP and Video calls and budgets consistent with the CAC/SAC requirements in [Section 2.15.3](#), CCA Support for Admission Control.

SCM-006250 [Required] As part of SC-Level ASAC and WAN-Level ASAC Policing, the CCA shall support PBAS/ASAC for both VoIP sessions and Video sessions, consistent with the ASAC requirements in [Section 2.15.3](#), CCA Support for Admission Control.

SCM-006260 [Required] The CCA shall allow an individual PEI (i.e., Proprietary, H.323, or SIP) to support both VoIP and Video sessions. The CCA shall allow an individual EI to have both VoIP and Video sessions active at the same time.

SCM-006270 [Required] The CCA shall allow an individual UEI (i.e., UC SIP) to support both VoIP and Video sessions. The CCA shall allow an individual UEI to have both VoIP and Video sessions active at the same time.

SCM-006280 [Required] The CCA shall support the routing of both VoIP and Video session requests from SCs to SSs, from SSs to SCs, and from SSs to SSs, using UC SIP. The CCA shall direct outgoing VoIP and Video session requests to SBCs, and shall accept incoming VoIP and Video session requests from SBCs, consistent with this SC-to-SS routing, SS-to-SC routing, and SS-to-SS routing.

2.15.10 CCA Interactions With Service Control Functions

SCM-006290 [Required] The CCA shall support the ability to remove VoIP and Video sessions and session requests from the media server so the CCA can continue with necessary session processing once the media server has completed its functions. Examples include the following:

- a. Removing a calling VoIP PEI or UEI from the media server after in-band audible ringing has been applied and then removed (for a local PEI-to-PEI or UEI-to-UEI call).
- b. Removing a called VoIP PEI or UEI from the media server after a Call Preemption tone or announcement has been applied and then removed.

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

2.16 MEDIA GATEWAY

This section provides Generic System Requirements (GSRs) for the Media Gateway (MG) function in the SC and SS network appliances. These appliances have defined designs that include a Media Gateway Controller (MGC) function and one or more MGs.

SCM-006300 The MG supports interconnection of VoIP, FoIP, and MoIP media streams with the following SC functions and end-user devices:

- a. **[Required: SC MG]** The SC media server, which provides tones and announcements for SC calls and SC features.
- b. **[Optional: SC MG]** Proprietary VoIP, FoIP, and MoIP EIs on the SC (when these EIs are supported on the SC).

- c. **[Optional: SC MG]** Proprietary SIP EIs on the SC (when these EIs are supported on the SC).
- d. **[Optional: SC MG]** Proprietary H.323 EIs on the SC (when these EIs are supported on the SC).
- e. **[Required: SC MG]** UC SIP VoIP, FoIP, and MoIP UEIs on the SC.

SCM-006310 [Optional – Deployable: SC MG] 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 should follow the MG requirements defined in this UCR.

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.

2.16.1 MG Call Denial Treatments to Support CAC

When the CCA determines that a VoIP session request should be blocked because an Appliance CAC restriction applies (e.g., the VoIP session count equals the VoIP session limit for the type of session being requested), the CCA will deny the session request and apply a Call Denial treatment (i.e., a busy signal or call denial announcement) to the calling party on that request. If the calling party is a TDM calling party whose call enters the appliance at an MG trunk group, the MG is responsible for applying the Call Denial treatment also.

SCM-006320 [Required] On incoming call requests to a TDM trunk group, where the CCA/MGC applies a CAC Call Denial treatment to that call request, the MG shall connect the TDM called party on the incoming call request to the appropriate CAC Call Denial tone or announcement when instructed to do so by the MGC.

2.16.1.1 MG Call Preemption Treatments to Support ASAC

When the CCA determines that an existing VoIP session or VoIP session request should be cleared because an Appliance ASAC preemption applies (e.g., a CAC limit applies and a call of a higher precedence level needs to complete within the appliance), the CCA will clear the existing session or session request and apply a Call Preemption treatment (i.e., a Call Preemption tone or announcement) to both the calling and called parties on that request. If the calling party is a TDM calling party whose call entered the appliance at an MG trunk group, or the called party is a TDM called party whose call left the appliance at an MG trunk group, the MG is responsible for applying the Call Preemption treatment also.

SCM-006330 [Required] On incoming calls or call requests to a TDM trunk group, where the CCA/MGC applies an ASAC Call Preemption treatment to that call or call request, the MG shall connect the TDM calling party on the incoming call or call request to the appropriate ASAC Call Preemption tone or announcement when instructed to do so by the MGC.

SCM-006340 [Required] On outgoing calls or call requests from a TDM trunk group, where the CCA/MGC applies an ASAC Call Preemption treatment to that call or call request, the MG shall connect the TDM called party on the outgoing call or call request to the appropriate ASAC Call Preemption tone or announcement when instructed to do so by the MGC.

2.16.1.2 MG and Information Assurance Functions

The MG interaction with Information Assurance function is consistent with the DOD Information Assurance requirements in Section 4, Information Assurance.

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

Requirements for CCA and MGC interaction with the Information Assurance server are found in [Section 2.15.5](#), CCA Support for Information Assurance. These requirements, therefore, apply to the MG.

SCM-006350 [Required] Each MG within an appliance shall support all the appliance requirements in Section 4, Information Assurance, that involve an Appliance MG.

The MG performs the following authentication and encryption functions in conjunction with the CCA and Information Assurance:

- When the MG registers with the MGC in the CCA, the MG exchanges authentication credentials with the CCA and, through the CCA, with Information Assurance.
- The MG exchanges encryption keys with the CCA and, through the CCA, with Information Assurance, before exchanging H.248 messages and encapsulated PRI messages with the MGC in the CCA.
- The MG uses the exchanged encryption keys to (1) encrypt H.248 messages and encapsulated PRI messages sent in the MG => CCA => Information Assurance direction, and (2) decrypt H.248 messages and encapsulated PRI messages sent in the Information Assurance => CCA => MG direction. The encryption and decryption are performed at the IP layer using IPsec packets, instead of being done at the message layer using H.248 messages or PRI messages.

- The MG also performs the following encryption functions in conjunction with PEIs or UEIs, and the media server in the SC (NOTE: These functions may or may not use Information Assurance, depending on the internal design of the SC.):
 - The MG exchanges encryption keys with local PEIs or UEIs and local MGs, remote PEIs or UEIs and remote MGs, and the media server, before exchanging encrypted VoIP media streams with these devices.
 - The MG uses the exchanged encryption keys to (1) encrypt VoIP SRTP media streams sent in the MG => PEI/UEI/other MG/media server direction, and (2) decrypt VoIP SRTP media streams received in the PEI/UEI/other MG/media server => MG direction. The encryption and decryption are performed above the UDP Transport Layer using SRTP packets.

2.16.1.3 MG Interaction With Service Control Functions

The media server is responsible for playing tones and announcements to calling and called parties on VoIP calls, and for playing audio/video clips (similar to tones and announcements) to calling and called parties on video calls. In addition, the media server may provide “play announcement and collect digits” functionality to calling and called parties on VoIP and video calls when this functionality is required by certain features that the CCA supports. Depending on the complexity of those features, the media server may act as a full Interactive Voice Response (IVR) system for Appliance PEIs/UEIs and other assured services end users, providing IVR-like features to local and remote VoIP callers, and providing video-enhanced IVR-like features to local and remote video callers.

The MG is responsible for routing individual VoIP, FoIP, and MoIP media streams to the media server when instructed to do so by the CCA/MGC. When instructed to do so by the CCA/MGC, the MG is responsible for removing individual VoIP, FoIP, and MoIP media streams from the media server, and for either disconnecting them entirely, or routing them on to other SC end users (e.g., VoIP or video EIs).

SCM-006360 [Required] When instructed to do so by the MGC, the MG shall direct TDM calls and call requests to the media server, so that the media server can do the following:

- a. Play tones and announcements to TDM parties on TDM calls and call requests (e.g., busy tone or announcement; call preemption tone or announcement).
- b. Provide “play announcement and collect digits” functionality when required by an Appliance VoIP feature.
- c. Provide full IVR-like functionality when required by an Appliance VoIP feature.

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

2.16.1.4 Interactions With IP Transport Interface Functions

The Transport Interface functions in the SC provide interface and connectivity functions with the ASLAN and its IP packet transport network. This section outlines high-level requirements for MG interaction with the SC Transport Interface functions. The detailed implementation methods for these requirements are left up to the vendor.

SCM-006370 [Required] Since each Appliance MG is an IP endpoint on the Appliance LAN, each MG shall support assignment of the following items to itself:

- a. Only one MG IP address (This one IP address may be implemented in the CCA as either a single logical IP address or a single physical IP address).
- b. An MG FQDN that maps to that IP address.
- c. An MG SIP URI that uses that MG FQDN as its domain name, and maps to a “SIP User Agent” function within the MG.

SCM-006380 [Required] The MG shall interact with the Transport Interface functions in the appliances in the following cases:

- a. When the MG uses the native LAN protocols, IP, and UDP to exchange SRTP media streams with PEIs, UEIs, other MGs, and the SBC over the Appliance LAN.
- b. **[Optional]** When the MG uses the native LAN protocols, IPsec, and UDP, TCP, or SCTP to exchange H.248 signaling messages with the MGC over the Appliance LAN.
- c. **[Optional]** When the MG uses the native LAN protocols, IPsec, and UDP, TCP, or SCTP to exchange encapsulated PRI messages with the MGC over the Appliance LAN.

2.16.1.5 MG–SBC Interaction

The SBC provides Session Border Control and firewall capabilities for the ASLAN, the PEIs, UEIs, 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, UEI, 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, UEI, or MG that is served by another appliance outside the SC).

SCM-006390 [Required] The SRTP media streams exchanged between the SC MG and a remote PEI, UEI, or MG shall pass through the SBC. [The SBC modifies these SRTP media streams by doing NAT/Network Address Port Translation (NAPT) on them.]

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

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

High-level MG requirements for interacting with an SBC are as follows:

SCM-006400 [Required] When sending VoIP media streams to PEIs or UEIs and MGs served by other network appliances, the MG shall direct these VoIP media streams to the SBC so the SBC can process them before sending them on to the remote PEIs or UEIs and MGs via the DISN WAN. The MG shall use IP address of the local SBC, when directing the VoIP media streams via the local SBC to the DISN WAN and the remote PEIs or UEIs and MGs.

SCM-006410 [Required] The MG shall direct VoIP media streams to remote PEIs or UEIs and MGs through the SBC in the following cases:

- a. When the MG is part of an SC and is directing VoIP media streams to PEIs or UEIs and MGs on another SC on the DISN WAN.
- b. When the MG is part of an SC and is directing VoIP media streams to PEIs or UEIs and MGs on an SS on the DISN WAN.
- c. When the MG is part of an SS and is directing VoIP media streams to PEIs or UEIs and MGs on an SC on the DISN WAN.
- d. When the MG is part of an SS and is directing VoIP media streams to PEIs or UEIs and MGs on another SS on the DISN WAN.

SCM-006420 [Required] When accepting VoIP media streams from PEIs or UEIs and MGs served by other network appliances, the MG shall accept these VoIP media streams from the appliance SBC, because the SBC relays them from the DISN WAN and the remote PEIs or UEIs and MGs on the DISN WAN. The MG shall recognize and act on the network-level IP addresses of the remote PEIs or UEIs and MGs, when accepting the VoIP sessions through the SBC from the DISN WAN and the remote PEIs or UEIs and MGs.

SCM-006430 [Required] The MG shall accept VoIP media streams from remote PEIs or UEIs and MGs through the SBC in the following cases:

- a. When the MG is part of an SC and is accepting VoIP media streams from PEIs or UEIs and MGs on another SC on the DISN WAN.
- b. When the MG is part of an SC and is accepting VoIP media streams from PEIs or UEIs and MGs on an SS on the DISN WAN.
- c. When the MG is part of an SS, and is accepting VoIP media streams from PEIs or UEIs and MGs on an SC on the DISN WAN.

- d. When the MG is part of an SS, and is accepting VoIP media streams from PEIs or UEIs and MGs on another SS on the DISN WAN.

2.16.1.6 MG Support for Appliance Management Functions

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

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.

2.16.1.7 IP-Based PSTN Interface

Voice and Video over IP interfaces from the UC network to the PSTN have not been defined. Therefore, the SC and SS to PSTN interface will remain TDM. Interfaces from an SC or SS to the PSTN will be via an MG with TDM interfaces.

2.16.1.8 MG Requirements: Interactions With VoIP EIs

The MG in the SS or SC needs to interact with VoIP EIs served by that SS or SC, and with VoIP EIs served by other SSs or SCs. The VoIP signaling interface between the PEI and the SS or SC is left up to the network appliance supplier. The VoIP signaling interface between the UEI and the SS or SC is UC SIP per [Section 2.9.6](#), Operational Framework for UEIs and Video EIs, of this document. Detailed requirements for this VoIP interface are beyond the scope of this section.

However, the following high-level requirements on VoIP EIs do apply and are part of the MG requirements for the SS and SC:

SCM-006440 [Required] The MG shall support the exchange of VoIP media streams with the following voice PEIs and UEIs both on the local appliance and on remote network appliances:

- a. Supplier-proprietary voice PEIs.
- b. Voice SIP EIs, when the appliance supplier supports these EIs.
- c. Voice H.323 EIs, when the appliance supplier supports these EIs.

- d. Voice UC SIP EIs.

SCM-006450 [Optional] When the MG supports the exchange of voice media streams with voice H.323 EIs (both on the local network appliance and on remote network appliances), the MG shall support a mechanism for interworking the G.7xx/SRTP/UDP/IP-based VoIP media streams that the MG uses with the H.323-based VoIP media streams that the H.323 EI uses.

2.16.1.9 MG Support for User Features and Services

SCM-006460 [Required] The MG shall support the operation of the following features for VoIP and Video end users, consistent with the operation of this feature on analog and ISDN lines in DOD TDM switches today:

- a. Call Hold.
- b. Music on Hold.
- c. Call Waiting.
- d. Precedence Call Waiting.
- e. Call Forwarding Variable.
- f. Call Forwarding Busy Line.
- g. Call Forwarding No Answer.
- h. Call Transfer.
- i. Three-way calling.
- j. Hotline Service.
- k. Calling Number Delivery
- l. Call Pickup.

2.16.2 MG Interfaces to TDM NEs in DOD Networks: PBXs, EOs, and MFSs

SCM-006470 [Required] Each appliance MG shall support TDM trunk groups that can interconnect with the following NEs in DOD networks, in the United States and worldwide:

- a. PBXs.
- b. SMEOs.
- c. EOs.
- d. MFSs.

SCM-006480 [Required] Each appliance MG shall support TDM trunk groups that can interconnect with DISN and DOD NEs in the United States and worldwide using the following types of trunk groups:

-
- a. **[Required: SC, SS]** U.S. National ISDN PRI, where the MG handles both the media channels and the signaling channel.
 - (1) ANSI T1.619 and T1.619a support is required for PRI MLPP signaling.
 - (2) Facility Associated Signaling is required for T1.619A PRIs, and NFAS is optional for T1.619A PRIs.
 - (3) Both FAS and NFAS are required for commercial PSTN PRIs, for access to the US PSTN.
 - b. **[Optional: SC, SS]** U.S. CAS trunks, where the MG handles both media and signaling on the same channel.
 - (1) **[Conditional: SC, SS]** If a U.S. CAS trunk is supported, then CAS MLPP signaling shall be required.

SCM-006490 [Required] Media Gateway support for these TDM trunk groups shall be identical to the support for these trunk groups in DOD TDM PBXs, EOs, Tandem switches, and MFSs.

2.16.3 MG Interfaces to TDM NEs in Allied and Coalition Partner Networks

The appliance suppliers should support TDM trunk groups on their MG product that can interconnect with NEs in U.S. Allied and Coalition partner networks worldwide.

SCM-006500 [Required] The MG shall support foreign country ISDN PRI trunk groups where the MG handles both the media channels and the signaling channel as follows:

- a. For interconnection with an allied or coalition partner network, using foreign ISDN PRI from the network of the allied or coalition partner.
- b. Support for MLPP using ISDN PRI, per ITU-T Recommendation Q.955.3, is required on SC trunk groups when these trunk groups are used to connect to an allied or coalition partner from a U.S. OCONUS ETSI-compliant country.
- c. Support for MLPP using ISDN PRI, per ITU-T Recommendation Q.955.3, is required on SS trunk groups when these trunk groups are used to connect to an allied or coalition partner from a U.S. OCONUS ETSI-compliant country.

SCM-006510 [Optional] The MG shall support foreign country CAS trunk groups where the MG handles both media and signaling on the same channel as follows:

- a. For interconnection with an allied or coalition partner network, using foreign CAS trunk groups from the network of the allied or coalition partner.
- b. Support for MLPP using CAS trunk signaling is not required on these trunk groups.

SCM-006520 [Conditional] If appliance suppliers support allied and coalition partner network TDM trunk groups on their MG, then MG support for these trunk groups shall be identical to the support for these trunk groups in DOD TDM PBXs, EOs, Tandem Switches, and MFSs.

2.16.4 MG Interfaces to TDM NEs in the PSTN in the United States

SCM-006530 [Required] Each appliance MG shall support TDM trunk groups that can interconnect with NEs in the PSTN in the United States, including CONUS, Alaska, Hawaii, and U.S. Caribbean and Pacific Territories.

SCM-006540 [Required] Each appliance MG shall support TDM trunk groups that can interconnect with the U.S. PSTN, using the following types of trunk groups:

- a. U.S. National ISDN PRI, where the MG handles both the media channels and the signaling channel:
 - (1) This is required for U.S. PSTN NEs nationwide.
 - (2) Support for MLPP using ISDN PRI is not required on these trunk groups.
 - (3) Support for both FAS and NFAS is required on these trunk groups.
- b. **[Optional]** U.S. CAS trunks, where the MG handles both media and signaling on the same channel:
 - (1) This is optional for U.S. PSTN NEs nationwide.
 - (2) Support for MLPP using CAS trunk signaling is not required on these trunk groups.

SCM-006550 [Required] Media Gateway support for these TDM trunk groups to the U.S. PSTN shall be identical to the support for these trunk groups in DOD TDM PBXs, EOs, Tandem Switches, and MFSs.

2.16.5 MG Interfaces to TDM NEs in OCONUS PSTN Networks

The appliance supplier (i.e., SC or SS supplier) should support TDM trunk groups on its MG product that can interconnect with NEs in foreign country PSTN networks (OCONUS) worldwide.

SCM-006560 [Required] The MG shall support foreign country ISDN PRI, where the MG handles both the media channels and the signaling channel:

- a. For interconnection with a foreign country PSTN, using foreign country ISDN PRI, from the country where the DOD user's B/P/C/S is located.
- b. Support for ETSI PRI is required on SC trunk groups when the SC is used in OCONUS ETSI-compliant countries.
- c. Support for ETSI PRI is required on SS trunk groups when the SS is used in OCONUS ETSI-compliant countries.
- d. Support for MLPP using ISDN PRI is not required on the above trunk groups.

SCM-006570 [Optional] The MG shall support foreign country CAS trunks, where the MG handles both media and signaling on the same channel:

- a. For interconnection with a foreign country PSTN, using foreign country CAS trunk groups from the country where the DOD user's B/P/C/S is located.
- b. Support for MLPP using CAS trunk signaling is not required on foreign country CAS trunk groups.

SCM-006580 [Conditional] If an appliance supplier supports foreign country PSTN TDM trunk groups on its MG, then MG support for these trunk groups shall be identical to the support for these trunk groups in DOD TDM PBXs, EOs, Tandem Switches, and MFSs.

2.16.6 MG Support for ISDN PRI Trunks

SCM-006590 [Required] The MG shall support ISDN PRI trunk groups that carry the U.S./National ISDN version of the ISDN PRI protocol. The MG shall support these U.S. PRI trunk groups conformant with the detailed U.S. ISDN PRI requirements in the following DOD and ANSI documents:

- a. [Section 2.26.3](#), ISDN, including [Table 2.26-12](#), PRI Access, Call Control, and Signaling, and [Table 2.26-13](#), PRI Features.
 - (1) The "MFS" column in these tables shall apply to the SS.
 - (2) The "PBX1" column in these tables shall apply to the SC.
- b. Section 2.26.1, Multilevel Precedence and Preemption, including
 - (1) [Section 2.26.1.4.2](#), (MLPP Preempt Signaling for) Primary Rate Interface.
 - (2) [Section 2.26.1.7](#), ISDN MLPP PRI.
 - (3) ANSI T1.619-1992 (R2005).
 - (4) ANSI T1.619a-1994 (R1999).
 - (5) FAS is required for T1.619 PRIs, and NFAS is conditional for T1.619 PRIs.
 - (6) Both FAS and NFAS are required for commercial PSTN PRIs, for access to the U.S. PSTN.

SCM-006600 [Required: SS, SC for ETSI PRI – Optional: SS, SC for Other Foreign PRI] The appliance supplier (i.e., SC or SS supplier) has the option of supporting one or more foreign versions of the ISDN PRI protocol on its product. As used here, the term "foreign version of ISDN PRI protocol" means the version of the PRI protocol that is used in the PSTN of a foreign country.

SCM-006610 [Conditional] If an appliance supplier supports a foreign version of the ISDN PRI protocol on its product, the MG shall support ISDN PRI trunk groups that support the version of the PRI protocol that is used in the PSTN of a foreign country. The MG shall support these foreign PRI trunk groups conformant with the PRI protocol standards that are used in the PSTN of that foreign country. Examples of these standards include ETSI standards and ITU-T standards.

SCM-006620 [Required] When used in OCONUS ETSI-compliant countries, the MG shall support ISDN PRI trunk groups that support ITU-T Recommendation Q.955.3 for MLPP.

SCM-006630 [Required] The MG shall support multiple U.S. PRI trunk groups based on the needs of the DOD user deploying the appliance. The MG shall allow each U.S. PRI trunk group at the MG to connect to: TDM EO and tandem components of the local MFS; a different U.S. PSTN TDM Network Element (NE) (e.g., PBX, TDM switch); a different DOD TDM NE (e.g., PBX, TDM switch); or a different DOD IP NE (e.g., SC, SS), based on the interconnection needs of the DOD user.

The MG shall have knowledge of which U.S. PSTN TDM, DOD TDM, and DOD IP NE each U.S. PRI trunk group is connected.

SCM-006640 [Required: SS, SC for ETSI PRI – Optional: SS, SC for Other Foreign PRI] When the appliance supplier supports foreign ISDN PRIs, the MG shall support multiple foreign PRI trunk groups based on the needs of the DOD user deploying the appliance. The MG shall allow each foreign PRI trunk group at the MG to connect to a different foreign PSTN TDM, a different allied network element, or a coalition partner TDM network element (e.g., PBX, switch), based on the interconnection needs of the DOD user.

SCM-006650 [Required] The MG shall have knowledge of which foreign PSTN TDM, or allied or coalition partner TDM NE each foreign PRI trunk group is connected.

SCM-006660 [Required] The MG shall support reception of ISDN PRI messages from the CCA MGC and transmission of ISDN PRI messages to the CCA MGC.

2.16.7 MG Support for CAS Trunks

SCM-006670 [Optional: SC, SS] The MG may support CAS trunk groups that carry the U.S. version of the CAS protocol.

SCM-006680 [Conditional: SC, SS] If supported, then the MG shall support these U.S. CAS trunk groups conformant with the detailed CAS trunk and CAS trunk signaling requirements in the following DOD documents:

- a. [Section 2.26.2](#), Signaling, including the following:
 - (1) [Section 2.26.2.4](#), Trunk Supervisory Signaling.
 - (2) [Section 2.26.2.5](#), Control Signaling.
 - (3) [Section 2.26.2.6](#), Alerting Signals and Tones.
- b. [Section 2.26.1](#), Multilevel Precedence and Preemption, including:
 - (1) [Section 2.26.1.4.1](#), Channel-Associated Signaling.

SCM-006690 [Optional] The appliance supplier (i.e., SC or SS supplier) has the option of supporting one or more foreign versions of CAS trunks and trunk signaling on its product. As

used here, the term “foreign version of CAS trunks and trunk signaling” means the version of CAS trunks and trunk signaling that is used in the PSTN of a foreign country.

SCM-006700 [Conditional] If an appliance supplier supports a foreign version of CAS trunks and trunk signaling on its product, the CCA IWF shall support the version of CAS trunks and CAS trunk signaling that is used in the PSTN of a foreign country, conformant with the CAS trunk standards that are used in the PSTN of that foreign country. Examples of these standards include ETSI CAS trunk standards and ITU-T CAS trunk standards.

The MG shall support multiple U.S. CAS trunk groups based on the needs of the DOD user deploying the appliance. The MG shall allow each U.S. CAS trunk group at the MG to connect to: a TDM EO and Tandem components of the local SS; a different U.S. PSTN TDM NE (i.e., PBX, TDM Switch); a different DOD TDM NE (i.e., PBX, TDM switch); or a different DOD IP NE (i.e., SC, SS), based on the interconnection needs of the DOD user.

The MG shall have knowledge of which U.S. PSTN TDM, DOD TDM, or DOD IP NE (i.e., SC, SS) each U.S. CAS trunk group is connected.

SCM-006710 [Conditional] If the appliance supplier supports foreign CAS trunk groups, the MG shall support multiple foreign CAS trunk groups based on the needs of the DOD user deploying the appliance. The MG shall allow each foreign CAS trunk group at the MG to connect to a different foreign PSTN, or allied or coalition partner TDM network element (e.g., PBX, TDM switch), based on the interconnection needs of the DOD user.

The MG shall have knowledge of which foreign PSTN TDM, or allied or coalition partner TDM network element each foreign CAS trunk group is connected.

SCM-006720 [Optional] The MG may support reception of U.S. CAS trunk signaling sequences (i.e., Supervisory, Control, and Alerting) from the CCA MGC, and transmission of U.S. CAS trunk signaling sequences to the CCA MGC.

SCM-006730 [Optional: SC, SS] The MG may support the requirements for MLPP Trunk Selection (Hunting) in [Section 2.26.1.3.3](#), MLPP Trunk Selection (Hunting). The MG shall support these MLPP Trunk Selection requirements on MG CAS trunk groups to DSN EOs and DSN SS. The MG shall also support these requirements on MG CAS trunk groups to DSN SMEOs, PBX1s, and PBX2s (when supported).

SCM-006740 [Optional] To meet the above requirements, the MG may support the definitions of Precedence Level/Calling Area (PL/CA), classmarks, voice-grade trunk groups, data-grade trunk groups, route digit, direct route, alternative route, preemptive search, and friendly search.

2.16.8 MG Requirements: VoIP Interfaces Internal to an Appliance

The requirements in the following section assume that a supplier-specific Gateway Control Protocol is used on the MGC-MG interface. In this case, these requirements assume that the protocol layers below the application layer that carries the supplier-specific Gateway Control

Protocol either can be industry standard (in the following paragraph) or supplier specific, which is outside the scope of this document.

When the H.248 Gateway Control Protocol is used over the open interface between the MG and the MGC, this open interface supports industry-standard protocol layers (i.e., physical, data link, network, and transport) below the application layer that carries the Gateway Control Protocol. The support for these protocol layers is optional.

2.16.8.1 MG Support for VoIP Interconnection at the Physical and Data Link Layers

SCM-006750 [Required] The MG shall connect to the ASLAN of the appliance using the physical layer and data link layer protocols of the ASLAN. In this case, the MG shall appear to the MGC, SBC, and appliance PEIs/UEIs as a physical layer and data link layer endpoint on a LAN switch in the ASLAN.

2.16.8.2 MG Support for VoIP Interconnection at the Network Layer

SCM-006760 [Required] The MG shall connect to the ASLAN of the appliance using the IP as a Network Layer Protocol. In this case, the MG shall appear to the MGC, SBC, and appliance PEIs/UEIs as an IP endpoint on an IP router on the ASLAN.

SCM-006770 [Required] The MG shall support IPv4 as a Network Layer Protocol, conformant with RFC 791.

SCM-006780 [Required] The MG shall also support IPv6 as a Network Layer Protocol, conformant with RFC 2460.

SCM-006790 [Required] Conformant with Section 5, IPv6, the MG shall support dual IPv4 and IPv6 stacks (i.e., support both IPv4 and IPv6 in the same IP end point) as described in RFC 4213.

SCM-006800 [Conditional] If an open H.248 MGC-MG interface is used, then the MG shall support IPsec for use with securing IP packets containing H.248 signaling messages and encapsulated ISDN PRI signaling messages. The MG support for IPsec shall be conformant with the appliance IPsec requirements in Section 4, Information Assurance.

NOTE: The MG is not required to support IPsec for use in IP packets containing SRTP media streams for VoIP, FoIP, and MoIP calls.

2.16.8.3 MG Support for VoIP Interconnection at the Transport Layer

The following conditional requirements apply if an open MGC-MG interface, that is optional, is supported:

SCM-006810 [Conditional] If an open MGC-MG interface is used, then the MG shall support transport of H.248 signaling messages and encapsulated ISDN PRI signaling messages using the

TCP as a Transport Layer Protocol. In this case, the MG shall support TCP conformant with RFC 793.

SCM-006820 [Conditional] If an open MGC-MG interface is used, then the MG shall support transport of H.248 signaling messages and encapsulated ISDN PRI signaling messages using the UDP as a Transport Layer Protocol. In this case, the MG shall support UDP conformant with RFC 768.

SCM-006830 [Conditional] If an open MGC-MG interface is used, then the MG shall support transport of H.248 signaling messages and encapsulated ISDN PRI signaling messages using the SCTP as a Transport Layer Protocol. In this case, the MG shall support SCTP conformant with RFC 4960.

SCM-006840 [Conditional] If an open MGC-MG interface is used, then the MG shall support a per-MG parameter that controls which of the three Transport Layer Protocols (i.e., UDP, TCP, or SCTP) is used to exchange H.248 signaling messages and encapsulated PRI signaling messages with the MGC. This parameter shall support the following values:

- a. When this parameter is set to “TCP,” the MG shall exchange application layer messages with the MGC using TCP.
- b. When this parameter is set to “UDP,” the MG shall exchange application layer messages with the MGC using UDP.
- c. When this parameter is set to “SCTP,” the MG shall exchange application layer messages with the MGC using SCTP.

NOTE: The MG is not required to support TLS at the Transport Layer for securing H.248 signaling messages or encapsulated PRI signaling messages that are exchanged with the MGC using UDP, TCP, or SCTP. IPsec, which provides security at the Network Layer, is used in these cases instead of TLS, which provides security at the Transport Layer. Transport Layer Security is used elsewhere in the appliance to secure UC SIP signaling messages on the appliance-to-UEI and appliance-to-appliance interfaces, but it is not used to secure H.248 or PRI signaling messages on the MG-to-MGC interface.

NOTE: The SCTP is used in other telecommunication industry documents as the Transport Layer Protocol for communication between VoIP SSs and their MGs.

2.16.8.4 MG Support for VoIP Interconnection for Media Stream Exchange Above the Transport Layer

SCM-006850 [Required] The MG shall support exchange of VoIP media streams with appliance PEIs/UEIs, other appliance MGs, and the appliance SBC (and through the appliance SBC, with other PEIs/UEIs and MGs on other network appliances) using the following IETF-defined Media Transfer Protocols:

- a. SRTP, conformant with RFC 3711.
- b. SRTCP, conformant with RFC 3711.

SCM-006860 [Required] The MG shall secure all VoIP media streams exchanged with appliance PEIs/UEIs, other appliance MGs, and the appliance SBC (and through the SBC, with PEIs/UEIs and MGs on other network appliances) using SRTP and SRTCP.

SCM-006870 [Required] The MG shall use UDP as the underlying Transport Layer Protocol, and IP as the underlying Network Layer Protocol, when SRTP is used for media stream exchange.

2.16.8.5 MG Support for VoIP Interconnection for Signaling Stream Exchange Above the Transport Layer

SCM-006880 [Conditional] If an open MGC-MG interface is used, then the MG shall support exchange of VoIP signaling streams with the appliance MGC. When the VoIP signaling streams contain ISDN PRI signaling messages at the Application Layer, the MG shall use the ISDN User Adaptation (IUA) Protocol between the Transport Layer and the Application Layer (the ISDN PRI signaling). The MG shall support the IUA Protocol consistent with RFC 4233.

NOTE: The IUA Protocol is used in other telecommunication industry documents as the ISDN Adaptation Layer Protocol above the SCTP Transport Layer Protocol for ISDN communication between VoIP SSs and their MGs.

SCM-006890 [Conditional] If the VoIP signaling streams contain supplier-proprietary protocol messages instead of H.248 or ISDN PRI messages, then the MG shall secure the proprietary protocol message exchange with the MGC using mechanisms that are as strong as, or stronger than, the use of IPsec to secure H.248 and PRI message exchange.

2.16.8.6 MG Support for VoIP Interworking for ISDN PRI Trunks

SCM-006900 [Required] When an MG interworks a TDM call from an ISDN PRI trunk group with a VoIP session within the network appliance, the MG shall perform the following:

- a. Convert between the ISDN media stream on the ISDN PRI B-Channel and the VoIP SRTP/Transport Layer/IP media stream within the appliance.
- b. **[Optional]** Convert between ISDN signaling messages (ITU-T Recommendation Q.931 messages in Q.921 frames) on the ISDN PRI D-Channel and encapsulated ISDN signaling messages (ITU-T Recommendation Q.931 messages in IUA frames) in a VoIP IUA/Transport Layer/IPsec signaling stream within the appliance.

NOTE: The method of converting PRI signaling into VoIP signaling and the method of conveying this information to and from the CCA are dependent on the MGC protocol used. Some protocols will not use encapsulation at all. If H.248 is used, signaling is encapsulated between the MG and CCA.

2.16.8.6.1 MG Support for VoIP Interworking for National ISDN PRI

SCM-006910 [Optional] For U.S. ISDN PRI trunks carrying National ISDN PRI signaling, the MG shall interwork the National ISDN PRI Data Link Layer Protocol (the National ISDN version of ITU T Recommendation Q.921) with the IETF IUA Protocol and the underlying Transport Layer and IPsec protocols.

2.16.8.7 MG Support for VoIP Interworking for CAS Trunks

Support for CAS trunks is optional, but if they are supported the MG needs to read and understand incoming CAS signaling sequences before translating them into MGC messages and sending them to the MGC using IP. Similarly, the MG has to understand and generate outgoing CAS signaling sequences after receiving signaling messages from the MGC using IP and translating the signaling messages into the appropriate CAS signaling sequences. The method of converting CAS signaling into VoIP signaling and the method of conveying this information to and from the CCA are dependent on the MG control protocol used. The H.248 protocol provides a standard way of doing this.

2.16.8.7.1 MG Support for VoIP Interworking for U.S. CAS Trunks

SCM-006920 [Conditional] If the MG supplier supports U.S. CAS trunks, then the MG shall interwork a TDM call from a U.S. CAS trunk with a VoIP session within the appliance and shall perform the following:

- a. Convert between the TDM media stream on the CAS trunk and the VoIP SRTP/Transport Layer/IP media stream within the appliance.
- b. Convert between the CAS signaling sequences on the CAS trunk and the VoIP signaling sequences within the appliance.

2.16.8.7.2 MG Support for VoIP Interworking for Foreign CAS Trunks

SCM-006930 [Conditional] If the MG supplier supports foreign CAS trunks, then the MG shall interwork a TDM call from a foreign CAS trunk with a VoIP Session within the appliance and shall perform the following:

- a. Convert between the TDM media stream on the foreign CAS Trunk and the VoIP SRTP/Transport Layer/IP media stream within the appliance.
- b. Convert between the CAS signaling sequences on the foreign CAS trunk and the VoIP signaling sequences within the appliance.

2.16.8.8 MG Support for VoIP Codecs for Voice Calls

The MG must support a set of internationally standard and DISN-standard VoIP codecs for use in converting TDM media streams to VoIP media streams, and in converting VoIP media streams to TDM media streams.

SCM-006940 [Required] The MG shall support TDM voice streams using the following:

- a. ITU-T 64 Kbps G.711 μ -law PCM over digital trunks.
- b. ITU-T 64 Kbps G.711 A-law PCM over digital trunks.
- c. North American 56 Kbps G.711 μ -law PCM over digital trunks.
- d. North American analog voice transmission over analog trunks on TDM trunk groups on the TDM side of the MG.

SCM-006950 [Required] The MG shall convert between North American 56 Kbps G.711 μ -law PCM and ITU-T 64 Kbps G.711 μ -law PCM in cases where North American 56 Kbps TDM voice trunks are used on the TDM side of the MG.

SCM-006960 [Required] The MG shall convert between North American analog voice transmission and ITU T 64 Kbps G.711 μ -law PCM in cases where North American analog voice trunks are used on the TDM side of the MG.

SCM-006970 [Conditional] If the MG supplier supports analog foreign CAS trunks, then the MG shall support TDM voice streams using international (foreign) analog voice transmission over analog trunks on TDM trunk groups on the TDM side of the MG.

SCM-006980 [Conditional] If the MG supplier supports analog foreign CAS trunks, then the MG shall convert between international (foreign) analog voice transmission and ITU-T 64 Kbps G.711 A law PCM in cases where international (foreign) analog voice trunks are used on the TDM side of the MG.

2.16.8.8.1 Support for Uncompressed, Packetized VoIP per ITU-T Recommendation G.711

SCM-006990 [Required] The MG shall support uncompressed, packetized VoIP streams using ITU-T Recommendation G.711 μ law PCM and ITU-T Recommendation G.711 A-law PCM (ITU-T Recommendation G.711, November 1998, plus Appendix I, September 1999, and Appendix II, September 2000) over the IP network on the VoIP side of the MG.

SCM-007000 [Required] The MG shall packetize/depacketize G.711 media streams received or sent between its TDM side and its VoIP side.

SCM-007010 [Required] The MG shall transport each packetized G.711 VoIP stream to and from the destination local PEI, local UEI, local MG, remote PEI (via an SBC), remote UEI (via

an SBC), or remote MG (via an SBC) using SRTP, UDP, and IP protocol layers on the VoIP side of the MG.

SCM-007020 [Required] The MG shall support the use of uncompressed, packetized G.711 μ -law and A-law VoIP media streams for both Fixed and Deployable applications.

2.16.8.8.2 Support for Compressed, Packetized VoIP per ITU-T Recommendation G.72x

SCM-007030 [Required] The MG shall support compressed, packetized VoIP streams over the IP network on the VoIP side of the MG, according to the following international standards:

- a. ITU-T Recommendation G.723.1.
- b. ITU-T Recommendation G.729, plus Erratum 1, and Annexes A through J, and Appendices I, II, and III.

The MG shall use internal G.723.1 and G.729 codecs to perform this compression and decompression. These compressed VoIP codecs are referred to collectively as G.72x in this section. The MG shall use these internal codecs to 1) compress G.711 TDM media to G.72x VoIP media, for media transfer in the TDM-to-IP direction, and 2) decompress G.72x VoIP media to G.711 TDM media, for media transfer in the IP-to-TDM direction.

SCM-007040 [Required] The MG shall transport each packetized G.72x VoIP stream to and from the destination local PEI, local UEI, local MG, remote PEI (via an SBC), remote UEI (via an SBC), or remote MG (via an SBC) using SRTP, UDP, and IP protocol layers on the VoIP side of the MG.

SCM-007050 [Required] The MG shall support the use of packetized G.72x VoIP media streams for both Deployable and Fixed applications.

2.16.8.9 MG Support for Group 3 Fax Calls

SCM-007060 [Required] The MG shall support Group 3 Facsimile (G3 Fax) calls between TDM trunk-side interfaces on the MG, PEIs, UEIs, TAs, IADs, TDM line-side interfaces on the MG, and SBCs.

The MG shall support G3 Fax calls on TDM trunks for the following TDM trunk types:

- U.S. ISDN PRI.
- U.S. CAS trunk (Conditional: when the MG supplier supports U.S. CAS trunks).
- Foreign ISDN PRI (Required: When the MG supplier supports ETSI PRI – Optional: when the MG supplier supports other foreign ISDN PRIs).

SCM-007070 [Required] The MG support for G3 Fax calls on the TDM trunk types listed in this section shall be identical to the support for G3 Fax calls on these trunk groups in DOD TDM PBXs, EOs, Tandem switches, and MFSs.

SCM-007080 [Required] The MG support for G3 Fax calls on the TDM trunk types listed in this section shall allow G3 Fax calls to:

- a. Originate from a PEI, UEI, TA, IAD, or MG line card that supports G3 Fax, and terminate on a G3 Fax device in a TDM network (i.e., DOD; U.S. or foreign PSTN; allied or coalition partner), via an MG trunk card.
- b. Originate from a G3 Fax device in a TDM network (i.e., DOD; U.S. or foreign PSTN; allied or coalition partner) via an MG trunk card, and terminate on a PEI, UEI, TA, IAD, or MG line card supporting G3 Fax.
- c. Originate from a G3 Fax device in a TDM network, and terminate to a G3 Fax device in a TDM network, where either TDM network can be DOD, U.S. or foreign PSTN, or allied or coalition partner, when the VVoIP network is used as a tandem network in between the originating TDM network and the terminating TDM network.

SCM-007090 [Required] The MG shall support a mechanism to detect FoIP calls, to distinguish them from VoIP calls, and to treat them differently from VoIP calls. The MG shall support this FoIP detection mechanism on both TDM-to-FoIP calls (i.e., inbound from a TDM network to the IP appliance) and FoIP-to-TDM calls (i.e., outbound from the IP appliance to a TDM network).

SCM-007100 [Required] The MG shall not rely on called number screening or calling number screening for detecting inbound TDM-to-FoIP calls or outbound FoIP-to-TDM calls.

In other words, the IP appliance administrator are not be required to maintain a list of calling and called fax numbers that are local to the IP appliance (representing FoIP end points within the appliance), and a list of calling and called fax numbers that are outside the IP appliance (representing G3 Fax and FoIP end points outside of the appliance) to determine whether the call is an FoIP call.

SCM-007110 [Required] The MG, in conjunction with the MGC, shall support two separate options for “Handling of FoIP calls within the IP appliance:”

- a. Handle FoIP calls as G.711 VoIP calls (Fax Passthrough Calls).
- b. Handle FoIP calls as ITU-T Recommendation T.38 FoIP calls (Fax Relay Calls).

The MG and the MGC shall allow the IP appliance administrator to set the value of this option on a per-MG basis. Compression of FoIP calls via ITU-T Recommendation G.723.1 or G.729 is not recommended.

SCM-007120 [Required] In the case where an FoIP call enters the IP appliance MG over one TDM trunk or line card, and then leaves the same IP appliance MG over another TDM trunk or line card, the MG shall support the ability to interconnect the two-way TDM media streams from

the first trunk/line card directly with the two-way TDM media streams from the second trunk/line card, without performing any TDM-to-FoIP and FoIP-to-TDM conversions on those two TDM media streams.

2.16.8.9.1 MG Option to “Handle FoIP Calls as G.711 VoIP Calls” (Fax Passthrough Calls)

SCM-007130 [Required] When the MG is configured to “Handle FoIP calls as G.711 VoIP Calls,” the MG shall support the use of uncompressed, packetized G.711 μ -law and A-law FoIP media streams for both Fixed and Deployable applications.

SCM-007140 [Required] When the MG is configured to “Handle FoIP calls as G.711 VoIP Calls,” the MG shall handle FoIP calls within the appliance in exactly the same way it handles G.711 VoIP calls within the appliance (e.g., the MG shall not allow compression of the media streams on these calls), with these clarifications:

- a. The MG shall still disable ECs for a FoIP call being handled as a G.711 VoIP call, when the MG detects an “EC disabling” tone from either the TDM side or the FoIP side of the call (see [Section 2.16.9](#), MG Requirements for Echo Cancellation).
- b. The MG may disable silence suppression on the FoIP side of the call.

SCM-007150 [Required] When the MG is configured to “Handle FoIP calls as G.711 VoIP Calls,” the MG shall support uncompressed, packetized FoIP streams using ITU-T Recommendation G.711 μ -law PCM and G.711 A-law PCM over the IP network on the FoIP side of the MG.

SCM-007160 [Required] When the MG is configured to “Handle FoIP calls as G.711 VoIP Calls,” the MG shall transport each packetized G.711 FoIP stream to and from the local EI/IAD/TA, local MG, remote EI/IAD/TA (via an SBC), or remote MG (via an SBC) using SRTP, UDP, and IP protocol layers on the FoIP side of the MG.

NOTE: That end-to-end (E2E) synchronization of the calling and called fax machines (or fax-equipped devices) is not guaranteed on a fax passthrough call. Even though a fax passthrough call may complete between these two devices (i.e., a successful UC SIP signaling INVITE/200 OK/ACK exchange can occur, and G.711 media can be exchanged over SRTP, UDP, and IP), there is no guarantee that the two devices will be able to synchronize and exchange fax data using the resulting G.711 media streams. Even if the two devices do synchronize and exchange fax data, there is no guarantee that this synchronization and exchange will be maintained over time, or that the synchronization and exchange will result in a data throughput that matches what would be provided by a Fax Relay call, or by an E2E TDM fax call in a TDM voice network.

Because of this, there are no requirements in this section for the reliability of fax synchronization, reliability of data exchange, or rate of data transfer on fax passthrough calls. It

is expected that these calls will complete using UC SIP signaling and SRTP media exchange like VoIP calls do. However, it is not expected that the resulting synchronization and data exchange will be 100 percent reliable, or that the data rate provided will match what would be provided on a Fax Relay call or a TDM fax call under the same conditions.

2.16.8.9.2 MG Option to “Handle FoIP Calls as T.38 FoIP Calls” (Fax Relay Calls)

SCM-007170 [Required] When the MG is configured to “Handle FoIP Calls as T.38 FoIP Calls,” the MG shall not handle FoIP calls within the appliance in the same way it handles G.711 VoIP calls within the appliance. Instead, upon detection that a VoIP call request is actually a FoIP call request, the MG shall direct the FoIP call request to a “T.38 Fax Server” that is internal to the appliance.

NOTE: This “T.38 Fax Server” may be part of the MG, part of the separate UFS Server in the appliance, or part of the separate media server in the appliance.

SCM-007180 [Required] The T.38 Fax Server shall support the full set of procedures and protocols for Fax Relay in ITU-T Recommendation T.38.

SCM-007190 [Required] The T.38 Fax Server shall support the full set of procedures and protocols for Group 3 Fax reception and transmission in ITU-T Recommendation T.4.

SCM-007200 [Required] The T.38 Fax Server shall support adequate T.38 Fax Relay resources so at least 10 percent of the total number of calls that pass through the trunk-side interfaces of the MG (from TDM end points to IP end points, or from IP end points to TDM end points) can receive Fax Relay treatment, instead of receiving Fax Passthrough treatment.

NOTE: The acquiring activity for the MG and T.38 Fax Server should also determine, based on traffic engineering and vendor prices, the required number of MG Fax Relay resources [e.g., Fax-Relay-equipped trunk cards, or Fax Relay Digital Signal Processing (DSP) cards] that will support T.38 Fax Relay. T.38 Fax Relay is needed to support IP fax devices on an SC or SS, and analog fax devices behind TAs, IADs, and MG line cards on an SC or SS.

2.16.8.10 MG Support for ISDN Over IP Calls and 64-Kbps Clear Channel Data Streams

SCM-007210 [Required] The MG shall support 64-Kbps Clear Channel Data on TDM trunks for the following TDM trunk types:

- a. U.S. ISDN PRI.
- b. **[Required: When MG supports ETSI PRIs – Optional: When MG supports other foreign ISDN PRIs]** Foreign ISDN PRI.

SCM-007220 [Required] Media Gateway support for 64-Kbps Clear Channel Data calls on the TDM trunk types listed in this section shall be identical to the support for 64-Kbps Clear Channel Data on these trunk groups in DOD TDM PBXs, EOs, Tandem Switches, and MFSs.

SCM-007230 [Required] Media Gateway support for 64-Kbps Clear Channel Data calls on the trunk types listed in this section shall allow 64-Kbps Clear Channel Data calls to originate or terminate between an EI supporting 64-Kbps Clear Channel Data and an ISDN terminal supporting 64-Kbps Clear Channel Data in a TDM network (i.e., DOD, U.S. or foreign PSTN, allied or coalition partner). This includes the case when both the calling and called ISDN terminals are on TDM networks, and the IP network is used as a tandem network in between the originating TDM network and the terminating TDM network.

SCM-007240 [Required] The MG shall support a mechanism to detect 64-Kbps Clear Channel Data calls; to distinguish them from VoIP, FoIP, MoIP, and SCIP over IP calls; and to treat them differently from VoIP, FoIP, MoIP, and SCIP over IP calls. The MG shall support this 64-Kbps Clear Channel Data detection mechanism on both TDM-to-IP calls (i.e., inbound from a TDM network to the IP appliance) and IP-to-TDM calls (i.e., outbound from the IP appliance to a TDM network).

SCM-007250 [Required] When a 64-Kbps Clear Channel Data call enters the IP appliance MG over one TDM trunk, and then leaves the same IP appliance MG over another TDM trunk, the MG shall support the ability to interconnect the two-way TDM media streams from the first trunk directly with the two-way TDM media streams from the second trunk, without performing any TDM-to-IP and IP-to-TDM conversions.

SCM-007260 [Required] The MG shall support the procedures and protocols for carrying 64-Kbps Clear Channel Data streams over IP, UDP, and RTP as described in RFC 4040. This shall include the coding of SDP MIME parameters in the following manner (as excerpted from RFC 4040):

- a. MIME media type name: audio.
- b. MIME subtype name: clearmode.
- c. Optional parameters:ptime, maxptime.
 - (1) “ptime” gives the length of time in milliseconds represented by the media in a packet, as described in RFC 4566.
 - (2) “maxptime” represents the maximum amount of media that can be encapsulated in each packet, expressed as time in milliseconds, as described in RFC 4566.
- d. Encoding considerations: This type is only defined for transfer via RTP.
- e. Parameter mapping considerations:
 - (1) The MIME type (audio) goes in the SDP “m=” attribute as the media name.

- (2) The MIME subtype (clearmode) goes in the SDP “a=rtpmap” attribute as the encoding name.
- (3) The optional parameters “ptime” and “maxptime” go in the SDP “a=ptime” and “a=maxptime” attributes, respectively.

2.16.8.11 MG Support for “Hairpinned” MG Calls

SCM-007270 [Required] The MG shall support VoIP sessions between trunks on the same MG, including all combinations of TDM call legs and VoIP media end points.

SCM-007280 [Required] In the TDM-to-TDM sessions, the MG shall not establish any IP, UDP/TCP/SCTP, RTP, or VoIP codec communication between the “call-originating” and “call-terminating” side of the MG. In addition, the MG shall not establish any TDM-to-VoIP media conversion, or VoIP-to-TDM media conversion, on either side of the MG, for either direction of media transmission.

2.16.8.12 MG Support for Multiple Codecs for a Given Session

SCM-007290 [Required] Each media gateway shall support at least ten audio and voiceband data codecs, including the eight identified as follows:

- a. ITU-T G.711 μ -law.
- b. ITU-T G.711 A-law.
- c. ITU-T G.722.1.
- d. ITU-T G.723.1.
- e. ITU-T G.729 or G.729A.
- f. IETF RFC 4040 (G.711 clear mode).
- g. ITU-T T.38 Fax Relay.
- h. ITU-T V.150.1 Modem Relay.

The media gateway shall be capable of simultaneously offering at least five codecs for a given session, except when RFC 4040 is used.

2.16.9 MG Requirements for Echo Cancellation

The following basic requirements for MG Echo Cancellation are based on the commercial VoIP network Echo Cancellation requirements in Telcordia Technologies GR-3055-CORE.

2.16.9.1 Trunk Gateway Echo Cancellation

SCM-007300 [Required] The MG shall provide an echo canceller (EC) capability with an echo path capacity (echo tail length) of at least 64 ms.

SCM-007310 [Optional] The MG may provide an EC capability with an echo path capacity (echo tail length) of at least 128 ms.

According to ITU Recommendation G.168, ECs may remain active for several types of non-voice calls as well; in particular, for G3 Fax calls and VBD modem calls.

SCM-007320 [Required] The MG shall provide echo cancellation for voice, G3 Fax, and VBD modem fax calls. (In the G3 Fax and VBD modem call cases, the MG shall provide echo cancellation if an “echo canceller disabling signal” is not sent by any end user’s equipment on the G3 Fax or modem call.) This echo cancellation shall conform to the echo cancellation requirements specified in ITU-T Recommendation G.168.

SCM-007330 [Required] Each MG EC shall be equipped with an “echo canceller disabling signal” tone detector. This tone detector shall detect and respond to an in-band EC disabling signal from an end user’s G3 Fax or VBD modem device. The EC disabling signal detected shall consist of a 2100-Hz tone with periodic phase reversals inserted in that tone.

SCM-007340 [Required] The MG tone detector/EC disabler shall detect the “echo canceller disabling signal” and disable the MG EC when, and only when, that signal is present for G3 Fax or VBD modem.

SCM-007350 [Required] The MG shall support all DSN Echo Cancellation requirements in [Section 2.26.5](#), Echo Canceller. In the case of a discrepancy between the DSN Echo Cancellation requirements in [Section 2.26.5](#) and the VVoIP Echo Cancellation requirements here, the VVoIP Echo Cancellation requirements here shall take precedence.

2.16.10 MG Requirements for Clock Timing

SCM-007360 [Required] The MG shall derive its clock timing from a designated T1 or PRI interface.

SCM-007370 [Required: MG] The MG shall meet the external timing mode requirements specified in the Telcordia Technologies GR-518-CORE, Paragraph 18.1. Most SMEOs and PBX1s will only support line timing.

SCM-007380 [Required: MG] The MG shall support external timing modes as defined in Telcordia Technologies TR-NWT-001244.

SCM-007390 [Required: MG] The MG shall support line timing modes as defined in Telcordia Technologies TR-NW-001244.

SCM-007400 [Required: MG] The MG shall provide internal clock requirements as described in the Telcordia Technologies GR-518-CORE, Paragraph 18.2.

SCM-007410 [Required: MG] The MG shall provide a stratum 4 or better internal clock.

SCM-007420 [Required: MG] The MG shall meet the synchronization performance monitoring criteria as described in Telcordia Technologies GR-518-CORE, Paragraph 18.3.

SCM-007430 [Required: MG] The MG shall meet the DS1 traffic interfaces as described in the Telcordia Technologies GR 518-CORE, Paragraph 18.4.

SCM-007440 [Required: MG] The MG shall meet the DS0 traffic interconnects as described in the Telcordia Technologies GR 518-CORE, Paragraph 18.5.

2.16.11 MGC-MG CCA Functions

NOTE: A MGC and MG(s) are optional for Deployable SC locations.

SCM-007450 [Required] The MGC within the CCA shall be responsible for controlling all the MGs within the SC or SS.

SCM-007460 [Required] The MGC within the CCA shall be responsible for controlling all the trunks (i.e., PRI or CAS) within each MG within the SC or SS.

SCM-007470 [Required] The MGC within the CCA shall be responsible for controlling all media streams on each trunk within each MG.

SCM-007480 [Required] The MGC within the CCA shall accept IP signaling streams from an MG, conveying received PRI or CAS trunk signaling. The MGC shall return IP signaling streams to the MG accordingly, for conversion to transmitted PRI or CAS trunk signaling.

SCM-007490 [Conditional] If the appliance supplier supports foreign PRI or CAS trunks on its product, the CCA shall know which national variant of PRI or CAS signaling (e.g., ETSI/TTC/TTA; Germany/Japan/South Korea) the Foreign PRI or CAS Trunk supports.

SCM-007500 [Required] Within the appliance (i.e., SC or SS), the MGC shall use either ITU-T Recommendation H.248 (Gateway Control Protocol Version 3) or a supplier-proprietary protocol to accomplish the MG, trunk, and media stream controls described previously.

2.16.11.1 MG Support for MGC-MG Signaling Interface

An open MGC-MG interface that involves ITU-T Recommendation H.248 is optional. A closed (i.e., proprietary) MGC-MG interface may be used instead.

SCM-007510 [Optional] The MGC may use ITU-T Recommendation H.248 for MG control.

SCM-007520 [Required] The MGC protocol for MG control (MG Control Protocol) shall support the following:

- a. Control message exchanges that are functionally equivalent to the control message exchanges used in ITU-T Recommendation H.248.

- b. Transport Layer functionality, including message sequencing, detection of message loss, and recovery from message loss, which are functionally equivalent to the sequencing, loss detection, and loss recovery mechanisms in TCP and SCTP.
- c. Strong security for the exchange of gateway control messages and their underlying Transport Layer packets and Network Layer packets, so security controls (i.e., MG and MGC authentication, encryption and decryption of exchanged messages down to the Network Layer) are at least as strong as the IPSec security protection used when ITU-T Recommendation H.248 is used as the MGC-MG protocol. This strong security shall be supported consistent with the H.248-over-IPSec requirements in Section 4, Information Assurance.

SCM-007530 [Required] The CCA and MGC shall be able to select the VoIP codec used by the MG to match the type of end point (i.e., PEI, UEI, SBC) and service requested (i.e., uncompressed VoIP; compressed VoIP, FoIP, MoIP, SCIP over IP; or video over IP).

SCM-007540 [Required] The CCA and MGC shall ensure that both endpoints of each VVoIP session use the same VVoIP codec for both directions of media stream transmission between the MG and the peer SBC, PEI, UEI, or other MG. (“VVoIP session,” as used here, includes VoIP sessions, FoIP sessions, MoIP sessions, SCIP over IP sessions, and video over IP sessions.)

SCM-007550 [Required] If the VoIP codec requested by a calling or called PEI, UEI, or SBC end point does not match any of the VVoIP codecs supported by a called or calling MG end point (based on CCA signaling with the EI or SBC, and MGC signaling with the MG), the CCA shall reject the VVoIP media “offer” from this calling or called end point, and indicate to the calling or called end point which VVoIP codec(s) should be used to send compatible VVoIP media to that MG.

“SBC end point,” as used here, means a remote PEI, UEI, or MG endpoint served by another appliance elsewhere on the DISN WAN, where signaling and media streams enter the Local Assured Services Domain from the DISN WAN via that domain’s SBC.

“VVoIP codec,” as used here, includes VoIP codecs, FoIP codecs, MoIP codecs, SCIP over IP codecs, and video over IP codecs.

“VVoIP media,” as used here, includes VoIP media, FoIP media, MoIP media, SCIP over IP media, and video over IP media.

SCM-007560 [Required] Since the CCA and MGC support selection and negotiation of VoIP codecs on calls to and from MGs, the CCA and MGC shall support, at a minimum, the following set of ITU-T standard VoIP codecs:

- a. ITU-T Recommendation G.711, both North American μ -law and international A-law variants.
- b. ITU-T Recommendation G.723.1.

- c. ITU-T Recommendation G.729.

2.16.11.2 MG Support for Encapsulated National ISDN PRI Signaling

SCM-007570 [Required] The MG shall transport ISDN PRI signaling messages between the MG and the MGC. The MG shall support the following:

- a. Transparent passing of ISDN PRI messages between the MG and MGC.
- b. Preservation of correct message sequences, in both directions of transmission.
- c. Detection of message loss and recovery from message loss (e.g., by retransmission of lost messages), in both directions of transmission.
- d. Detection of message errors and correction of message errors (e.g., by retransmission of errored messages), in both directions of transmission.
- e. Securing of ISDN PRI messages using MG and MGC encryption, in both directions of transmission.

The MG shall support all these capabilities over the supplier-specific protocol so the resulting exchange of ISDN PRI messages (and security of exchanged ISDN PRI messages) is identical to what would occur if IUA, UDP/TCP/SCTP, and IPsec were used.

SCM-007580 [Conditional] If an open protocol is used to support the transport of ISDN PRI signaling messages between the MG and MGC, then the MG shall use the following protocol stack to support encapsulation of ISDN PRI signaling messages sent from the MG to the MGC, and de-encapsulation of ISDN PRI signaling messages sent from the MGC to the MG:

- a. National ISDN PRI signaling messages, as described in Telcordia Technologies SR 4994.
- b. IUA frames, where IUA shall be supported as defined in RFC 4233.
- c. One of the following IETF-standard Transport Layer Protocols:
 - (1) TCP.
 - (2) UDP.
 - (3) SCTP.
- d. IPsec packets, secured using mutual MGC and MG encryption, at the IP Network Layer. This encryption shall be performed consistent with the MGC and MG encryption of encapsulated ISDN PRI messages described in Section 4, Information Assurance.

2.16.11.3 MG Support for Mapped CAS Trunk Signaling Using H.248 Packages for MF and DTMF Trunks

SCM-007590 [Conditional] If CAS trunks and trunk signaling are supported, then the MG shall transport the CAS trunk signaling between the MG and the MGC. In this case, the MG shall still support the following:

-
- a. Transparent passing of CAS trunk signaling (or indications of CAS trunk signaling) using supplier-specific messages between the MG and MGC.
 - b. Preservation of correct message sequences, in both directions of transmission.
 - c. Detection of message loss and recovery from message loss (e.g., by retransmission of lost messages), in both directions of transmission.
 - d. Detection of message errors and correction of message errors (e.g., by retransmission of errored messages), in both directions of transmission.
 - e. Securing of supplier-specific messages using MGC and MG encryption, in both directions of transmission.

The MG shall support all these capabilities over the supplier-specific protocol so the resulting exchange of CAS trunk signaling (and security of the messages carrying the CAS trunk signaling) is identical to what would occur if H.248, UDP/TCP/SCTP, and IPsec were used.

If CAS trunks and trunk signaling are supported and an open protocol is used to support the transport of CAS signaling messages between the MG and MGC, then the following conditional requirements apply:

SCM-007600 [Conditional] The MGC shall use the following protocol stack to support encapsulation of CAS trunk signaling sent from the MG to the MGC, and de-encapsulation of CAS trunk signaling sent from the MGC to the MG:

- a. ITU-T Recommendation H.248 signaling messages carrying indications of MGC-to-MG and MG-to-MGC signaling for Dual Tone Multifrequency (DTMF) trunks and MF trunks. This H.248 signaling message shall include DTMF, MF, and CAS information from the following H.248 packages:
 - (1) Basic DTMF Generator Package (from ITU-T Recommendation H.248.1).
 - (2) DTMF Detection Package (from ITU-T Recommendation H.248.1).
 - (3) Multi-Frequency Tone Generation and Detection Packages (from ITU-T Recommendation H.248.24).
 - (4) Basic CAS Packages (from ITU-T Recommendation H.248.25).
 - (5) International CAS Packages (from ITU-T Recommendation H.248.28).
- b. One of the following IETF-standard Transport Layer Protocols:
 - (1) TCP.
 - (2) UDP.
 - (3) SCTP.

- c. IPSec packets, secured using mutual MG and MGC encryption, at the IP Network Layer. This encryption shall be performed consistent with the MG and MGC encryption of H.248 messages described in Section 4, Information Assurance.

[Conditional] If CAS trunks and trunk signaling are supported, then the MGC shall support the following set of CAS trunk signals, consistent with their use in Telcordia Technologies GR-3055-CORE (for the MG) and GR-3051-CORE (for the MGC):

- a. Seizure Signal. A signal, sent from the originating switching system (or MGC/MG) to the terminating switching system (or MGC/MG), that defines the transition from the trunk idle state to the trunk seizure state.
- b. Addressing Control Signal. A signal that marks the transition from the seizure state to the addressing state. Two addressing control methods of operation exist:
 - (1) Wink Start. After receiving a seizure signal, the terminating switching system (or MGC/MG) sends an off-hook signal with a defined duration (wink) to indicate that it is prepared to receive address information.
 - (2) Immediate-Dial. No addressing control signal is used. The originating switching system (or MGC/MG) waits for a specified time after sending a seizure signal before sending the first address digit.
- c. Answer Signal. A signal that defines the transition from the call-processing state to the communications state, and persists for the duration of the communications state.
- d. Transfer of address digits using DTMF signaling for DTMF trunk groups.
- e. Transfer of address digits using MF signaling for MF trunk groups.
- f. Disconnect Signal. A signal that defines the transition from the call-processing state or the communications state to the idle state.

2.16.11.4 MG Support for Glare Conditions on Trunks

In DSN switching systems, glare occurs when both interfaces of switching systems connected to the same inter-switching-system facility (trunk) apply a seizure signal at approximately the same time. In this section, at least one of the “switching systems connected to the same inter-switching-system facility (trunk)” is an SC or SS MG, as represented by a CAS trunk group.

NOTE: MG support for CAS trunks is optional.

SCM-007610 [Conditional: SC, SS] If CAS trunks and trunk signaling are supported, then the MG shall provide functions required to handle a glare situation on CAS trunks as specified in Telcordia Technologies GR-506-CORE, Section 11.5, Glare Resolution.

2.16.11.5 MGC and IWF Treatments for PRI-to-UC SIP Mapping for TDM MLPP

[Required] In conjunction with the IWF, the MGC shall support the following mapping of PRI-signaled MLPP information to UC SIP-signaled Reservation Priority High (RPH) information on calls or sessions that involve TDM MLPP and PRI/UC SIP interworking:

- a. The four Network Infrastructure (NI) digits received in octets 5 and 6 of the ISDN PRI precedence level IE shall be mapped to the network-domain subfield of the Namespace field in the UC SIP RPH.
- b. The “MLPP Service domain” information received in octets 7, 8, and 9 of the ISDN PRI precedence level IE shall be mapped to the precedence-domain subfield of the Namespace field in the UC SIP RPH.
- c. The “Precedence level” information received in bits 4 through 1 of octet 4 of the ISDN PRI precedence level IE shall be mapped to the “Resource-Priority (r-priority)” field in the UC SIP RPH.

In the absence of a received ISDN PRI precedence level IE, the following requirements apply:

SCM-007620 [Required] The MGC/IWF shall use a default network-domain value of “uc” in the Namespace field in the UC SIP RPH.

SCM-007630 [Required] The MGC/IWF shall use a default precedence-domain value of “000000” in the Namespace field in the UC SIP RPH.

SCM-007640 [Required] The MGC/IWF shall use a default Resource Priority value of “0 (Routine)” in the “r-priority” field in the UC SIP RPH.

SCM-007650 [Required] The MGC/IWF shall support mapping of the four NI digits to the network-domain subfield of the Namespace field in the RPH as follows:

- a. Until the 2012 timeframe, the MGC/IWF shall always use the value “uc” in the network-domain subfield, independent of the NI digits received.
- b. For the 2012-and-onwards timeframe, the MGC/IWF shall first check the NI digits translation table that is configured in the CCA for the PRI on which the precedence level IE was received. [Table 2.16-1](#), NI Digit Translation Table, contains a set of valid NI digit sequences (e.g., 0000, 0001, 0002) that the MGC/IWF will accept on that PRI, and the corresponding set of RPH network-domain values (e.g., “uc,” “cuc,” “dod,” “nato”) that the valid NI digit sequences map to.

Table 2.16-1. NI Digit Translation Table

LEVEL IE NI DIGITS	OUTPUT SIP RPH NETWORK DOMAIN
0000	uc
0001	cuc

LEVEL IE NI DIGITS	OUTPUT SIP RPH NETWORK DOMAIN
0002	dod
0003	nato
LEGEND	
IE: Information Element	RPH: Resource Priority Header
NI: Network Identifier	SIP: Session Initiation Protocol

- c. For the 2012-and-onwards timeframe, the MGC/IWF shall set the value in the network-domain subfield to the network-domain value that is configured for the received NI digits in this translation table for the PRI in question.

If the received NI digits are not included in the translation table for this PRI, the MGC/IWF shall use a default network-domain value of “uc” for this call.

SCM-007660 [Required] The MGC/IWF shall support mapping of the PRI “MLPP Service domain” field to the precedence-domain subfield of the Namespace field in the RPH as follows:

- a. The MGC/IWF shall convert the three-octet hexadecimal values from the three-octet PRI MLPP service domain field into a text string consisting of six text characters. The MGC/IWF shall use this six-character string as the precedence-domain subfield of the Namespace field in the RPH. For example:
- (1) For the 2012-and-onwards timeframe, the MGC/IWF shall set the NI digits value to the NI digits value that is configured for the received network-domain value in this translation table for the PRI in question.
- b. If the received network-domain value is not included in the translation table for this PRI, the MGC/IWF shall use a default NI digits value of “0000” for this call.

SCM-007670 [Required] The MGC/IWF shall support mapping of the precedence-domain subfield of the Namespace field in the RPH to the PRI MLPP service domain field as follows:

- a. The MGC/IWF shall replace the six-character text string from the RPH precedence-domain with the hexadecimal-encoded number “000000” in the three-octet PRI MLPP service domain field. The MGC/IWF shall use this three-octet hexadecimal-encoded number, “000000,” in the MLPP service domain field in the ISDN PRI precedence level IE.

SCM-007680 [Required] The MGC/IWF shall support mapping of the Resource-Priority field of the RPH to the PRI Precedence Level field (a semi-octet) as follows:

- a. If the network-domain field in the RPH is “uc,” then the MGC/IWF shall set the Precedence Level field in the ISDN PRI precedence level IE according to [Table 2.16-2, Mapping of RPH r-priority Field to PRI Precedence Level Value](#).

Table 2.16-2. Mapping of RPH r-priority Field to PRI Precedence Level Value

MLPP PRECEDENCE LEVEL	PRI PRECEDENCE LEVEL VALUE (DECIMAL NUMBER, SEMI-OCTET)	RPH FIELD (SINGLE CHARACTER, TEXT)
ROUTINE	4	0
PRIORITY	3	2
IMMEDIATE	2	4
FLASH	1	6
FLASH OVERRIDE	0	8
Spare, not used	5 through 15	0
LEGEND		
MLPP: Multilevel Precedence and Preemption PRI: Proprietary End Instrument RPH: Resource Priority Header		

- b. If the network-domain field in the RPH is any value other than “uc,” then the MGC/IWF shall set the Precedence Level field in the ISDN PRI precedence level IE to the value of “0 1 0 0” (4, meaning Routine).

2.16.11.6 MGC Support for MG-to-MG Calls

SCM-007690 [Required] The MGC shall be able to support multiple MGs.

SCM-007700 [Required] The MGC shall support VoIP sessions between trunk/line cards on the same or different MGs of the MGC, without requiring them to route to a VoIP EI on the appliance, or requiring them to be routed through the appliance’s SBC to the DISN WAN.

SCM-007710 [Required] For MG-to-MG sessions where a single MG is involved, the MGC shall handle MG-to-MG calls within a single MG as TDM-to-TDM calls that are local to the MG, rather than as TDM-to-VoIP-to-TDM calls that use VoIP resources within the MG and other appliance components. In this case, the MGC shall instruct the MG to connect the TDM media locally from the one TDM leg of the call, to the TDM media from the other TDM leg of the call, for both directions of TDM media transmission.

2.16.12 MGs Using the V.150.1 Protocol

SCM-007720 [Required: MG] Whenever the MG uses ITU-T Recommendation V.150.1, the following applies:

- a. ITU-T Recommendation V.150.1 provides for three states: audio, VBD, and modem relay. After call setup, inband signaling may be used to transition from one state to another. In addition, V.150.1 provides for the transition to FoIP using Fax Relay per ITU-T Recommendation T.38.
- b. When the MG uses V.150.1 inband signaling to transition between audio, FoIP, modem relay, or VBD states or modes, the MG shall continue to use the established session’s

protocol (e.g., decimal 17 for UDP) and port numbers so that the transition is transparent to the SBC.

2.16.13 MG Preservation of Call Ringing State During Failure Conditions

SCM-007730 [Required: SC MG, SS MG] The SC MG and SS MG shall not allow UC SIP sessions that have reached the ringing state (i.e., an UC SIP 180 (Ringing) message or 183 (Session Progress) has been sent from the called party to the calling party, and the calling party is receiving an audible ringing tone) to fail when an internal failure occurs within that MG. (“Internal failure” as used here includes cases where one component of the MG fails, and a failover occurs within the MG so a second redundant component is brought into service to replace the first failed component.) Instead, the MG shall ensure that the “call ringing state” is preserved (rather than dropped) at both the calling party interface (where audible ringing tone is being returned to the caller) and the called party interface (where incoming call alerting is being provided to the called party).

2.16.14 Remote Media Gateway

SCM-007740 [Conditional: SC, SS, Remote MG, SBC] If an MG is geographically separated from the MGC that controls it, then the following five specific conditional requirements address the SBC, the MG control protocol, the DSCP for the control packets, and the security aspects for that arrangement.

SCM-007750 [Conditional: Remote MG, SBC] The SRTP media stream and the H.248.1 control packets shall pass through an SBC deployed as part of the Remote MG SUT. The H.248.1 protocol uses well known UDP ports: MG port 2727 and MGC port 2427. Within the IPsec channel, these two ports shall be left open by the SBC, which shall only allow authenticated SCs and SSs to access these port numbers. The requirements for the SBC are given in [Section 2.17.10](#), SBC Requirements to Support Remote MG.

SCM-007760 [Conditional: SC, SS, Remote MG] The signaling/control protocol between the SC/SS MGC and the remote MG shall be ITU-T Recommendation H.248.1, Media Gateway Control Protocol. Proprietary protocols for controlling remote MGs are not permitted. The MG VVoIP media stream protocol shall be SRTP.

SCM-007770 [Conditional: SC, SS, Remote MG] The precedence level information for each session shall be contained in the SDP part of H.248.1 messages, as specified in UC SIP 2013, Section 6, Precedence and Preemption.

SCM-007780 [Conditional: SC, SS, Remote MG] The H.248.1 protocol packets are a form of signaling packets with respect to their placement in the CE-R QoS queues. Consequently, when transiting the IP CAN/MAN/WAN the H.248.1 packets shall be marked with DSCP 40, as described in Section 6.3.2, Differentiated Services Code Point Assignments.

SCM-007790 [Conditional: SC, SS, Remote MG, SBC] The IP Sec with H.248.1 shall be used on the MGC to MGC SBC channel, the MGC SBC to remote MG SBC channel, and on the remote MG SBC to Remote MG channel to secure the MG control protocol packets as specified in Section 4.2.5, Confidentiality [Internet Key Exchange (IKE) version 1, Advanced Encryption Standard (AES) 128, Oakley Group 2048 support, etc.]. Multiple Remote MGs can be controlled by a single MGC. A single IPSec channel shall be used between the MGC and the MGC SBC to encapsulate the multiple H.248.1 control streams. The MGC SBC shall establish separate IPSec channels to each of the Remote MG SBCs, and use the H.248.1 packet header IP address information to route the H.248.1 packets (using NAT if used) to the corresponding IPSec channel to each of the remote MG SBCs. The Remote MG SBC shall unencapsulate the IPSec channel, use the control information to open and close media stream pinholes, apply NAT if used, and reencapsulate the H.248.1 packets into the IPSec channel to the MG.

2.17 SBC

SCM-007800 [Required: SBC] The SBC shall present one or more signaling IP addresses to each network side (one to the LAN [red] side and one to the network [black] side). The SBC shall also present one or more media IP addresses to each network side (one to the LAN [red] side and one to the network [black] side). In both the signaling and media cases, each individual IP address may be implemented in the SBC as either a single logical IP address or a single physical IP address.

SCM-007810 [Required: SBC] The SBC shall still meet all of the VVoIP Intrusion Detection System (IDS) monitoring requirements in this configuration (multiple signaling IP address and multiple media IP addresses on each network side). The SBC IDS monitoring requirements are in Section 4.2.3.4, Ancillary Equipment. The functionality that each VVoIP IDS/Intrusion Prevention System (IPS) shall provide is specified in Section 13.2.4, IPS Functionality, and Section 13.2.5, IPS VVoIP Signal and Media Inspection.

2.17.1 UC SIP Back-to-Back User Agent

SCM-007820 [Required: SBC] The product shall act as an UC SIP B2BUA for interpreting the UC SIP messages to meet its functions.

NOTE: The requirements of the product to secure the UC SIP messages properly are specified in Section 4, Information Assurance, and the proper processing of an UC SIP message is found in this section and UC SIP 2013.

SCM-007830 [Required: SBC] The product shall be capable of bidirectionally anchoring (NAT and NAPT) the media associated with a voice or video session that originates or terminates within its enclave.

- a. The product shall assign a locally unique combination of “c” and “m” lines when anchoring the media stream.

- b. If an INVITE request is forwarded to a product fronting an SS for which the INVITE request is not destined (i.e., the SS will forward the INVITE request downstream to another SS or SC), the product shall be capable of anchoring the media upon receipt of the INVITE request, but shall restore the original “c” and “m” lines upon receipt of the forwarded INVITE request from the SS.

NOTE: The SS will not modify the “c” and “m” lines. The reason why the anchoring occurs upon receipt of the message is that the product does not know at that point whether the session will terminate within the enclave.

- c. If a session is forwarded or transferred so the session is external to the enclave (i.e., the session no longer terminates or originates within the enclave), then the product shall restore the original received “c” and “m” lines to the forwarding/transfer message, as appropriate, to ensure that the media is no longer anchored to that product.

SCM-007840 [Required: SBC] The SBC shall be capable of processing Route headers IAW RFC 3261, Sections 20.34, 8.1.2, 16.4, and 16.12.

SCM-007850 [Required: SS] The SS will generate Route headers for the SBC to identify the next hop for the UC SIP message.

SCM-007860 [Optional: SC] The SC should generate Route headers for the SBC.

SCM-007870 [Required: SBC] The product shall preserve/pass the CCA-ID field in the Contact header.

SCM-007880 [Required: SBC] The product shall always decrement the Max-Forward header.

SCM-007890 [Required: SBC] The product shall modify the Contact header to reflect its IP address to ensure it is in the return routing path.

SCM-007900 [Required: SBC] The product fronting an SC shall be capable of maintaining a persistent TLS session between the SBC fronting the primary SS and the SBC fronting the secondary SS. Persistent means the TLS session is established when the product joins the signaling network, and it is not established on a session-by-session basis.

- a. The SBC shall be capable of distinguishing between the primary (associated with the primary SS) and a secondary (associated with the secondary SS) TLS path for the purposes of forwarding UC SIP messages.
- b. The SBC initiates a session toward its fronted SC/SS (arriving from the WAN) when receiving an incoming INVITE UC SIP message from the WAN.

2.17.2 Call Processing Load

SCM-007910 [Required: SBC] The product shall be capable of handling the aggregated WAN call processing load associated with its SCs and SSs.

NOTE: For instance, if the B/P/C/S has three SCs within the B/P/C/S and each SC is expected to handle 50 WAN calls per minute, then the SBC shall handle 150 calls per minute.

2.17.3 Network Management

SCM-007920 [Required: SBC] The product shall support FCAPS Network Management functions as defined in [Section 2.19](#), Management of Network Appliances, of this document.

2.17.4 DSCP Policing

Every ASLAN, whether Fixed (Strategic) or Deployable (Tactical), has an associated SBC. All outgoing VVoIP media packets within the ASLAN that are marked for Assured Services and destined for points outside the ASLAN must be delivered to this SBC. All incoming VVoIP media packets on the WAN Access Circuit serving the ASLAN that are marked for Assured Services and destined for points within the ASLAN must be delivered to the SBC.

SCM-007930 [Required: SBC] The SBC shall be capable of ensuring that media streams associated with a particular session use the appropriate DSCP based on the information in the UC SIP RPH.

Packets that are not marked with the appropriate DSCP shall be dropped.

The SBC shall perform this policing for media packets received from the ASLAN that are destined for points outside of the ASLAN, and for media packets received from the WAN that are destined for points within the ASLAN.

NOTE: This requires that the product maintain a table of the appropriate DSCP for an RPH marking. The mapping between precedence and DSCP is found in Section 6, Network Infrastructure End-to-End Performance.

2.17.5 Codec Bandwidth Policing

SCM-007940 [Required: SBC] The SBC shall be capable of ensuring that the media streams associated with a particular session use the appropriate codec (bandwidth) based on the SDP information in the UC SIP message. The SBC is allowed to drop any session with an associated media stream that exceeds the negotiated bandwidth, or it may perform traffic shaping.

2.17.6 Availability

There are two types of SBCs: High Availability and Medium Availability. High Availability SBCs support No Loss of Active Sessions and are recommended for locations that serve F/FO users, I/P users, and R users with PRIORITY and above precedence service. It is also noted that Medium Availability SBCs provide a cost-effective solution for locations that serve R users.

SCM-007950 [Required: High Availability SBC] The product shall have an availability of 99.999 percent (non-availability of no more than 5 minutes per year). The product shall meet the requirements specified in [Section 2.8.2](#), Product Quality Factors, of this document.

SCM-007960 [Required: Medium Availability SBC] The product shall have an availability of 99.99 percent. The product shall meet the requirements specified in [Section 2.8.2.1](#), Product Availability, except for Item i, No Loss of Active Sessions.

NOTE: The vendor will provide a reliability model for the product showing all calculations for how the availability was met.

2.17.7 IEEE 802.1Q Support

SCM-007970 [Required: SBC] The product shall be capable of supporting the IEEE 802.1Q 2-byte TCI Field 12-bit Virtual Local Area Network Identification (VID).

NOTE: The VID field has 12 bits and allows the identification of 4096 (2¹²) VLANs. Of the 4096 possible VIDs, a VID value of 0 and 4095 (Hexadecimal FFF) are reserved, so the maximum possible VIDs are 4094. The component shall be capable of distinctly tagging each media (i.e., voice, video, data, signaling, and NM) with any of the 4094 VIDs.

2.17.8 Packet Transit Time

SCM-007980 [Required: SBC] The product shall be capable of receiving, processing, and transmitting an UC packet within 2 ms to include executing all internal functions.

NOTE: Internal functions do not include Domain Name Service (DNS) lookups and other external actions or processes.

2.17.9 H.323 Support

SCM-007990 [Conditional: SBC] If the SBC supports H.323 video, then the product shall be capable of processing and forwarding H.323 messages IAW Section 4, Information Assurance.

2.17.10 SBC Requirements to Support Remote MG

SCM-008000 [Conditional: SBC] If an MG is geographically separated from the MGC that controls it, then the media stream encapsulated in SRTP, and the H.248.1 control packets encapsulated with IPsec shall pass through an SBC deployed as part of the Remote MG SUT. Within the IPsec channel, the H.248.1 protocol uses well-known UDP ports: MG port 2727 and MGC port 2427. The MG SBC shall act as an Application Layer Gateway on H.248.1 sessions, in the same manner as it acts as a B2BUA on UC SIP sessions, to open and close pinholes for authorized and authenticated bearer sessions.

2.17.11 SBC Support for Multiple SCs

SCM-008010 [Optional: SBC] The product shall support more than one SC.

NOTE: A physical SBC may house two or more logical SBCs supporting two or more SCs. Each logical SBC is a software based partition of the single physical SBC asset. Each logical SBC will have its own IP address. Virtual machine middleware may be employed for the partitioning of the physical SBC into two or more logical SBCs.

2.18 WORLDWIDE NUMBERING AND DIALING PLAN

SCM-008020 [Required: SC, SS; Conditional: PEI, UEI] The precedence level and dialed number input to the PEI or UEI shall be as specified in the following paragraphs. [**Conditional: PEI, UEI**], when used below, means that PEIs and UEIs may support a different method (e.g., a softkey) for indicating that a call is Routine or Precedence, and are not required to use 94 dialing or 9P dialing (P = 0, 1, 2, or 3) to indicate this.

In the following text, “intra-SC” means both “within the same SC” and “between an SC and an EO/PBX on the same B/P/C/S.” In the following text, “inter-SC” means both “from one SC on one B/P/C/S to another SC on another B/P/C/S” and “from one SC on one B/P/C/S to an EO/PBX on another B/P/C/S.”

These definitions are for Fixed cases. For Deployed cases, the term “enclave” replaces the term “B/P/C/S.”

SCM-008030 [Required: PEI, UEI, SC, SS] Seven-digit intra-SC dialing options as well as 7- and 10-digit inter-SC dialing shall be supported by UC EIs and signaling appliances.

SCM-008040 [Required: PEI, UEI, SC, SS] Seven-digit dialing shall consist of using the seven digits of the SC code and line number to establish either inter-SC or intra-SC calls within the same numbering plan area. Number assignments for this plan shall be of the form KXX-XXXX, where X is any digit 0–9 and K is any digit 2–8. The specific KXX of each SC will be assigned by DISA to preclude conflicts with other SC codes. Access to the local attendant shall be obtained by dialing zero. The UC ROUTINE precedence 7-digit inter-SC or intra-SC calls are initiated by dialing the appropriate sequence of (1X) KXX-XXXX or [**Conditional: PEI, UEI**] 94 (1X) KXX-XXXX. [**Conditional: PEI, UEI**] The UC calls above the ROUTINE precedence are initiated by the appropriate sequence of 9P (1X) KXX-XXXX, where P is the precedence digit (0, 1, 2, or 3). Access to other Government and/or commercial services is obtained by dialing 9 followed by the appropriate service digit(s).

SCM-008050 [Required: PEI, UEI, SC, SS] Ten-digit dialing shall consist of using ten digits comprising the area code, SC code, and line number to establish inter-SC calls where the number plan area of the calling party is different from the number plan area of the called party.

Number assignments for this plan shall be of the form KXX-KXX-XXXX, where K is any digit 2–8, and X is any digit 0–9. The ROUTINE precedence 10-digit interswitch calls are initiated by

dialing the appropriate sequence of (1X) KXX-KXX-XXXX or [**Conditional: PEI, UEI**] 94 (1X) KXX-KXX-XXXX. [**Conditional: PEI, UEI**] The calls above the ROUTINE precedence are initiated by the appropriate sequence of 9P (1X) KXX- KXX-XXXX, where P is the precedence digit (0, 1, 2, 3 or 4). Access to other Government and/or commercial services is obtained by dialing 9 followed by the appropriate service digit(s).

2.18.1 DSN Worldwide Numbering and Dialing Plan

SCM-008060 [**Required: SC, SS**] The DSN Worldwide Numbering and Dialing Plan will be used as the addressing schema within the current DSN and its migration into the SIP environment. The highlights of the DSN Worldwide Numbering and Dialing Plan are summarized in the following paragraphs. The SC shall operate with the dialing format illustrated in [Table 2.18-1](#), DSN User Dialing Format. The digits shown in parentheses may not be dialed by the DSN user on all calls.

Table 2.18-1. DSN User Dialing Format

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

[Table 2.18-2](#), Mapping of DSN tel Numbers to SIP URIs, provides examples of DSN numbers using SIP URIs that use the syntax defined in RFC 3966 and referenced in RFC 3261, Section 19.1.6.

Table 2.18-2. Mapping of DSN tel Numbers to SIP URIs

ALIAS TYPE	SIP URI
7-digit intradomain (SC enclave) call	sip:4305335;phone-context=uc.mil@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

SCM-008070 [**Required: SC, SS**] The CCA shall allow session requests from SC, SS EIs, other appliances, and SS MGs to contain the following:

- a. Called addresses including DSN numbers from the DSN numbering plan.
- b. Called addresses including E.164 numbers from the E.164 numbering plan.

NOTE: The SC and SS may require the use of a DSN escape code, such as “98” or “8,” as a prefix to a DSN number from the DSN numbering plan.

NOTE: The SC and SS may require the use of a PSTN escape code, such as “99” or “9,” as a prefix to an E.164 number from the E.164 numbering plan.

SCM-008080 [Required: SC, SS] When a session request’s called address includes a DSN number from the DSN numbering plan, the CCA shall determine whether the called DSN number is local to the SC or SS, or external to the SC or SS.

If the called DSN number is local to the SC or SS, the CCA shall complete the session request within the SC or SS.

If the called DSN number is external to the SC or SS, the CCA shall route the session request outside of the SC or SS, using one of the following:

- The external IP address of the next appliance (i.e., SC or SS) that should handle the session request.
- The local IP address of the SC or SS MG and MG trunk group that should handle the session request.

SCM-008090 [Required: SC, SS] When a session request’s called address includes an E.164 number from the E.164 numbering plan, the CCA shall determine whether the called E.164 number is local to the SC or SS, or external to the SC or SS.

If the called E.164 number is local to the SC or SS, the CCA shall complete the session request within the SC or SS.

If the called E.164 number is external to the SC or SS, the CCA shall route the session request outside of the SC or SS, using one of the following:

- The external IP address of the next signaling appliance that should handle the session request.
- The local IP address of the SC or SS MG and MG trunk group that should handle the session request.

Access Code

SCM-008100 [Required: SC, SS] The access code shall include the access digit, followed by the precedence digit or the service digit.

Access Digit

SCM-008110 [Required: SC, SS] The access digit (e.g., 9) shall provide the indication to the SC/SS that the following digits will indicate either UC call precedence, selected egress to the services of other systems or networks, or selected access to special UC features, such as individual trunk tests.

Precedence Digit

SCM-008120 [Required: SC, SS] The precedence digit (0, 1, 2, 3, or 4) shall permit a UC user to dial an authorized UC precedence level from properly classmarked 12-button telephone instruments. When the 7-digit intraSC dialing option is used, it is not necessary to dial or key the precedence access digit for ROUTINE precedence calls. The assignment of precedence digits is shown in [Table 2.18-3](#), Precedence and Service Access.

Table 2.18-3. Precedence and Service Access

ASSIGNMENTS FOR TELEPHONE KEYSETS		
Access Digit	Precedence Digit	Precedence
e.g., 9	0	UC FLASH OVERRIDE
e.g., 9	1	UC FLASH
e.g., 9	2	UC IMMEDIATE
e.g., 9	3	UC PRIORITY
e.g., 9	4	UC ROUTINE
ASSIGNMENTS FOR SERVICE ACCESS CODES		
Access Digit	Service Digit	Precedence
e.g., 9	5	Off-Net 700 Services
e.g., 9	6	Not Assigned
e.g., 9	7	DSN CONUS FTS
e.g., 9	8	Not Assigned
e.g., 9	9	Local PTN

SCM-008130 [Required: SC, SS] The service digits, 5 through 9, shall provide information to the SC/SS to connect calls to Government or public telephone services or networks that are not part of the UC. The UC SC/SS will collect the access code and all routing and address digits before attempting to route a call to prevent numbering ambiguities between the access codes and the 2-digit abbreviated dial codes. The assignment of service access codes is shown in [Table 2.18-3](#), Precedence and Service Access.

2.18.1.1 CCA and SSLs Support for Dual Assignment of DSN and E.164 Numbers to SS EIs

SCM-008140 [Required: SC, SS] The CCA shall allow each VoIP and Video PEI and UEI served by an SC or SS to have both a DSN number assigned and an E.164 number assigned.

SCM-008150 [Required: SC, SS] For VoIP and Video PEIs or UEIs that have both a DSN number and an E.164 number assigned, the CCA shall be able to match each PEI's or UEI's

DSN number with its E.164 number, and to match each PEI's or UEI's E.164 number with its DSN number.

2.18.1.2 CCA Differentiation Between DSN Numbers and E.164 Numbers

SCM-008160 [Required: SC, SS] The CCA shall be able to distinguish DSN called numbers from E.164 called numbers when processing VoIP and Video session requests from PEIs, UEIs, SBCs, MG line cards, and MG trunk groups.

SCM-008170 [Required: SC, SS] The CCA shall be able to distinguish local DSN called numbers from external DSN called numbers when processing VoIP and Video session requests from PEIs, UEIs, SBCs, MG line cards, and MG trunk groups.

SCM-008180 [Required: SC, SS] The CCA shall be able to distinguish local E.164 called numbers from external E.164 called numbers when processing VoIP and Video session requests from PEIs, UEIs, SBCs, MG line cards, and MG trunk groups.

SCM-008190 [Optional: SC, SS] On SIP and UC SIP calls from PEIs or UEIs and the SBC, the CCA (and its SCLS and SSLs Servers) shall use the contents of the phone-context parameter in the called SIP URI to determine the following:

- a. Whether the session request is intended for a DSN number or an E.164 number.
- b. In the E.164 case, whether the E.164 number is locally significant, nationally significant, or internationally significant.

SCM-008200 [Required: SC, SS] On ISDN PRI calls from an MG, the CCA shall use the contents of the Type of Number and Numbering Plan Identification fields in the ISDN Called Party Number IE in the SETUP message to determine the following:

- a. Whether the call request is intended for a DSN number or an E.164 number.
- b. In the E.164 case, whether the E.164 number is locally significant, nationally significant, or internationally significant.

SCM-008210 [Conditional: SC, SS] If CAS trunks and trunk signaling are supported, then the CCA shall use the identity of the trunk group that the call was received on (and the presence or absence of prefix digits in the received Called Party Number) to determine the following for CAS trunk calls from an MG:

- a. Whether the call request is intended for a DSN number or an E.164 number.
- b. In the E.164 case, whether the E.164 number is locally significant, nationally significant, or internationally significant.

2.18.1.3 CCA Use of SIP “phone-context” to Differentiate Between DSN and E.164 Numbers

SCM-008220 [Optional: SC, SS] On SIP and UC SIP calls from PEIs or UEIs and other appliances, the CCA shall use the contents of the “phone-context” parameter in the called SIP URI to distinguish DSN numbers from E.164 numbers as follows:

- a. If the “phone-context” parameter in the “User” portion of the called SIP URI indicates “uc.mil” (or a subordinate domain name built on “uc.mil”), then the CCA shall treat the 10-digit number that precedes the “phone-context” parameter as a DSN number.
- b. If the “phone-context” parameter in the “User” portion of the called SIP URI indicates a sequence of digits, possibly prefixed with a “+” character, then the CCA shall treat the variable length number that precedes the “phone-context” parameter as an E.164 number.

SCM-008230 [Optional: SC, SS] On SIP and UC SIP calls from SS PEIs or UEIs and other appliances, the CCA shall use the contents of the “phone-context” parameter in the called SIP URI to distinguish local, national, and international E.164 numbers from one another as follows:

- a. If there is no “phone-context” parameter in the “User” portion of the called SIP URI, then the CCA shall treat the variable length number in the “User” portion of this URI as an international E.164 number.
- b. If the “phone-context” parameter in the “User” portion of the called SIP URI contains a “+” character followed by an E.164 country code, but no area code or city code, then the CCA shall treat the variable length number that precedes the “phone-context” parameter as a national E.164 number (for the country identified by the country code).
- c. If the “phone-context” parameter in the “User” portion of the called SIP URI contains a “+” character followed by an E.164 country code and an area code or city code, then the CCA shall treat the variable length number that precedes the “phone-context” parameter as a local E.164 number (for the country identified by the country code, and the area or city identified by the area code or city code).

2.18.1.4 Use of SIP URI Domain Name With DSN Numbers and E.164 Numbers

The SIP URIs used for VVoIP calls contain both a username (with a numeric Called Party Number and an optional “phone-context” parameter) and a domain name, such as “patch.eur.uc.mil” or “ysm.pac.uc.mil.” Signaling appliances need some mechanism to accept, reject, or overwrite the domain name values received as part of Called SIP URIs in each VoIP and Video session request.

NOTE: Support for IETF Domain Names implies that UC also supports IETF DNS, which uses domain name servers and allows Domain Names to be resolved to IP addresses (and vice versa). The UC support for DNS is optional.

SCM-008240 [Optional: SC, SS] Each signaling appliance may support a configurable per-appliance parameter that indicates how the appliance handles domain names received in VoIP and Video session requests.

This parameter, named “Domain Name Treatment for Session Requests,” shall support the following values:

- Overwrite with Network Domain Name.
- Overwrite with Appliance FQDN.
- Passthrough.

The default value shall be Overwrite with Network Domain Name.

SCM-008250 [Conditional: SC, SS] If a signaling appliance supports the “Domain Name Treatment for Session Requests” parameter, then it shall meet all of the following conditional requirements:

- a. The appliance shall support all three options noted above, and shall support the default parameter value of “Overwrite with Network Domain Name.” The appliance shall allow the option selected to be software-configurable.
- b. When the value of the Domain Name Treatment for Session Requests parameter for the signaling appliance is Overwrite with Network Domain Name, the appliance CCA shall discard all domain names received in called SIP URIs in session requests, and overwrite them with the Domain Name of the DOD network that the appliance belongs to.
- c. The appliance shall support a per-appliance parameter called the “UC Network Domain Name,” to be used in overwriting the received domain names in this case. (Support for this additional parameter is not a requirement for UC Spiral 1.) The value of this parameter shall be a text string that identifies the Domain Name of the DOD network that the appliance belongs to, for domain name overwriting purposes. At a minimum, the following FQDNs for DOD networks (i.e., UC, Classified UC[CUC]) shall be supported: “uc.mil” and “cuc.mil.”
- d. When the value of the Domain Name Treatment for Session Requests parameter for the appliance is Overwrite with Appliance FQDN, the appliance CCA shall discard all domain names received in called SIP URIs in session requests, and overwrite them with the FQDN of the appliance.
- e. The appliance shall support a per-appliance parameter called the “Appliance FQDN,” to be used in overwriting the received domain names in this case. The value of this parameter shall be a text string that identifies the FQDN of the appliance, for domain name overwriting purposes. Examples of possible FQDNs for appliances (i.e., SCs, SSs) are as follows:
 - (1) “sc10.ss20.patch.germany.eur.uc.mil” (i.e., SC 10, subordinate to SS 20, located at the Patch Barracks in Germany in the European Theater on the UC network).

- (2) “sc20.sc30.ss40.ysm.korea.pac.uc.mil” (i.e., SC 20, subordinate to SC 30, subordinate to SS 40, located at Yongsan Main in South Korea in the Pacific Theater on the UC network).
 - (3) “ss50.scott.cent.conus.uc.mil” (i.e., SS 50, located at Scott Air Force Base in Central CONUS on the UC network).
- f. When the value of the Domain Name Treatment for Session Requests parameter for the appliance is “Passthrough,” the appliance CCA shall transparently passthrough all domain names received in called SIP URIs in session requests, without altering them.

2.18.1.4.1 SIP URI Domain Names in UC Spiral 1

SCM-008260 [Required: SC, SS] The SS or SC is only required to support one network FQDN for use with SIP URI domain names: “uc.mil” if that appliance is used for Sensitive but Unclassified (SBU) traffic, and “cuc.mil” if that appliance is used for classified traffic.

SCM-008270 [Required: SC, SS] The SS or SC is required to ensure that all UC SIP session requests entering or leaving that appliance use the network FQDN of that appliance (i.e., “uc.mil” for SBU traffic, or “cuc.mil” for Classified traffic) as the domain name in called SIP URIs.

In cases where a received called SIP URI in a received UC SIP message has a domain name other than “uc.mil” (for SBU traffic) or “cuc.mil” (for Classified traffic), the SS or SC shall do either of the following:

- Reject the UC SIP session request that contained the unexpected domain name.
- Accept the UC SIP session request that contained the unexpected domain name, but overwrite the received domain name with “uc.mil” (for SBU traffic) or “cuc.mil” (for Classified traffic).

Future versions of the UCR document will give additional detail on requirements for the support of SIP URI domain names that are different from “uc.mil” and “cuc.mil.”

2.18.1.5 Domain Directory

SCM-008280 [Required: SC, SS] SC and SS shall maintain subscriber assignment information in the form of a domain directory. A domain directory shall support the following functions:

- a. A Directory Look-Up function that shall allow a user assigned to an SC to look up the telephone numbers of other users assigned to (i.e., served by) that common SC. This function is referred to as “white pages” services, and it should not be confused with call routing tables used for forwarding SIP call requests.
- b. For security reasons, the Directory Look-Up function shall only be available from a user’s IP telephone instrument, not via the Internet. The IP telephone instrument will contain a small display and function keys that facilitate the Directory Look-Up function.

- c. Access to the Directory Look-Up function shall be controlled by assigned attributes. There may be specific reasons for denying this privilege to certain users.
- d. The SC shall allow the system administrator to update the directory database in response to service order activity (i.e., subscriber adds, moves, changes, or removals). The SC shall update the white pages data automatically as well as subscriber line information contained as part of the Directory Look-Up function.
- e. **[Optional: SC, SS]** When automatic instrument registration is supported, a service order “flag” shall be sent to the system administrator terminal so the administrator can update the subscriber’s location information as necessary.
- f. The data elements shown in [Table 2.18-4](#), White Pages Directory Data Elements, shall be incorporated as part of the white pages directory portion of the SC subscriber database.

Table 2.18-4. White Pages Directory Data Elements

DATA ITEM	EXAMPLE
USER 10-DIGIT DSN TELEPHONE NUMBER	315-454-1192
USER ORGANIZATION CODE	SCX
ORGANIZATION NAME	1st Comm Squadron
USER GEOGRAPHIC LOCATION	Langley AFB
USER NAME	Civ Bill Smith

- g. **[Optional: SC, SS]** The SC may support a periodic update of a “global directory” database via an automated electronic transfer of directory data. Any such transfer will be under the control of a system administrator responsible for the global directory.
- h. The user shall be offered the following ways of searching for local (domain) directory information:
 - (1) User access to the local domain directory is provided by a “directory” feature available on the VoIP instrument. Directory search will be limited to information contained within the SC subscriber information.
 - (2) The basic search shall be made based on Last Name, First Name.
 - (3) **[Optional: SC, SS]** The search utility may allow users to specify Boolean expressions for search criteria, such as using OR with multiple entries in a single field, or using AND across multiple fields to identify the desired directory entries.

2.19 MANAGEMENT OF NETWORK APPLIANCES

2.19.1 General Management

SCM-008290 [Required: SC, SS, SBC] There shall be a local craftsperson interface [Craft Input Terminal (CIT)] for OAM&P for all VVoIP appliances. The CIT is a supplier-provided

input/output device that is locally connected to a network component. The CIT may be connected to the local EMS, which is in turn connected to the VVoIP appliance using the local EMS Ethernet management interface. The CIT may be connected directly to the VVoIP appliance also, using the Ethernet management interface on the component that would otherwise be used by the local EMS (when there is no local EMS). The CIT may be connected directly to the VVoIP appliance using a separate serial interface.

SCM-008300 [Required: SC, SS, SBC] Communications between VVoIP EMS and the VVoIP appliances shall be via IP.

Where an EMS is the interface with a VVoIP component, the TCP/IP-based communications between the VVoIP EMS and the local EMS shall be via the following:

- a. **[Required: SC, SS and SBC Local EMS]** Extensible Markup Language (XML).

SCM-008310 [Required: SC, SS, SBC] A network appliance shall issue state change notifications for changes in the states of replaceable components, including changes in operational state or service status, and detection of new components.

SCM-008320 [Required: SC, SS, SBC] A network appliance shall be provisioned by the VVoIP EMS with the address and Transport Layer port information associated with its Core Network interfaces.

SCM-008330 [Required: SC, SS, SBC] A network appliance shall be capable of maintaining and responding to VVoIP EMS requests for resource inventory, configuration, and status information concerning Core Network interface resources (e.g., IP or MAC addresses) that have been installed and placed into service.

SCM-008340 [Required: SC, SS, SBC] A network appliance shall be capable of setting the Administrative state and maintaining the Operational state of each Core Network interface, and maintaining the time of the last state change.

SCM-008350 [Required: SC, SS, SBC] A network appliance shall generate an alarm condition upon the occurrence of any of the following failure conditions, as defined in ITU-T Recommendation M.3100:

- a. Power loss.
- b. Environmental condition not conducive to normal operation.
- c. Loss of data integrity.

SCM-008360 [Required: SC, SS, SBC] A network appliance shall generate an alarm condition when the number of received packets that fail encoding integrity checks exceeds a configurable threshold.

SCM-008370 [Required: SC, SS, SBC] A network appliance shall generate an alarm condition when the number of received packets that fail decryption exceeds a configurable threshold.

SCM-008380 [Required: SC, SS, SBC] A network appliance shall be capable of maintaining and responding to requests for physical resource capacity information for installed components. This information includes the following:

- a. Component type and model.
- b. Shelf location.
- c. Rack location.
- d. Bay location.

2.19.2 Requirements for FCAPS Management

General requirements for the five management functional areas are defined in the following sections.

2.19.2.1 Fault Management

SCM-008390 [Required: SC, SS, SBC] Faults shall be reported IAW IETF RFC 1215.

2.19.2.1.1 Alarm Messages

SCM-008400 [Required: SC, SS, SBC] Alarm messages shall be distinguishable from administrative log messages.

2.19.2.1.2 Self-Detection of Fault Conditions

SCM-008410 [Required: SC, SS, SBC] The appliances shall detect their own fault (alarm) conditions.

2.19.2.1.3 Alarm Notifications

SCM-008420 [Required: SC, SS, SBC] The NEs shall generate alarm notifications.

2.19.2.1.4 Near-Real-Time Alarm Messages

SCM-008430 [Required: SC, SS, SBC] The network elements shall send the alarm messages in near-real time (NRT). More than 99.95 percent of alarms shall be detected and reported in NRT. NRT is defined as event detection and alarm reporting within 5 seconds of the event, excluding transport time.

2.19.2.1.5 SNMP Version 3 Format Alarm Messages

SCM-008440 [Required: NM] The network components shall send alarm messages in Simple Network Management Protocol (SNMP) version 3 (SNMPv3) format.

2.19.2.2 Configuration Management

SCM-008450 [Optional: SC, SS, SBC] All Configuration Management (CM) information may be presented IAW RFCs 1213 and 3418.

2.19.2.2.1 Read-Write Access to CM Data by the VVoIP EMS

SCM-008460 [Required: SC, SS, SBC] Capability to access and modify configuration data by the VVoIP EMS shall be controllable by using an access privileges function within the network appliance.

2.19.2.3 Accounting Management

Requirements for Accounting Management are found in [Section 2.20](#), Accounting Management.

2.19.2.4 Performance Management

SCM-008470 [Optional: SC, SS, SBC] Performance Management (PM) information may be presented IAW RFCs 1213 and 3418.

2.19.2.4.1 Near-Real-Time Network Performance Monitoring

Near-real-time network performance monitoring is a subset of PM. The VVoIP EMS collects alarm messages in real time and selected performance data from the appliances on a NRT basis in 5- or 15-minute intervals. Network control personnel evaluate the alarm and performance data and, to minimize the effect on network traffic caused by a network anomaly, the control personnel implement traffic flow (NM) controls. The appliances must be capable of receiving and responding to NM controls from the VVoIP EMS.

2.19.2.4.2 Remote Network Management Commands

2.19.2.4.2.1 Automatic Congestion Controls

SCM-008480 [Required: SC, SS] When ASAC budgets are reduced, by NM action, below the current budget allocation, any previous sessions (regardless of precedence level) in excess of the new budget shall be one of the following:

- a. Allowed to terminate naturally.
- b. Deterministically preempted starting with those of lowest precedence until the number of sessions in progress equals the new budget allocation.

2.19.2.4.2.2 Destination Code Controls

Destination Code Control (DCC) is applied to reduce calls to a specific area or location that has been temporarily designated as “difficult to reach” due to circumstances.

SCM-008490 [Required: SC, SS] The SC and SS shall support DCC implemented based on specifying:

- a. An entire Numbering Plan Area (NPA).
- b. A group of specific NNX codes within an NPA. (The following is an example of when this control becomes necessary: when a large military base having multiple NNX codes becomes isolated.)
- c. A single NNX.
- d. An NNX-D (hundred group within an NNX. Reason: There are locations within CONUS that share an NNX.)

SCM-008500 [Optional: SC, SS] The SC and SS shall have the capability of setting the percentage of calls to be blocked to the designated destination(s).

SCM-008510 [Required: SC, SS] FLASH and FLASH OVERRIDE calls shall not be affected by DCC.

SCM-008520 [Required: SC, SS] The SC and SS shall play the "No Circuit Available" (NCA) announcement back towards the calling party on call attempts where the calling party is on the UC IP network, and DCC causes call blocking. The content of the NCA announcement shall be as follows: "Network service disruption has prevented the completion of your call. Please hang-up and try your call later. In case of emergency, please contact your Attendant or Operator."

SCM-008530 [Required: SC, SS] On SC or SS calls where the calling party is on the DISA TDM network, and the SC or SS MG is located in the session path between the IP called party and the TDM calling party, the MG shall return the Q.850 Cause Code Number 27, Destination out of order, in the DCC call rejection message sent towards the calling party on the T1.619A PRI between the MG and the DISA TDM network.

This cause code indicates that the destination indicated by the calling user cannot be reached because the interface to the destination is not functioning correctly.

2.19.2.4.2.3 Total Office Manual Control Removal

The ability to remove all controls that were put in place is equally applicable to TDM- and IP-based voice systems.

2.19.2.4.2.4 Call Budget Control

SCM-008540 [Required: SS] The SS shall be able to set ASAC call budgets for each SC under its control.

SCM-008550 [Required: SS] The SS shall be able to set ASAC call budgets for a SC while there are active calls to/from that SC.

SCM-008560 [Conditional: SC, SS] If directionalization is supported, then the SS and SC shall be able to swap between directionalization and no directionalization on a UC SIP trunk group while there are active calls on the trunk group.

SCM-008570 [Required: SC] The SC shall be able to set ASAC call budgets for the PEI/UEIs under its control.

SCM-008580 [Required: SC] The SC shall be able to set ASAC call budgets for the PEI/UEIs while there are active calls to/from the SC.

SCM-008590 [Required: SC, SS] ASAC shall maintain the separate counts for voice and video, in 5-minute intervals. SS ASAC shall provide these counts for each of the SCs under its control and the SC shall provide these counts for the PEIs/UEIs that it controls.

The SS WAN-level ASAC and the SC-level ASAC session budgets and counts are as follows:

a. VoIP Session Budgets:

- (1) IPB. The total budget of VoIP sessions plus session attempts in the session setup phase that are allowed on the IP access link.
- (2) [Optional] IPBo. The budget for outbound VoIP sessions plus session attempts in the session setup phase that are allowed on the IP access link.
- (3) [Optional] IPBi. The budget for inbound VoIP sessions plus session attempts in the session setup phase that are allowed on the IP access link.

b. TDM Session Budget:

- (1) TDMB. The overall number of TDM sessions plus sessions in the session setup phase on the TDM link. This equals the number of DS0s on the trunk between the SC MG and the EO/SMEO/PBX1/PBX2.

c. VSU Budgets:

- (1) VDB. The total number of inbound and outbound VSUs plus the in-progress VSUs connection attempts that an SC is allowed to have over the IP access link.
- (2) [Optional] VDBi. The total number of inbound VSUs plus the in-progress inbound VSUs connection attempts that an SC is allowed to have over the IP access link.
- (3) [Optional] VDBo. The total number of outbound VSUs plus the in-progress outbound VSUs connection attempts that an SC is allowed to have over the IP access link.

d. VoIP Session Counts:

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

- (2) [Optional] IPCo. The number of outbound IP sessions in progress plus the number of outbound session attempts in the session setup phase.
- (3) [Optional] IPCi. The number of inbound IP sessions in progress plus the number of inbound session attempts in the session setup phase.
- e. TDM Session Counts:
 - (1) TDMC. The total number of sessions in progress between the TDM switch and the MG plus the total number of session attempts in the session setup phase.
- f. VSU Counts:
 - (1) VBC. The total number of interbase VSU sessions in progress plus the number of session attempts in the session setup phase.
 - (2) [Optional] VBCo. The number of outbound VSU sessions in progress plus the number of outbound session attempts in the session setup phase.
 - (3) [Optional] VBCi. The number of inbound VSU sessions in progress plus the number of inbound session attempts in the session setup phase.

2.19.2.4.2.5 PEI/UEI Origination Capability Control

Setting the PEI and UEI origination capability involves setting the parameters for the precedence and destinations of a call that may be originated from a PEI or UEI.

SCM-008600 [Required: SC] The product shall have the capability of setting a PEI/UEI's maximum allowed precedence level for originating a call. This is a "subscriber class mark feature," which is controlled by the SC system administrator.

SCM-008610 [Required: SC] The product shall have the capability of controlling the destination(s) that a PEI or UEI is restricted from calling. This is a subscriber class mark feature that is controlled by the SC system administrator. This action or function can be performed by:

- a. [Required] Setting the destinations to which calls are to be blocked by:
 - (1) [Required] NPA/NNX.
 - (2) [Optional] Blocked by a specific 7-digit directory number (NPA-NNX Dxxx).

2.19.2.5 Security Management

SCM-008620 [Required: SC, SS, SBC] All network management interactions shall meet the access control, confidentiality, integrity, availability, and non-repudiation requirements in Section 4, Information Assurance.

2.20 ACCOUNTING MANAGEMENT

SCM-008630 [Required: SC, SS] Call Detail Records (CDRs) shall be created and maintained for each session processed and shall include the following items:

- a. Host Name of the CCA controlling the call processing.
- b. Start Date of call (In Julian or Calendar).
- c. Start Time of Call (Hour + Minute + Second).
- d. Elapsed Time of Call and/or Stop Time of call.
- e. Calling Number.
- f. Called Number (included all dialed digits).
- g. **[Optional]** Call Answered/Unanswered Indicator.
- h. Precedence level of call.

(NOTE: This may be accomplished either by a specific precedence level designation field in the call, or by providing the dialed precedence level access digits in the called number field.)

- i. **[Optional]** Indication of either a VoIP or Video over IP call.
- j. **[Optional]** Indication of the assigned bandwidth for Video over IP call.
- k. **[Optional]** Conference Call Indicator.
- l. **[Optional]** Customer/Business Group Identification.

The following subsections describe the types of VoIP calls (e.g., PSTN to IP, IP to PSTN), and provide additional call information that shall be captured in the CDR.

2.20.1 VoIP to PSTN

The term VoIP to PSTN calls refer to calls routed to the PSTN from a VoIP network.

SCM-008640 [Required: SC, SS] In addition to the call data specified previously, the following call data shall be provided in the CDR for calls that are routed to the PSTN from the VoIP network:

- a. IP address of originating subscriber (if the call originated from the subscriber on the VoIP network).
- b. IP address of the gateway connecting to the PSTN.
- c. Outgoing trunk group of the call.
- d. Outgoing trunk group member of the call.

2.20.2 PSTN to VoIP

PSTN to VoIP refers to the type of call where the call that originates in the PSTN network enters the VoIP network for completion.

SCM-008650 [Required: SC, SS] In addition to the call data specified previously, the following call data shall be provided in the CDR for calls that are routed from the PSTN to the VoIP network:

- a. IP address of terminating subscriber (if the call terminates to a subscriber on the VoIP network).
- b. IP address of the gateway connecting to the PSTN.
- c. Incoming trunk group of the call.
- d. Incoming trunk group member of the call.

2.20.3 VoIP to VoIP

A VoIP to VoIP call can be one of the following three basic scenarios:

1. Subscriber in the UC VoIP network originates a call and the call terminates in the UC VoIP network.
2. Subscriber in the UC VoIP network originates a call to the call terminates in another VoIP network.
3. Call from another VoIP network terminates a call to a UC VoIP subscriber.

SCM-008660 [Required: SC, SS] In addition to the call data specified previously, the following call data shall be provided in the CDR (that captures both the originating and terminating information) for calls that originate and terminate within the UC VoIP network:

- a. IP address of originating subscriber.
- b. IP address of terminating subscriber.

SCM-008670 [Required: SC, SS] In addition to the call data specified previously, the following call data shall be provided in the CDR for calls that originate from the UC VoIP network and terminate to another VoIP network:

- a. IP address of originating subscriber.
- b. IP address of the gateway connecting to the other VoIP network (if applicable).

SCM-008680 [Required: SC, SS] In addition to the call data specified previously, the following call data shall be provided in the CDR for calls that originate in another VoIP network and terminate in the UC VoIP network:

- a. IP address of terminating subscriber.

- b. IP address of the gateway connecting to the other VoIP network (if applicable).

2.20.4 Quality of Service

The “product” for the following requirements is the combination of the Enterprise SC and the set of PEIs and UEIs that it serves.

NOTE: The requirement to provide a voice quality record is optional for SCs in other than the Enterprise Services application.

SCM-008690 [Required: ESC, PEI, UEI] The product shall provide a voice quality record at the completion of each voice session. The voice quality record shall be included in the CDR that the ESC generates for that session, and shall conform to the E-Model, as described in TIA TSB-116-A and ITU-T Recommendation G.107. The voice quality record shall contain the calculated R-Factor for the voice session per TIA TSB-116-A. The allowable error for the voice quality calculations shall be ± 3 IAW TIA TSB-116-A.

NOTE: This requirement is only related to VoIP EIs and is not applicable to MGs.

SCM-008700 [Required: ESC, PEI, UEI] As part of the voice quality record, the product shall provide the raw voice session statistics that are used to make the R-Factor calculation to include, as a minimum, the latency, packet loss, Equipment Impairment Factor (Ie), and the Weighted Terminal Coupling Loss (TCLw).

SCM-008710 [Required: ESC, PEI, UEI] As part of the voice quality record, the product shall provide the jitter for the session.

SCM-008720 [Required: ESC, UEI] For UEIs, the voice quality record shall be transmitted at the completion of a session to the CCA, in an UC SIP BYE message if the UEI ends the call, or an UC SIP 200 (OK) response to a BYE message if the ESC ends the call.

SCM-008730 [Optional: ESC, PEI, UEI] The EI may use one of the following SIP Quality of Service Statistics (QoS Stats) headers to convey the loss, latency, and jitter information in the UC SIP BYE message or the UC SIP 200 (OK) response.

- a. X-RTP-Stat.
- b. P-RTP-Stat.

Note that these QoS Stats headers do not currently include the Ie or TCLw values.

SCM-008740 [Optional: ESC] The product may generate an alarm to the VVoIP EMS when the session R-Factor calculation in the CDR fails to meet a configurable threshold. By default, the threshold shall be an R-Factor value of 80, which is equivalent to an MOS value of 4.0.

2.21 V.150.1 MODEM RELAY SECURE PHONE SUPPORT

This section identifies requirements for “V.150.1 Modem Relay Secure Phone Support,” to ensure that UC MGs can support SCIP-based secure phones for all scenarios required by the National Security Agency (NSA).

V.150.1 Secure Phone Support relies on the following:

- SCIP-216 Modem Relay capabilities in UC MGs, ATAs, and IADs.
- SCIP-215 Modem Relay capabilities in UC SEI.

2.21.1 SCIP/V.150.1 Gateway

This section contains the SCIP/V.150.1 Gateway requirements for the UCR, based on the NSA document, SCIP-216. All references to “SCIP-216” that follow are references to SCIP-216, Revision 2.1.

2.21.1.1 *Basic Minimum Essential Requirements*

The following requirements are based on the Basic Minimum Essential Requirements in SCIP-216 Section 3.

2.21.1.1.1 *IP Transport Layer Protocol*

SCM-008750 [Required: MG-TS – Optional: MG-LS, TA, IAD] The SCIP/V.150.1 Gateway shall meet all the requirements for “IP Transport Layer Protocol” in SCIP-216, Section 3.1.

SCM-008760 [Required: MG-TS – Optional: MG-LS, TA, IAD] The SCIP/V.150.1 Gateway shall support V.150.1 Simple Packet Relay Transport (SPRT) for reliable IP transport of the demodulated modem signals, per SCIP-216, Section 3.1.

2.21.1.1.2 *Operational Mode*

SCM-008770 [Required: MG-TS – Optional: MG-LS, TA, IAD] The SCIP/V.150.1 Gateway shall meet all the requirements for “V.150.1 Operational Mode” in SCIP-216, Section 3.2.

SCM-008780 [Required: MG-TS – Optional: MG-LS, TA, IAD] The SCIP/V.150.1 Gateway shall support the V.150.1 Audio and Modem Relay (MR) modes, per SCIP-216, Section 3.2.

2.21.1.1.3 *Modem Relay Gateway Type*

SCM-008790 [Required: MG-TS – Optional: MG-LS, TA, IAD] The SCIP/V.150.1 Gateway shall meet all the requirements for “Modem-Relay Gateway Type” in SCIP-216, Section 3.3.

SCM-008800 [Required: MG-TS – Optional: MG-LS, TA, IAD] The SCIP/V.150.1 Gateway shall support the V.32 and V.34 duplex modulation types in the MR mode, per SCIP-216, Section 3.3.

SCM-008810 [Required: MG-TS – Optional: MG-LS, TA, IAD] The SCIP/V.150.1 Gateway shall also support the V.90 digital and V.92 digital modulation types in the MR mode, per SCIP-216, Section 3.3 (where they are optional) and ITU-T Recommendation V.150.1, Section 9.1, where they are required.

SCM-008820 [Optional: MG-TS, MG-LS, TA, IAD] The SCIP/V.150.1 Gateway shall also support the V.90 Analog and V.92 analog modulation types in the MR mode, per SCIP-216, Section 3.3 (where they are optional) and ITU-T Recommendation V.150.1, Section 9.1 (where they are also optional).

2.21.1.1.4 Simple Packet Relay Transport

The following requirements are based on the SPRT requirements in SCIP-216, Section 3.4.

SCM-008830 [Required: MG-TS – Optional: MG-LS, TA, IAD] The SCIP/V.150.1 Gateway shall meet all the requirements for “Transport Channel” in SCIP-216, Section 3.4.1.

SCM-008840 [Required: MG-TS – Optional: MG-LS, TA, IAD] The SCIP/V.150.1 Gateway shall support SPRT Transport Channels TC0, TC2, and TC3 for the exchange of ACKs and control messages, per SCIP-216, Section 3.4.1.

SCM-008850 [Required: MG-TS – Optional: MG-LS, TA, IAD] The SCIP/V.150.1 Gateway shall support the “Suggested values for SPRT timers” for Timers TA01, TA02, and TR03, and for Transport Channel TC2, per Table B.3 in Section B.2.3.6 of ITU-T Recommendation V.150.1.

SCM-008860 [Required: MG-TS – Optional: MG-LS, TA, IAD] The SCIP/V.150.1 Gateway shall meet all the requirements for “SPRT Modem Relay Messages” in SCIP-216, Section 3.4.2.

SCM-008870 [Required: MG-TS – Optional: MG-LS, TA, IAD] In the MR mode, the SCIP/V.150.1 Gateway shall meet all the requirements for the INIT, JM-INFO, CONNECT, MR_EVENT, I_OCTET, and I_OCTET-CS MR messages, as described in Table 3-3 in SCIP-216, Section 3.4.2.

SCM-008880 [Required: MG-TS – Optional: MG-LS, TA, IAD] The SCIP/V.150.1 Gateway shall meet all the requirements for “SPRT Timers” in Section 3.4.3 of SCIP-216.

2.21.1.1.5 State Signaling Event

The following requirements are based on the “State Signaling Event (SSE)” requirements in Section 3.5 of SCIP-216.

SCM-008890 [Required: MG-TS – Optional: MG-LS, TA, IAD] The SCIP/V.150.1 Gateway shall use the SSE protocol to transition between the Audio (native state) and MR modes of operation, per Section 3.5 of SCIP-216.

SCM-008900 [Required: MG-TS – Optional: MG-LS, TA, IAD] The SCIP/V.150.1 Gateway shall meet all the requirements for “SSE Call Discrimination Messages” in Section 3.5.1 of SCIP-216.

SCM-008910 [Required: MG-TS – Optional: MG-LS, TA, IAD] The SCIP/V.150.1 Gateway shall meet all the requirements for “SSE Reliability” in Section 3.5.2 of SCIP-216.

SCM-008920 [Required: MG-TS – Optional: MG-LS, TA, IAD] The SCIP/V.150.1 Gateway shall meet all the requirements for “SSE Reason Identifier Codes” in Section 3.5.3 of SCIP-216.

SCM-008930 [Required: MG-TS – Optional: MG-LS, TA, IAD] The SCIP/V.150.1 Gateway shall meet all the requirements for “SSE Timers” in Section 3.5.4 of SCIP-216.

2.21.1.1.6 Call Setup Protocol

The following requirements are based on the “Call Setup Protocol Requirements for Negotiating Specific V.150.1 Capabilities” in Section 3.6 of SCIP-216.

SCM-008940 [Required: MG-TS – Optional: MG-LS, TA, IAD] The SCIP/V.150.1 Gateway shall meet all the requirements for “V.150.1 Version Declaration” in Section 3.6.1 of SCIP-216.

SCM-008950 [Required: MG-TS – Optional: MG-LS, TA, IAD] The SCIP/V.150.1 Gateway shall advertise a V.150.1 version number of “1” or higher, per Section 3.6.1 of SCIP-216.

SCM-008960 [Required: MG-TS – Optional: MG-LS, TA, IAD] The SCIP/V.150.1 Gateway shall meet all the requirements for “Transcompression Capability” in Section 3.6.2 of SCIP-216.

SCM-008970 [Required: MG-TS – Optional: MG-LS, TA, IAD] The SCIP/V.150.1 Gateway shall meet all the requirements for “Modem Relay Type Declaration” in Section 3.6.3 of SCIP-216.

SCM-008980 [Required: MG-TS – Optional: MG-LS, TA, IAD] The SCIP/V.150.1 Gateway shall meet all the requirements for “Modulation Support Indication” in Section 3.6.4 of SCIP-216.

SCM-008990 [Required: MG-TS; Optional: MG-LS, TA, IAD] The SCIP/V.150.1 Gateway shall meet all the requirements for “RFC 2833 Events” in Section 3.6.5 of SCIP-216.

SCM-009000 [Required: MG-TS – Optional: MG-LS, TA, IAD] In the Audio state, the SCIP/V.150.1 Gateway shall declare support for the four Answer events listed in Table 3-8 of Section 3.6.5 in SCIP-216, using the procedures defined in RFC 2833 (RTP Payload for DTMF Digits, Telephony Tones and Telephony Signals).

NOTE: “Support” means that the SCIP/V.150.1 Gateway shall be able to:

- a. Transmit the RFC 2833 Event over its IP interface after detecting the corresponding Answer event on its Data Communications Equipment (DCE) interface.
- b. Transmit the Answer event on its DCE interface after detecting the corresponding RFC 2833 Event on its IP interface.

SCM-009010 [Optional: MG-TS, MG-LS, TA, IAD] The SCIP/V.150.1 Gateway shall meet all the requirements for “SPRT Payload and Window Size Parameter” in Section 3.6.6 of SCIP-216.

SCM-009020 [Required: MG-TS – Optional: MG-LS, TA, IAD] The SCIP/V.150.1 Gateway shall meet all the requirements for “JM Delay Support” in Section 3.6.7 of SCIP-216.

SCM-009030 [Required: MG-TS – Optional: MG-LS, TA, IAD] The SCIP/V.150.1 Gateway shall meet all the requirements for “Call Discrimination Mode Parameters” in Section 3.6.8 of SCIP-216.

SCM-009040 [Required: MG-TS – Optional: MG-LS, TA, IAD] The SCIP/V.150.1 Gateway shall meet all the requirements for “SSE Capability Indications” in Section 3.6.9 of SCIP-216.

SCM-009050 [Required: MG-TS – Optional: MG-LS, TA, IAD] The SCIP/V.150.1 Gateway shall meet all the requirements for “SPRT Protocol Support Parameters” in Section 3.6.10 of SCIP-216.

SCM-009060 [Required: MG-TS – Optional: MG-LS, TA, IAD] The SCIP/V.150.1 Gateway shall meet all the requirements for “NoAudio Support” in Section 3.6.11 of SCIP-216.

2.21.1.1.7 Data Communications Equipment (DCE) Interface

The following requirements are based on the “DCE Interface Requirements” in Section 3.7 of SCIP-216.

SCM-009070 [Optional: MG-TS, MG-LS, TA, IAD] The SCIP/V.150.1 Gateway shall meet all the requirements for “V.14” in Section 3.7.1 of SCIP-216. The I_RAW-OCTET requirements in this section are Optional.

SCM-009080 [Required: MG-TS – Optional: MG-LS, TA, IAD] The SCIP/V.150.1 Gateway shall meet all the requirements for “Answer Tone Generation” in Section 3.7.2 of SCIP-216.

SCM-009090 [Required: MG-TS – Optional: MG-LS, TA, IAD] The SCIP/V.150.1 Gateway shall meet all the requirements for “Absence of V.42” in Section 3.7.3 of SCIP-216.

2.21.1.2 Procedural Minimum Essential Requirements

The following requirements are based on the “Procedural Minimum Essential Requirements” in Section 4 of SCIP-216.

2.21.1.2.1 *SSE State Transition*

SCM-009100 [Required: MG-TS – Optional: MG-LS, TA, IAD] The SCIP/V.150.1 Gateway shall meet all the requirements for SSE State Transition in Section 4.1 of SCIP-216.

SCM-009110 [Required: MG-TS – Optional: MG-LS, TA, IAD] The SCIP/V.150.1 Gateway shall meet all the requirements for SSE State Transitions defined in ITU-T Recommendation V.150.1, Annex C, to coordinate the transition between media states.

2.21.1.2.2 *SPRT Procedures*

The following requirements are based on the “SPRT Procedures Requirements” in Section 4.2 of SCIP-216.

SCM-009120 [Optional: MG-TS – Optional: MG-LS, TA, IAD] The SCIP/V.150.1 Gateway shall meet all the requirements for Modem Relay Data Type Selection in Section 4.2.1 of SCIP-216. The I_RAW-OCTET requirements in this section are also Optional.

SCM-009130 [Required: MG-TS; Optional: MG-LS, TA, IAD] The SCIP/V.150.1 Gateway shall meet all the requirements for “SPRT Message Ordering” in Section 4.2.2 of SCIP-216.

SCM-009140 [Required: MG-TS – Optional: MG-LS, TA, IAD] In the MR mode, the SCIP/V.150.1 Gateway shall transmit the INIT message first, followed by the MR_EVENT message and/or the CONNECT message, as described in Section 4.2.2 of SCIP-216.

SCM-009150 [Optional: MG-TS, MG-LS, TA, IAD] The SCIP/V.150.1 Gateway shall meet all the requirements for “SPRT Window and Payload Size Negotiation” in Section 4.2.3 of SCIP-216.

SCM-009160 [Required: MG-TS – Optional: MG-LS, TA, IAD] The SCIP/V.150.1 Gateway shall use the MR_EVENT and CONNECT messages to indicate the data rate in bps, as described in Section 4.2.3 of SCIP-216 (which follows the Data Matching Rule defined in ITU-T Recommendation V.150.1).

SCM-009170 [Required: MG-TS – Optional: MG-LS, TA, IAD] The SCIP/V.150.1 Gateway shall meet all the requirements for SPRT Data Signaling Rate Indication in Section 4.2.4 of SCIP-216.

SCM-009180 [Required: MG-TS – Optional: MG-LS, TA, IAD] The SCIP/V.150.1 Gateway shall use the MR_EVENT and CONNECT messages to indicate the data rate negotiated on its DCE interface in bits per second (bps), per Section 4.2.4 of SCIP-216. The SCIP/V.150.1 Gateway shall also adhere to the Rate Matching Rule defined in Section 12.3.2.1 of ITU-T Recommendation V.150.1.

2.21.1.2.3 *RFC 2833 Event Transmission Procedures*

SCM-009190 [Required: MG-TS – Optional: MG-LS, TA, IAD] The SCIP/V.150.1 Gateway shall meet all the requirements for RFC 2833 Event Transmission Procedures in Section 4.3 of SCIP-216.

2.21.1.2.4 *Native Session to Modem-Based Session Transition Procedures*

The following requirements are based on the “Native Session to Modem-Based Session Transition Procedures” in Section 4.4 of SCIP-216.

SCM-009200 [Required: MG-TS – Optional: MG-LS, TA, IAD] The SCIP/V.150.1 Gateway shall use the SSE protocol to transition between the Audio (native state) and MR modes of operation, per Section 4.4 of SCIP-216.

SCM-009210 [Required: MG-TS – Optional: MG-LS, TA, IAD] The SCIP/V.150.1 Gateway SSE state shall always start in the Audio mode, per Section 4.4.1 of SCIP-216.

SCM-009220 [Required: MG-TS – Optional: MG-LS, TA, IAD] The SCIP/V.150.1 Gateway shall meet all the requirements for “SSE Audio to Modem Relay Transitions” in Section 4.4.1 of SCIP-216.

SCM-009230 [Required: MG-TS – Optional: MG-LS, TA, IAD] The SCIP/V.150.1 Gateway shall meet all the requirements for “Procedures for SPRT Modem Relay Setup” in Section 4.4.2 of SCIP-216.

2.21.1.2.5 *Modem-Based Session to Native Session Transition (Cleardown) Procedures*

The following requirements are based on the “Modem-Based Session to Native Session Transition (Cleardown) Procedures” in Section 4.5 of SCIP-216.

SCM-009240 [Required: MG-TS – Optional: MG-LS, TA, IAD] The SCIP/V.150.1 Gateway shall meet all the requirements for “Procedures for PSTN Initiated Cleardown” in Section 4.5.1 of SCIP-216.

SCM-009250 [Required: MG-TS – Optional: MG-LS, TA, IAD] The SCIP/V.150.1 Gateway shall meet all the requirements for “Procedures for IP Initiated Cleardown” in Section 4.5.2 of SCIP-216.

2.21.1.2.6 *Transition to On-Hook While in a Modem-Based Session*

The following requirements are based on the “Transition to On-Hook While in a Modem-Based Session” in Section 4.6 of SCIP-216.

SCM-009260 [Required: MG-TS – Optional: MG-LS, TA, IAD] The SCIP/V.150.1 Gateway shall meet all the requirements for “Procedures for IP Initiated On-Hook” in Section 4.6.1 of SCIP-216.

SCM-009270 [Required: MG-TS – Optional: MG-LS, TA, IAD] The SCIP/V.150.1 Gateway shall meet all the requirements for “Procedures for PSTN Initiated On-Hook” in Section 4.6.2 of SCIP-216.

2.21.1.2.7 SPRT CLEARDOWN Procedures

SCM-009280 [Optional: MG-TS, MG-LS, TA, IAD] The SCIP/V.150.1 Gateway shall meet all the requirements for “SPRT CLEARDOWN Procedures” in Section 4.7 of SCIP-216.

2.21.1.2.8 Call Menu – Joint Menu Procedures

SCM-009290 [Required: MG-TS – Optional: MG-LS, TA, IAD] The SCIP/V.150.1 Gateway shall meet all the requirements for “Call Menu (CM) – Joint Menu (JM)” Procedures in Section 4.8 of SCIP-216.

2.21.1.2.9 NoAudio Payload Type Requirements for SCIP-216 Compliant Gateways

SCM-009300 [Required: MG-TS – Optional: MG-LS, TA, IAD] The SCIP/V.150.1 Gateway shall meet all the requirements for NoAudio Payload Type in Section 4.9 of SCIP-216.

SCM-009310 [Required: MG-TS – Optional: MG-LS, TA, IAD] The SCIP/V.150.1 Gateway shall support a NoAudio payload type for “Modem-Relay-Preferred” end points, per Section 4.9 of SCIP-216.

The SCIP-216 defines a “Modem-Relay-Preferred” end point as a SCIP-216 end point that immediately transitions to the Modem Relay state without transmitting information in the Audio state.

2.21.1.2.10 Transfer of Application Data Between the IP and DCE Interfaces

The following requirements are based on the “Transfer of Application Data between the IP and DCE Interfaces” requirements in Section 4.10 of SCIP-216.

SCM-009320 [Optional: MG-TS, MG-LS, TA, IAD] The SCIP/V.150.1 Gateway shall meet all the requirements for “Processing of Data Received on the DCE Interface” in Section 4.10.1 of SCIP-216. I_RAW-OCTET requirements in this section are optional.

SCM-009330 [Required: MG-TS – Optional: MG-LS, TA, IAD] The SCIP/V.150.1 Gateway shall support the formatting of data received from the DCE (modem) interface into the I_OCTET and I_OCTET-CS Modem Relay data types sent on the IP interface, according to Section 4.10.1 of SCIP-216.

SCM-009340 [Optional: MG-TS – MG-LS, TA, IAD] The SCIP/V.150.1 Gateway shall meet all the requirements for “Processing of Data Received on the IP Interface” in Section 4.10.2 of SCIP-216. I_RAW-OCTET requirements in this section are Optional.

SCM-009350 [Required: MG-TS – Optional: MG-LS, TA, IAD] The SCIP/V.150.1 Gateway shall support the conversion of data received in the I_OCTET and I_OCTET-CS Modem Relay data types on the IP interface into asynchronous V.14 data characters sent on the DCE (modem) interface, according to Section 4.10.2 of SCIP-216.

SCM-009360 [Required: MG-TS – Optional: MG-LS, TA, IAD] The SCIP/V.150.1 Gateway shall meet all the requirements for “Lost Packet Processing with I_OCTET-CS” in Section 4.10.3 of SCIP-216.

2.21.1.3 SSE and SPRT Message Content

The following requirements are based on the “SSE and SPRT Message Content” requirements in Section 5 of SCIP-216.

2.21.1.3.1 SSE Messages

The following requirements are based on the “SSE Messages” requirements in Section 5.1 of SCIP-216.

SCM-009370 [Required: MG-TS – Optional: MG-LS, TA, IAD] The SCIP/V.150.1 Gateway shall meet all the requirements for the SSE Audio Message in Section 5.1.1 of SCIP-216.

SCM-009380 [Required: MG-TS – Optional: MG-LS, TA, IAD] The SCIP/V.150.1 Gateway shall meet all the requirements for the “SSE Modem Relay Message” in Section 5.1.2 of SCIP-216.

2.21.1.3.2 SPRT Messages

The following requirements are based on the “SPRT Messages” requirements in Section 5.2 of SCIP-216.

SCM-009390 [Required: MG-TS – Optional: MG-LS, TA, IAD] The SCIP/V.150.1 Gateway shall meet all the requirements for the “SPRT INIT Message” in Section 5.2.1 of SCIP-216.

SCM-009400 [Required: MG-TS – Optional: MG-LS, TA, IAD] The SCIP/V.150.1 Gateway shall meet all the requirements for the “SPRT JM_INFO Message” in Section 5.2.2 of SCIP-216.

SCM-009410 [Required: MG-TS – Optional: MG-LS, TA, IAD] The SCIP/V.150.1 Gateway shall meet all the requirements for the “SPRT CONNECT Message” in Section 5.2.3 of SCIP-216.

SCM-009420 [Required: MG-TS – Optional: MG-LS, TA, IAD] The SCIP/V.150.1 Gateway shall meet all the requirements for the “SPRT MR_EVENT Message” in Section 5.2.4 of SCIP-216.

SCM-009430 [Required: MG-TS – Optional: MG-LS, TA, IAD] The SCIP/V.150.1 Gateway shall meet all the requirements for the “SPRT CLEARDOWN Message” in Section 5.2.5 of SCIP-216.

NOTE: Transmission of this message is optional in SCIP-216, but reception of this message is required.

SCM-009440 [Conditional: MG-TS, MG-LS, TA, IAD] If the SPRT I_RAW-OCTET Message is supported, the SCIP/V.150.1 Gateway shall meet all the requirements for that Message in Section 5.2.6 of SCIP-216. (Support for the I_RAW-OCTET data type is currently optional in SCIP-216, but may become a requirement later.)

SCM-009450 [Required: MG-TS – Optional: MG-LS, TA, IAD] The SCIP/V.150.1 Gateway shall meet all the requirements for the SPRT I_OCTET Message in Section 5.2.7 of SCIP-216.

SCM-009460 [Required: MG-TS – Optional: MG-LS, TA, IAD] The SCIP/V.150.1 Gateway shall meet all the requirements for the SPRT I_OCTET-CS Message in Section 5.2.8 of SCIP-216.

2.21.1.4 Use of Common UDP Port Numbers for SRTP, SSE, and SPRT Messages

SCM-009470 [Required: MG-TS – Optional: MG-LS, TA, IAD] The SCIP/V.150.1 Gateway shall use the same UDP port numbers and protocol numbers for the following:

- a. The SRTP media packets sent and received during the Audio mode (when the call is “in the clear”).
- b. The SSE media packets sent and received during transitions between the Audio and Modem Relay modes (when the call is moving between “in the clear” and “secure”).
- c. The SPRT media packets sent and received during the Modem Relay mode (when the call is “secure”).

The UDP port numbers shall be the UDP port numbers negotiated by the SCIP/V.150.1 Gateway and the remote party (SCIP/V.150.1 EI or remote SCIP/V.150.1 Gateway) using SDP during UC SIP session establishment.

The UDP protocol number (the protocol number used in IP packets to indicate that the UDP protocol is being transported) shall be protocol number 17, as registered with the Internet Assigned Numbers Authority (IANA). Per the IANA Web site page on Assigned Internet Protocol Numbers (<http://www.iana.org/assignments/protocol-numbers/>):

“In the Internet Protocol version 4 (IPv4) [RFC 791] there is a field called “Protocol” to identify the next level protocol. This is an 8-bit field. In Internet Protocol version 6 (IPv6) [RFC 2460], this field is called the “Next Header” field.”

SCM-009480 [Required: MG-TS – Optional: MG-LS, TA, IAD] When an SCIP/V.150.1 Gateway transitions the media stream between a normal session using SRTP and a secure session using SPRT, the SCIP/V.150.1 Gateway shall use the same UDP port numbers and UDP protocol number (17) for both the normal session and the secure session, so that the media stream transition is transparent to the SBC (when the SBC is located in the media stream for those sessions).

SCM-009490 [Required: MG-TS – Optional: MG-LS, TA, IAD] The SCIP/V.150.1 Gateway shall not use UC SIP and SDP to negotiate a new UDP port number when the call is changing from audio mode (SRTP) and modem relay mode (SPRT), or from modem relay mode back to audio mode.

SCM-009500 [Required: MG-TS – Optional: MG-LS, TA, IAD] The SCIP/V.150.1 Gateway shall not use UC SIP and SDP to negotiate multiple UDP port numbers (one for Audio (SRTP), another for mode transitions (SSE), and yet another for modem relay (SPRT)) during UC SIP session establishment.

The SCIP-216 allows this multiple UDP port number approach, but the SCIP/V.150.1 Gateway shall not use this approach because it adds complexity to session establishment and has a negative effect on SBCs.

2.21.1.5 UDP Port Number for SRTCP Media Control Packets

SCM-009510 [Required: MG-TS – Optional: MG-LS, TA, IAD] The SCIP/V.150.1 Gateway shall maintain, for the duration of a call, the UDP port number used for the SRTCP media control packets that are sent and received during the Audio mode (when the call is “in the clear”).

This UDP port number shall be the UDP port number negotiated for SRTCP media control packets by the SCIP/V.150.1 Gateway and the remote party (SCIP/V.150.1 EI or remote SCIP/V.150.1 Gateway) using SDP during UC SIP session establishment.

SCM-009520 [Required: MG-TS – Optional: MG-LS, TA, IAD] When a call transitions from Audio mode to Modem Relay mode, the SCIP/V.150.1 Gateway shall stop sending SRTCP packets, but shall maintain the UDP port number that had been used for exchanging SRTCP packets.

SCM-009530 [Required: MG-TS – Optional: MG-LS, TA, IAD] If a call transitions from Audio mode to Modem Relay mode, and then later back to Audio mode, the SCIP/V.150.1 Gateway shall resume sending and receiving SRTCP packets using the same UDP port number that was previously used in Audio mode for those packets.

2.21.1.6 Use of V.150.1 SSE Messages for Media Transitions Between Audio and Modem Relay

SCM-009540 [Required: MG-TS – Optional: MG-LS, TA, IAD] Per Section 4, Information Assurance, SCIP/V.150.1 Gateways shall protect audio and video media streams using SRTP, when exchanging these media streams with SCIP/V.150.1 Phones and other SCIP/V.150.1 Gateways.

(When SCIP/V.150.1 Gateways exchange modem relay media streams with SCIP/V.150.1 Phones and other gateways, the modem relay media streams are sent over SPRT, and not sent over SRTP. As a result, these modem relay media streams are not protected by SRTP.)

SCM-009550 [Required: MG-TS – Optional: MG-LS, TA, IAD] When SCIP/V.150.1 Gateways exchange RFC 2833 Events and V.150.1 SSE messages with SCIP/V.150.1 Phones and other Gateways, these RFC 2833 Events and SSE messages shall also be protected using SRTP. These messages and events shall not be exchanged using SPRT, and they shall not be exchanged using RTP without SRTP.

SCM-009560 [Required: MG-TS – Optional: MG-LS, TA, IAD] For all IP-TDM and TDM-IP interworking calls, SCIP/V.150.1 Gateways shall declare that they support audio, modem relay, SRTP, SSE, and SPRT in the original SDP offer (UC SIP INVITE message) and SDP answer (200 OK response) for each call. SCIP/V.150.1 Gateways shall not reserve or allocate a modem relay resource at this point because the call will typically begin as an audio call, which does not require a modem relay resource.

SCM-009570 [Required: MG-TS – Optional: MG-LS, TA, IAD] After one end of the call (the TDM SCIP phone or IP SCIP phone) decides to go secure, the SCIP/V.150.1 Gateway shall begin the process of changing the established media stream from audio media to modem relay media. On the IP portion of this call, the SCIP/V.150.1 Gateway shall begin this processing by exchanging SSE messages with the SCIP/V.150.1 Phone, SBC, or other SCIP/V.150.1 Gateway, per ITU-T Recommendation V.150.1 and SCIP-216.

SCM-009580 [Required: MG-TS – Optional: MG-LS, TA, IAD] As part of the Audio-media-to-Modem-Relay-media conversion process, the SCIP/V.150.1 Gateway shall not send an outgoing UC SIP re-INVITE message that requests Audio-to-Modem-Relay media conversion.

SCM-009590 [Required: MG-TS – Optional: MG-LS, TA, IAD] As part of the Audio-media-to-Modem-Relay-media conversion process, the SCIP/V.150.1 Gateway shall not require the receipt of an incoming UC SIP re-INVITE message that requests Audio-to-Modem-Relay media conversion.

SCM-009600 [Required: MG-TS – Optional: MG-LS, TA, IAD] The SCIP/V.150.1 Gateway shall not reserve and allocate one of its modem relay resources for the media stream for this call, until the SSE message exchange for Audio-to-Modem-Relay media conversion has begun.

SCM-009610 [Required: MG-TS – Optional: MG-LS, TA, IAD] After one end of the call (the TDM SCIP phone or IP SCIP phone) decides to return to “voice in the clear,” the SCIP/V.150.1 Gateway shall begin the process of changing the established media stream from modem relay media to Audio media. On the IP portion of this call, the SCIP/V.150.1 Gateway shall begin this processing by exchanging SSE messages with the SCIP/V.150.1 Phone, SBC, or other SCIP/V.150.1 Gateway, per ITU-T Recommendation V.150.1 and SCIP-216.

SCM-009620 [Required: MG-TS – Optional: MG-LS, TA, IAD] As part of the Modem-Relay-media-to-Audio-media conversion process, the SCIP/V.150.1 Gateway shall not send an outgoing UC SIP re-INVITE message that requests Modem-Relay-to-Audio media conversion.

SCM-009630 [Required: MG-TS – Optional: MG-LS, TA, IAD] As part of the Modem-Relay-media-to-Audio-media conversion process, the SCIP/V.150.1 Gateway shall not require the receipt of an incoming UC SIP re-INVITE message that requests Modem-Relay-to-Audio-media conversion.

SCM-009640 [Required: MG-TS – Optional: MG-LS, TA, IAD] The SCIP/V.150.1 Gateway shall not release and de-allocate its modem relay resource for the media stream for this call until the SSE message exchange for Modem-Relay-to-Audio media conversion has begun.

SCM-009650 [Required: MG-TS – Optional: MG-LS, TA, IAD] The SCIP/V.150.1 Gateways shall still be able to send and receive UC SIP re-INVITE messages during an audio call. (For example, the gateway can use the UC SIP re-INVITE message to request an Audio codec change during the audio/clear voice portion of a call, when the Gateway is using G.711 for audio media but then asks the far end to use G.729 for Audio media instead.) When the Gateway includes modem relay media information in an UC SIP re-INVITE message, the Gateway shall make sure that this is the same modem relay information that was present in the initial UC SIP INVITE message or 200 OK response that established the call. In this way, the UC SIP re-INVITE message is not used to request an Audio-to-Modem-Relay transition.

2.21.1.7 Modem Relay and VoIP for SCIP/V.150.1 Gateways

SCM-009660 [Required: MG-TS – Optional: MG-LS, TA, IAD] When an SCIP/V.150.1 Gateway is unable to provide modem relay on an MoIP call (e.g., because the remote end is not modem relay capable, or the remote end is modem relay capable but does not currently have any modem relay resources available), then the SCIP/V.150.1 Gateway shall instead provide VoIP treatment for that call. In this case, the SCIP/V.150.1 Gateway shall handle the MoIP call in the SC or SS in the same way that it would handle a G.711 VoIP call in the SC or SS, with these clarifications:

- a. The Gateway shall still disable EC for the MoIP call being handled as a G.711 VoIP call, when the Gateway detects an “EC disabling” tone from either the TDM side or the MoIP side of the call (see [Section 2.16.9](#), MG Requirements for Echo Cancellation).
- b. The Gateway may disable silence suppression on the MoIP side of the call.

If the Gateway also supports Voiceband Data codecs (proprietary and/or V.152) then the Gateway may provide VBD treatment for the MoIP call instead of providing VoIP treatment for that call.

NOTE: End-to-end synchronization of the calling and called modems (or modem-equipped SCIP phones) is not guaranteed on a VoIP call. Even though a VoIP call may complete between these two modems (i.e., a successful UC SIP signaling INVITE/200 OK/ACK exchange can occur, and G.711 media can be exchanged over SRTP, UDP, and IP), there is no guarantee that the two modems will be able to synchronize and exchange data using the resulting G.711 media streams. Even if the two modems do synchronize and exchange data, there is no guarantee that this synchronization and exchange will be maintained over time, or that the synchronization and exchange will result in a data throughput that matches what would be provided by a modem relay call, or by an E2E TDM call in a TDM voice network.

Because of this, there are no requirements in this section for the reliability of modem synchronization, reliability of data exchange, or rate of data transfer on VoIP calls. It is expected that these calls will complete using UC SIP signaling and SRTP media exchange like VoIP calls do. But it is not expected that the resulting synchronization and data exchange will be 100 percent reliable, or that the data rate provided will match what would be provided on a modem relay call or TDM modem call under the same conditions.

SCM-009670 [Required: MG-TS] The SCIP/V.150.1 Gateway shall support adequate V.150.1/SCIP-216 modem relay resources so that 10 percent of the maximum number of calls that can pass through the trunk-side interfaces of the MG (from TDM end points to IP end points, and from IP end points to TDM end points) can receive modem relay treatment, instead of receiving VoIP treatment.

NOTE: The acquiring activity for the SCIP/V.150.1 Gateway should also determine, based on traffic engineering and vendor prices, the required number of MG modem relay resources (e.g., Modem-Relay-equipped trunk cards, or modem relay DSP cards) that will support V.150.1/SCIP-216 modem relay. V.150.1/SCIP-216 modem relay is needed to support IP SCIP phones (SCIP-215 phones) on an SC or SS, and analog SCIP phones behind TAs, IADs, and MG line cards on an SC or SS.

2.21.1.8 Modem Relay Support for V.92 and V.90 Modulation Types

SCM-009680 [Required: MG-TS] On SCIP-216 modem relay calls where the V.92 Digital modulation type (UCR Required) is used, the TDM side of the MG-TS shall act as the digital interface to the remote V.92 Server modem.

SCM-009690 [Conditional: MG-LS, TA, IAD] If V.92 Analog modulation type (UCR Optional) is used on a SCIP-216 modem relay call, then the TDM side of the MG-LS, TA, or

IAD shall act as the analog interface to the local V.92 client modem (e.g., a V.92 modem on an RJ-11 port on a DOD laptop computer).

SCM-009700 [Required: MG-TS – Optional: MG-LS, TA, IAD] The SCIP-216 modem relay communication between the MG-TS and the MG-LS, TA, or IAD shall support V.92-Server-modem-to-V.92-Client-modem communication in the MG-TS-to-MG-LS/IAD/TA direction, and V.92-Client-modem-to-V.92-Server-modem communication in the MG-LS/IAD/TA-to-MG-TS direction.

SCM-009710 [Required: MG-TS – Optional: MG-LS, TA, IAD] The data rate supported in the V.92-Server-modem-to-V.92-Client-modem direction shall be greater than 33.6 Kbps and less than 53.3 Kbps (the U.S. PSTN limit on 56 Kbps data communication). The data rate supported in the V.92-Client-modem-to-V.92-Server-modem direction shall be greater than 33.6 Kbps and less than 53.3 Kbps also.

SCM-009720 [Required: MG-TS] On SCIP-216 modem relay calls where the V.90 digital modulation type (UCR Required) is used, the TDM side of the MG-TS shall act as the digital interface to the remote V.90 server modem.

SCM-009730 [Conditional: MG-LS, TA, IAD] On SCIP-216 modem relay calls where the V.90 analog modulation type (UCR Optional) is used, the TDM side of the MG-LS, TA, or IAD shall act as the analog interface to the local V.90 client modem (e.g., a V.90 modem on an RJ-11 port on a DOD laptop computer).

SCM-009740 [Required: MG-TS – Optional: MG-LS, TA, IAD] The SCIP-216 modem relay communication between the MG-TS and the MG-LS, TA, or IAD shall support V.90-Server-modem-to-V.90-Client-modem communication in the MG-TS-to-MG-LS/IAD/TA direction, and V.90-Client-modem-to-V.90-Server-modem communication in the MG-LS/IAD/TA-to-MG-TS direction.

SCM-009750 [Required: MG-TS – Optional: MG-LS, TA, IAD] The data rate supported in the V.90-Server-modem-to-V.90-Client-modem direction shall be greater than 33.6 Kbps and less than 53.3 Kbps (the U.S. PSTN limit on 56 Kbps data communication). The data rate supported in the V.90-Client-modem-to-V.90-Server-modem direction shall be greater than 28.8 Kbps and less than or equal to 33.6 Kbps.

2.21.1.9 Going Secure, Glare Conditions, and Modem Relay Preferred Devices

SCM-009760 [Required: MG-TS – Optional: MG-LS, TA, IAD] The calling or called SCIP/V.150.1 Gateway shall be able to initiate going secure. The calling or called SCIP/V.150.1 Gateway shall be able to send an answer message (ANS) signal toward the far-end SCIP endpoint (MG or EI).

SCM-009770 [Required: MG-TS – Optional: MG-LS, TA, IAD] If a glare condition results from an SCIP/V.150.1 Gateway initiating going secure and sending an ANS signal toward the

far-end SCIP endpoint (MG or EI) at the same time that the far endpoint initiates going secure and sends an ANS signal to the SCIP/V.150.1 Gateway, then the SCIP/V.150.1 Gateway and the far end SCIP endpoint both shall back off their request and try again later.

SCM-009780 [Required: MG-TS – Optional: MG-LS, TA, IAD] An SCIP/V.150.1 Gateway operating as a SCIP Modem Relay Preferred (MRP) device shall transition automatically from the audio state to the modem relay state upon the SCIP call being answered. This means that the first media stream packet sent by the MRP device shall be a Secure RTP (SRTP) packet containing an IETF RFC 2833 message indicating that an ANS, /ANS, ANSam, or /ANSam Event is being signaled.

This also means that the first media stream packet received by the MRP device (i.e., sent to the MRP device by the other V.150.1 device on the call) shall be an SRTP packet containing an SSE message indicating a transition from audio to modem relay (Event Code 3). Once this transition is successful, the MRP device shall begin sending SPRT packets containing SCIP protocol information (secure voice or secure data media).

If the MRP device receives an RFC 233 message containing an ANS, /ANS, ANSam, or /ANSam Event before that device sends its own RFC 2833 message and ANS, /ANS, ANSam, or /ANSam Event, the MRP device shall send an SRTP packet back to the other V.150.1 device, containing an SSE message indicating a transition from audio to modem relay (Event Code 3). Once this transition is successful, the MRP device shall begin sending SPRT packets containing SCIP protocol information (secure voice or secure data media).

2.21.2 SCIP/V.150.1 EI

This section contains the SCIP/V.150.1 EI requirements for UCR, based on the NSA document: SCIP-215, Revision 2.1. All references to “SCIP-215” in the following paragraphs are references to SCIP-215, Revision 2.1.

A “SCIP/V.150.1 EI” is a Secure IP Phone that conforms to SCIP-215, conforms to the requirements in this section, and is served by a SC.

A SCIP/V.150.1 EI also communicates with the SC using one of the following:

- Vendor-proprietary signaling and transport protocols.
- UC SIP signaling over TLS.

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

The following SCIP/V.150.1 EI requirements apply to both SCIP/V.150.1 EIs in Strategic (Fixed) Networks, and to SCIP/V.150.1 EIs in Tactical (Deployable) networks.

2.21.2.1 Basic Minimum Essential Requirements (MERs)

The following requirements are based on the basic MER in Section 4 of SCIP-215.

2.21.2.1.1 IP Transport Layer Protocol

SCM-009790 [Required: SCIP/V.150.1 EI] The SCIP/V.150.1 EI shall meet all the requirements for “IP Transport Layer Protocol” in Section 4.1 of SCIP-215.

2.21.2.1.2 V.150.1 Operational Mode

SCM-009800 [Required: SCIP/V.150.1 EI] The SCIP/V.150.1 EI shall meet all the requirements for “V.150.1 Operational Mode” in Section 4.2 of SCIP-215.

2.21.2.1.3 Modem-Relay Gateway Type

SCM-009810 [Required: SCIP/V.150.1 EI] The SCIP/V.150.1 EI shall meet all the requirements for “Modem-Relay Gateway Type” in Section 4.3 of SCIP-215.

2.21.2.1.4 Simple Packet Relay Transport

The following requirements are based on the SPRT requirements in Section 4.4 of SCIP-215.

SCM-009820 [Required: SCIP/V.150.1 EI] The SCIP/V.150.1 EI shall meet all the requirements for “Transport Channel” in Section 4.4.1 of SCIP-215.

SCM-009830 [Required: SCIP/V.150.1 EI] The SCIP/V.150.1 EI shall meet all the requirements for “SPRT Modem Relay Messages” in Section 4.4.2 of SCIP-215.

SCM-009840 [Required: SCIP/V.150.1 EI] The SCIP/V.150.1 EI shall meet all the requirements for “SPRT Timer” in Section 4.4.3 of SCIP-215.

2.21.2.1.5 SSE

The following requirements are based on the SSE requirements in Section 4.5 of SCIP-215.

SCM-009850 [Required: SCIP/V.150.1 EI] The SCIP/V.150.1 EI shall meet all the requirements for “SSE Call Discrimination Messages” in Section 4.5.1 of SCIP-215.

SCM-009860 [Required: SCIP/V.150.1 EI] The SCIP/V.150.1 EI shall meet all the requirements for “SSE Reliability” in Section 4.5.2 of SCIP-215.

SCM-009870 [Required: SCIP/V.150.1 EI] The SCIP/V.150.1 EI shall meet all the requirements for “SSE Reason Identifier Code” in Section 4.5.3 of SCIP-215.

SCM-009880 [Required: SCIP/V.150.1 EI] The SCIP/V.150.1 EI shall meet all the requirements for “SSE Timer” in Section 4.5.4 of SCIP-215.

2.21.2.1.6 *Call Setup Protocol*

The following requirements are based on the “Call Setup Protocol Requirements for Negotiating Specific V.150.1 Capabilities” in Section 4.6 of SCIP-215.

SCM-009890 [Required: SCIP/V.150.1 EI] The SCIP/V.150.1 EI shall meet all the requirements for “V.150.1 Version Declaration” in Section 4.6.1 of SCIP-215.

SCM-009900 [Required: SCIP/V.150.1 EI] The SCIP/V.150.1 EI shall meet all the requirements for “Transcompression Capability” in Section 4.6.2 of SCIP-215.

SCM-009910 [Required: SCIP/V.150.1 EI] The SCIP/V.150.1 EI shall meet all the requirements for “Modem Relay Type Declaration” in Section 4.6.3 of SCIP-215.

SCM-009920 [Required: SCIP/V.150.1 EI] The SCIP/V.150.1 EI shall meet all the requirements for “Modulation Support Indication” in Section 4.6.4 of SCIP-215.

SCM-009930 [Required: SCIP/V.150.1 EI] The SCIP/V.150.1 EI shall meet all the requirements for “RFC 2833 Events” in Section 4.6.5 of SCIP-215.

SCM-009940 [Optional: SCIP/V.150.1 EI] The SCIP/V.150.1 EI shall meet all the requirements for “SPRT Payload and Window Size Parameter” in Section 4.6.6 of SCIP-215.

SCM-009950 [Required: SCIP/V.150.1 EI] The SCIP/V.150.1 EI shall meet all the requirements for “JM Delay Support” in Section 4.6.7 of SCIP-215.

SCM-009960 [Required: SCIP/V.150.1 EI] The SCIP/V.150.1 EI shall meet all the requirements for “Call Discrimination Mode Parameter” in Section 4.6.8 of SCIP-215.

SCM-009970 [Required: SCIP/V.150.1 EI] The SCIP/V.150.1 EI shall meet all the requirements for “SSE Capability Indication” in Section 4.6.9 of SCIP-215.

SCM-009980 [Required: SCIP/V.150.1 EI] The SCIP/V.150.1 EI shall meet all the requirements for “SPRT Protocol Support Parameters” in Section 4.6.10 of SCIP-215.

SCM-009990 [Required: SCIP/V.150.1 EI] The SCIP/V.150.1 EI shall meet all the requirements for “NoAudio Support” in Section 4.6.11 of SCIP-215.

2.21.2.1.7 *SCIP Operational Mode*

SCM-010000 [Required: SCIP/V.150.1 EI] The SCIP/V.150.1 EI shall meet all the requirements for “SCIP Operational Mode” in Section 4.7 of SCIP-215.

2.21.2.1.8 *V.14*

SCM-010010 [Optional: SCIP/V.150.1 EI] The SCIP/V.150.1 EI shall meet all the requirements for “V.14” in Section 4.8 of SCIP-215.

2.21.2.2 Procedural MER

The following requirements are based on the Procedural MER in Section 5 of SCIP-215.

2.21.2.2.1 SSE State Transition

SCM-010020 [Required: SCIP/V.150.1 EI] The SCIP/V.150.1 EI shall meet all the requirements for “SSE State Transition” in Section 5.1 of SCIP-215.

2.21.2.2.2 SPRT Procedures

The following requirements are based on the “SPRT Procedures Requirements” in Section 5.2 of SCIP-215.

SCM-010030 [Optional: SCIP/V.150.1 EI] The SCIP/V.150.1 EI shall meet all the requirements for modem relay “Data Type Selection” in Section 5.2.1 of SCIP-215. The I_RAW-OCTET requirements in this section are conditional.

SCM-010040 [Required: SCIP/V.150.1 EI] The SCIP/V.150.1 EI shall meet all the requirements for “SPRT Message Ordering” in Section 5.2.2 of SCIP-215.

SCM-010050 [Optional: SCIP/V.150.1 EI] The SCIP/V.150.1 EI shall meet all the requirements for “SPRT Window and Payload Size Negotiation” in Section 5.2.3 of SCIP-215.

SCM-010060 [Required: SCIP/V.150.1 EI] The SCIP/V.150.1 EI shall meet all the requirements for “SPRT Data Signaling Rate Indication” in Section 5.2.4 of SCIP-215.

2.21.2.2.3 RFC 2833 Event Transmission Procedures

SCM-010070 [Required: SCIP/V.150.1 EI] The SCIP/V.150.1 EI shall meet all the requirements for “RFC 2833 Event Transmission Procedures” in Section 5.3 of SCIP-215.

2.21.2.2.4 Clear-to-SCIP Traffic Transition Procedures

The following requirements are based on the “Clear-to-SCIP Traffic Transition Procedures” in Section 5.4 of SCIP-215.

SCM-010080 [Required: SCIP/V.150.1 EI] The SCIP/V.150.1 EI shall meet all the requirements for SSE Audio to modem relay Transitions in Section 5.4.1 of SCIP-215.

SCM-010090 [Required: SCIP/V.150.1 EI] The SCIP/V.150.1 EI shall meet all the requirements for Procedures for SPRT modem relay Setup in Section 5.4.2 of SCIP-215.

2.21.2.2.5 *SCIP Traffic-to-Clear Transition (Cleardown) Procedures*

The following requirements are based on the “SCIP Traffic-to-Clear Transition (Cleardown) Procedures” in Section 5.5 of SCIP-215.

SCM-010100 [Required: SCIP/V.150.1 EI] The SCIP/V.150.1 EI shall meet all the requirements for “Procedures for PSTN Initiated Cleardown” in Section 5.5.1 of SCIP-215.

SCM-010110 [Required: SCIP/V.150.1 EI] The SCIP/V.150.1 EI shall meet all the requirements for “Procedures for IP Initiated Cleardown” in Section 5.5.2 of SCIP-215.

2.21.2.2.6 *Transition to On-Hook While in a Modem-Based Session*

The following requirements are based on the “Transition to On-Hook While Exchanging SCIP Information” requirements in Section 5.6 of SCIP-215.

SCM-010120 [Required: SCIP/V.150.1 EI] The SCIP/V.150.1 EI shall meet all the requirements for Procedures for IP Initiated On-hook in Section 5.6.1 of SCIP-215.

SCM-010130 [Required: SCIP/V.150.1 EI] The SCIP/V.150.1 EI shall meet all the requirements for “Procedures for PSTN Initiated On-Hook” in Section 5.6.2 of SCIP-215.

2.21.2.2.7 *SPRT CLEARDOWN Procedures*

SCM-010140 [Optional: SCIP/V.150.1 EI] The SCIP/V.150.1 EI shall meet all the requirements for “SPRT CLEARDOWN Procedures” in Section 5.7 of SCIP-215.

2.21.2.2.8 *Call Menu (CM) – Joint Menu (JM) Procedures*

SCM-010150 [Required: SCIP/V.150.1 EI] The SCIP/V.150.1 EI shall meet all the requirements for “Call Menu (CM) – Joint Menu (JM) Procedures” in Section 5.8 of SCIP-215.

2.21.2.2.9 *Use of the NoAudio Payload Type by “Modem Relay-Preferred” Terminals*

SCM-010160 [Required: SCIP/V.150.1 EI] The SCIP/V.150.1 EI shall meet all the requirements for “Use of the NoAudio Payload Type By ‘Modem Relay-Preferred’ Terminals” in Section 5.9 of SCIP-215.

2.21.2.2.10 *Bandwidth Negotiation*

SCM-010170 [Required: SCIP/V.150.1 EI] The SCIP/V.150.1 EI shall meet all the requirements for “Bandwidth Negotiation” in Section 5.10 of SCIP-215.

2.21.2.3 *SSE and SPRT Message Content*

The following requirements are based on the “SSE and SPRT Message Content” requirements in Section 6 of SCIP-215.

2.21.2.3.1 *SSE Messages*

The following requirements are based on the “SSE Messages” requirements in Section 6.1 of SCIP-215.

SCM-010180 [Required: SCIP/V.150.1 EI] The SCIP/V.150.1 EI shall meet all the requirements for the “SSE Audio Message” in Section 6.1.1 of SCIP-215.

SCM-010190 [Required: SCIP/V.150.1 EI] The SCIP/V.150.1 EI shall meet all the requirements for the “SSE modem relay Message” in Section 6.1.2 of SCIP-215.

2.21.2.3.2 *SPRT Messages*

The following requirements are based on the “SPRT Messages” requirements in Section 6.2 of SCIP-215.

SCM-010200 [Required: SCIP/V.150.1 EI] The SCIP/V.150.1 EI shall meet all the requirements for the “SPRT INIT Message” in Section 6.2.1 of SCIP-215.

SCM-010210 [Required: SCIP/V.150.1 EI] The SCIP/V.150.1 EI shall meet all the requirements for the “SPRT JM_INFO Message” in Section 6.2.2 of SCIP-215.

SCM-010220 [Required: SCIP/V.150.1 EI] The SCIP/V.150.1 EI shall meet all the requirements for the “SPRT CONNECT Message” in Section 6.2.3 of SCIP-215.

SCM-010230 [Required: SCIP/V.150.1 EI] The SCIP/V.150.1 EI shall meet all the requirements for the “SPRT MR_EVENT” message in Section 6.2.4 of SCIP-215.

SCM-010240 [Required: SCIP/V.150.1 EI] The SCIP/V.150.1 EI shall meet all the requirements for the “SPRT CLEARDOWN” message in Section 6.2.5 of SCIP-215.

NOTE: Transmission of this message is optional in SCIP-215, but reception of this message is required.

SCM-010250 [Conditional: SCIP/V.150.1 EI] If the SPRT I_RAW-OCTET message is supported (UCR Optional), the SCIP/V.150.1 EI shall meet all the requirements for that message in Section 6.2.6 of SCIP-215.

SCM-010260 [Required: SCIP/V.150.1 EI] The SCIP/V.150.1 EI shall meet all the requirements for the “SPRT I_OCTET” message in Section 6.2.7 of SCIP-215.

SCM-010270 [Required: SCIP/V.150.1 EI] The SCIP/V.150.1 EI shall meet all the requirements for the “SPRT I_OCTET-CS” message in Section 6.2.8 of SCIP-215.

2.21.2.4 Use of Common UDP Port Numbers for SRTP, SSE, and SPRT Messages

SCM-010280 [Required: SCIP/V.150.1 EI] The SCIP/V.150.1 EI shall use the same UDP port and protocol numbers for SRTP media packets sent and received during the Audio mode (when the call is “in the clear”), SSE media packets sent and received during transitions between the Audio and modem relay modes (when the call is moving between “in the clear” and “secure”), and SPRT media packets sent and received during the modem relay mode (when the call is “secure”).

The UDP port numbers shall be the UDP port numbers negotiated by the SCIP/V.150.1 EI and the remote party (SCIP/V.150.1 Gateway or other SCIP/V.150.1 EI) using SDP during UC SIP session establishment.

The UDP protocol number (the protocol number used in IP packets to indicate that UDP protocol is being transported) shall be protocol number 17, as registered with Internet Assigned Numbers Authority (IANA).

SCM-010290 [Required: SCIP/V.150.1 EI] When an SCIP/V.150.1 EI transitions the media stream between a normal session using SRTP and a secure session using SPRT, the SCIP/V.150.1 EI shall use the same UDP port numbers and UDP protocol number (17) for both the normal session and the secure session, so that the media stream transition is transparent to the SBC (when the SBC is located in the media stream for those sessions).

SCM-010300 [Required: SCIP/V.150.1 EI] The SCIP/V.150.1 EI shall not use UC SIP and SDP to negotiate a new UDP port number when the call is changing from Audio mode (SRTP) and Modem Relay mode (SPRT), or from Modem Relay mode back to Audio mode.

SCM-010310 [Required: SCIP/V.150.1 EI] The SCIP/V.150.1 EI shall not use UC SIP and SDP to negotiate multiple UDP port numbers (one for audio (SRTP), another for mode transitions (SSE), and another for modem relay (SPRT)) during UC SIP session establishment.

The SCIP-215 allows this multiple UDP port number approach, but the SCIP/V.150.1 EI shall not use this approach because it adds complexity to session establishment, and has a negative effect on SBCs.

2.21.2.5 UDP Port Number for SRTCP Media Control Packets

SCM-010320 [Required: SCIP/V.150.1 EI] The SCIP/V.150.1 EI shall maintain, for the duration of a call, the UDP port number used for the SRTCP media control packets that are sent and received during the Audio mode (when the call is “in the clear”).

SCM-010330 This UDP port number shall be the UDP port number negotiated for SRTCP media control packets by the SCIP/V.150.1 EI and the remote party (SCIP/V.150.1 EI or remote SCIP/V.150.1 Gateway) using SDP during UC SIP session establishment.

SCM-010340 [Required: SCIP/V.150.1 EI] When a call transitions from Audio mode to Modem Relay mode, the SCIP/V.150.1 EI shall stop sending SRTCP packets, but maintain the UDP port number that had been used for exchanging SRTCP packets.

SCM-010350 [Required: SCIP/V.150.1 EI] If a call transitions from Audio mode to Modem Relay mode, and then later back to the Audio mode, the SCIP/V.150.1 EI shall resume sending and receiving SRTCP packets using the same UDP port number previously used in Audio mode for those packets.

2.21.2.6 Use of V.150.1 SSE Messages for Media Transitions Between Audio and Modem Relay

SCM-010360 [Required: SCIP/V.150.1 EI] Per Section 4, Information Assurance, SCIP/V.150.1 EIs shall protect audio and video media streams using SRTP when exchanging these media streams with SCIP/V.150.1 Gateways and other SCIP/V.150.1 EIs.

NOTE: When SCIP/V.150.1 EIs exchange modem relay media streams with SCIP/V.150.1 Gateways and other EIs, the modem relay media streams are sent over SPRT, and not sent over SRTP. As a result, these modem relay media streams are not protected by SRTP.

SCM-010370 [Required: SCIP/V.150.1 EI] When SCIP/V.150.1 EIs exchange RFC 2833 events and V.150.1 SSE messages with SCIP/V.150.1 Gateways and other EIs, these RFC 2833 events and SSE messages shall also be protected using SRTP. These messages and events shall not be exchanged using SPRT, and they shall not be exchanged using RTP without SRTP.

SCM-010380 [Required: SCIP/V.150.1 EI] For all IP-TDM interworking, TDM-IP interworking, and IP-IP calls, SCIP/V.150.1 EIs shall declare that they support audio, modem relay, SRTP, SSE, and SPRT in the original SDP offer (UC SIP INVITE message) and SDP answer (200 OK response) for each call. The SCIP/V.150.1 EIs shall not reserve any modem relay resource at this point, because the call will typically begin as an audio call, which does not require a modem relay resource.

SCM-010390 [Required: SCIP/V.150.1 EI] Once one end of the call decides to go secure, the SCIP/V.150.1 EI shall begin the process of changing the established media stream from audio media to modem relay media. The SCIP/V.150.1 EI shall begin this processing by exchanging SSE messages with the SCIP/V.150.1 Gateway or other SCIP/V.150.1 EI, per V.150.1 and SCIP-215.

SCM-010400 [Required: SCIP/V.150.1 EI] As part of the Audio-media-to-Modem-Relay-media conversion process, the SCIP/V.150.1 EI shall not send an outgoing UC SIP re-INVITE message that requests Audio-to-Modem-Relay media conversion.

SCM-010410 [Required: SCIP/V.150.1 EI] As part of the Audio-media-to-modem-relay-media conversion process, the SCIP/V.150.1 EI shall not require the receipt of an incoming UC SIP re-INVITE message that requests Audio-to-Modem-Relay media conversion.

SCM-010420 [Required: SCIP/V.150.1 EI] The SCIP/V.150.1 EI shall not reserve and allocate its modem relay resources for the media stream for this call until the SSE message exchange for Audio-to-Modem-Relay media conversion has begun.

SCM-010430 [Required: SCIP/V.150.1 EI] Once one end of the call decides to return to “voice in the clear,” the SCIP/V.150.1 EI shall begin the process of changing the established media stream from modem relay media to audio media. The SCIP/V.150.1 EI shall begin this processing by exchanging SSE messages with the SCIP/V.150.1 Gateway or other SCIP/V.150.1 EI, per V.150.1 and SCIP-215.

SCM-010440 [Required: SCIP/V.150.1 EI] As part of the Modem-Relay-media-to-Audio-media conversion process, the SCIP/V.150.1 EI shall not send an outgoing UC SIP re-INVITE message that requests Modem-Relay-to-Audio media conversion.

SCM-010450 [Required: SCIP/V.150.1 EI] As part of the Modem-Relay-media-to-Audio-media conversion process, the SCIP/V.150.1 EI shall not require the receipt of an incoming UC SIP re-INVITE message that requests Modem-Relay-to-Audio media conversion.

SCM-010460 [Required: SCIP/V.150.1 EI] The SCIP/V.150.1 EI shall not release and de-allocate its modem relay resource for the media stream for this call, until the SSE message exchange for Modem-Relay-to-Audio media conversion has begun.

SCM-010470 [Required: SCIP/V.150.1 EI] The SCIP/V.150.1 EIs shall still be able to send and receive UC SIP re-INVITE messages during an audio call. (For example, the EI can use the UC SIP re-INVITE message to request an audio codec change during the audio/clear voice portion of a call when the EI is using G.711 for audio media but then asks the far end to use G.729 for audio media instead.) When the EI includes modem relay media information in an UC SIP re-INVITE message, the EI shall make sure that this is the same modem relay information that was present in the initial UC SIP INVITE message or 200 (OK) response that established the call. In this way, the UC SIP re-INVITE message is not used to request an Audio-to-Modem-Relay transition.

2.21.2.7 Going Secure, Glare Conditions, and Modem Relay Preferred Devices

SCM-010480 [Required: SCIP/V.150.1 EI] The calling or called SCIP/V.150.1 EI shall be able to initiate going secure. The calling or called SCIP/V.150.1 EI shall be able to send an ANS signal towards the far-end SCIP endpoint (MG or EI).

SCM-010490 [Required: SCIP/V.150.1 EI] If a glare condition results from an SCIP/V.150.1 EI initiating going secure and sending an ANS signal toward the far-end SCIP endpoint (MG or EI) at the same time that the far endpoint initiates going secure and sending an ANS signal to the SCIP/V.150.1 EI, then the SCIP/V.150.1 EI and the far-end SCIP endpoint should both back off their request and try again later.

SCM-010500 [Required: SCIP/V.150.1 EI] An SCIP/V.150.1 EI operating as a SCIP MRP device shall automatically transition from the audio state to the modem relay state upon the SCIP call being answered. This means that the first media stream packet sent by the MRP device shall be a Secure RTP (SRTP) packet containing an IETF RFC 2833 message indicating that an ANS, /ANS, ANSam, or /ANSam Event is being signaled.

This also means that the first media stream packet received by the MRP device (i.e., sent to the MRP device by the other V.150.1 device on the call) shall be an SRTP packet containing an SSE message indicating a transition from audio to modem relay (Event Code 3). Once this transition is successful, the MRP device shall begin sending SPRT packets containing SCIP protocol information (secure voice or secure data media).

If the MRP device receives an RFC 233 message containing an ANS, /ANS, ANSam, or /ANSam Event before that device sends its own RFC 2833 message and ANS, /ANS, ANSam, or /ANSam Event, the MRP device shall send an SRTP packet back to the other V.150.1 device, containing an SSE message indicating a transition from audio to modem relay (Event Code 3). Once this transition is successful, the MRP device shall begin sending SPRT packets containing SCIP protocol information (secure voice or secure data media).

2.21.3 SCIP/V.150.1 EI Requirements Using SCIP-214.2 Protocol

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

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

Support for SCIP/V.150.1 EIs using SCIP-214.2 is Optional. If SCIP-214.2 is supported then the following conditional requirements must be met.

SCM-010510 [Conditional: SCIP/V.150.1 EI] If the SCIP/V.150.1 EI supports secure communication using SCIP over Secure RTP, the SCIP/V.150.1 EI shall support all of the mandatory requirements in NSA document SCIP 214.2 with the following qualification:

- a. SCIP 214.2 allows RTP to be used as the media transport protocol for the two EIs. Since UC uses Secure RTP (SRTP) as the media transport protocol instead of RTP, SCIP/V.150.1 EIs shall also use SRTP as the media transport protocol, when exchanging SCIP media with another using SCIP-214.2. In other words, SCIP/V.150.1 EIs shall support SCIP over RTP per SCIP-214.2, except that SRTP shall be used to carry SCIP instead of RTP.

SCM-010520 [Conditional: SCIP/V.150.1 EI] The SCIP/V.150.1 EI shall use the payload type of “scip” in SDP attachments in UC SIP signaling to indicate that it supports SCIP over SRTP media using SCIP-214.2.

SCM-010530 [Conditional: SCIP/V.150.1 EI] Consistent with SCIP-214.2, the SCIP/V.150.1 EI shall “go secure” when one of the following conditions is met:

- a. When the two EIs negotiate the “scip” payload type to be the only selected codec.
- b. When the two EIs negotiate the “scip” payload type to be one of several selected codecs, and the first RTP packet with payload type “scip” is received from the other EI.

SCM-010540 [Conditional: SCIP/V.150.1 EI] Consistent with SCIP-216 and SCIP-215 requirements preventing the use of UC SIP re-INVITE or UPDATE messages for “clear voice” to “secure voice” transitions, the SCIP/V.150.1 EI shall not use UC SIP re-INVITE or UPDATE messages to perform “clear voice” to “secure voice” transitions, or to perform “secure voice” to “clear voice” transitions. The SCIP/V.150.1 EIs shall use the media stream methods defined in SCIP-214.2 to perform these transitions, and shall not use UC SIP signaling messages for this purpose.

As a result, SCIP/V.150.1 EIs that support SCIP-214.2 shall declare support for the “scip” payload type in the first UC SIP message in the SDP Offer-Answer exchange (e.g., in the INVITE message or in the 180 (Ringing) response).

SCM-010550 [Conditional: SCIP/V.150.1 EI] The SCIP/V.150.1 EIs shall use the following:

- a. One UDP port number for SRTP media packets for both “clear voice” and “secure voice.”
- b. A separate UDP port number for SRTCP media control packets for both “clear voice” and “secure voice.”

2.22 REQUIREMENTS FOR SUPPORTING UC SIP-BASED ETHERNET INTERFACES FOR VOICEMAIL SYSTEMS

SC and SS support for UC SIP-Based Ethernet Interfaces for voicemail systems (including Unified Messaging systems and ARDs) is optional; if such an interface is supported then the following conditional requirements specify how it is to be implemented.

SCM-010560 [Conditional: SC, SS] If a UC SIP-Based Ethernet Interface for voicemail systems is supported, then the SC and SS shall support all mandatory requirements in RFC 3842. Per this RFC:

“Message Waiting Indication is a common feature of telephone networks. It typically involves an audible or visible indication that messages are waiting, such as playing a special dial tone (which in telephone networks is called message-waiting dial tone), lighting a light or indicator on the phone, displaying icons or text, or some combination.” This RFC “describes a Session Initiation (SIP) event package to carry message waiting status and message summaries from a messaging system to an interested User Agent.”

SCM-010570 [Conditional: SC, SS] If a UC SIP-Based Ethernet Interface for voicemail systems is supported, then the SC and SS shall support the use of RFC 3842 Message Waiting Indication (MWI) for “tandeming” message waiting indications between Voicemail Systems, SSs, and SCs that are subtended from the SSs. The SC and SS shall support transmission of RFC 3842 MWIs in the Voicemail System => SS => SC direction, and transmission of any RFC 3842 MWI responses in the SC => SS => Voicemail System direction.

SCM-010580 [Conditional: MSC, SSC] If a UC SIP-Based Ethernet Interface for voicemail systems is supported, then Master SCs and Subtended SCs shall also support RFC 3842 MWI for “tandeming” message waiting indications between SSs, MSCs, and SSCs. MSCs and SSCs shall support transmission of RFC 3842 MWIs in the SS => MSC => SSC direction, and transmission of any RFC 3842 MWI responses in the SSC => MSC => SS direction.

SCM-010590 [Conditional: SC, SS] If a UC SIP-Based Ethernet Interface for voicemail systems is supported, then the SC and SS shall support all mandatory requirements in IETF Internet RFC 5806, Diversion Indication in SIP. Per this Internet RFC:

“This document proposes an extension to the Session Initiation Protocol (SIP). This extension provides the ability for the called SIP User Agent to identify from whom the call was diverted and why the call was diverted. The extension defines a general header, Diversion, which conveys the diversion information from other SIP user agents and proxies to the called user agent. This extension allows enhanced support for various features, including Unified Messaging, Third-Party Voicemail, and Automatic Call Distribution (ACD). SIP user agents and SIP proxies which receive diversion information may use this as supplemental information for feature invocation decisions.”

SCM-010600 [Conditional: SC, SS] If a UC SIP-Based Ethernet Interface for voicemail systems is supported, then the SC and SS shall support all the mandatory requirements in RFC 4244. Per this RFC:

“This document defines a standard mechanism for capturing the history information associated with a Session Initiation Protocol (SIP) request. This capability enables many enhanced services by providing the information about how and why a call arrives at a specific application or user.

This RFC defines a new optional SIP header, History-Info, for capturing the history information in requests.”

SCM-010610 [Conditional: SC, SS] If a UC SIP-Based Ethernet Interface for voicemail systems is supported, then the SC and SS shall support all of the mandatory requirements in RFC 3725. Per this RFC:

“Third party call control refers to the ability of one entity to create a call in which communication is actually between other parties. Third party call control is possible using the mechanisms specified within the Session Initiation Protocol (SIP). However, there are several possible approaches, each with different benefits and drawbacks. This RFC provides best current practices for the usage of SIP for third party control.”

2.22.1 Requirements for Supporting UC SIP Message Waiting Indications on UC SIP EIs, TAs, and IADs

SCM-010620 [Conditional: SC, UEI, TA, IAD] If a UC SIP-Based Ethernet Interface for voicemail systems is supported, then the SC, UEI, TA, and IAD shall support all of the mandatory requirements in the following:

- a. RFC 3842 for SIP Message Waiting Indication.
- b. RFC 5806 for Diversion Indication in SIP.
- c. RFC 4244 for SIP Request History Information.

In the case of TAs and IADs, this requirement only applies to TAs and IADs that support UC SIP on their IP side for signaling with the SC.

SCs shall be able to exchange SIP MWIs, SIP Diversion Indications, and SIP Request History Information with the UC SIP EIs, TAs, and IADs that they serve.

UC SIP EIs, TAs, and IADs shall be able to accept SIP MWIs, SIP Diversion Indications, and SIP Request History Information from the SCs that serve them, and relay the information in those SIP fields on to their end users.

For example, if an UC SIP EI, TA, or IAD receives an RFC 3842 SIP MWI from its SC, that UEI, TA, or IAD shall be able to provide a visual MWI (light a lamp, display an icon) and/or an audible MWI (burst of ringing, stutter dial tone) to the UC end user.

2.23 LOCAL ATTENDANT CONSOLE FEATURES

This section specifies requirements for a local attendant console or station on the SC.

2.23.1 Precedence and Preemption

SCM-010630 [Required: SC, SS] The attendant console shall interoperate with PBAS/ASAC as described in [Section 2.10.1](#), PBAS/ASAC.

The console shall be able to initiate all levels of precedence calls (i.e., ROUTINE through FLASH OVERRIDE).

SCM-010640 [Required: SC] The attendant console shall interoperate with MLPP as described in [Section 2.26.1](#), Multilevel Precedence and Preemption.

SCM-010650 [Required: SC, SS] When the attendant console receives a call at Precedence A and the attendant transfers the call to a destination at Precedence B, the resulting call should have the higher precedence between A and B.

2.23.2 Call Display

SCM-010660 [Required: SC, SS] The attendant console shall provide a visual display of each precedence level and the calling number, for incoming direct dialed calls to the attendant, and diverted calls to the attendant (e.g., calls that reach the attendant through PCD).

SCM-010670 [Conditional: SC, SS] If the SC or SS supports assignment of a CoS to an individual EI, then the attendant console also shall provide a visual display of the calling EI's CoS, for incoming direct dialed calls to the attendant and diverted calls to the attendant.

2.23.3 Class of Service Override

SCM-010680 [Conditional: SC, SS] If the SC or SS supports assignment of a Class of Service (CoS) to an individual EI, then this appliance and the attendant console shall give the attendant the ability to override any incoming call's calling party CoS (based on calling area or precedence) on a call-by-call basis.

The appliance and the attendant console shall also give the attendant the ability to override any diverting call's calling party CoS (based on calling area or precedence) on a call-by-call basis.

2.23.4 Busy Override and Busy Verification

SCM-010690 [Required: SC, SS] The appliance and the attendant console shall give the attendant the ability to verify and override a busy line condition. In commercial VoIP networks, attendant verification of a busy line is called Busy Line Verification (BLV), and attendant override of a busy line is called Emergency Interrupt. In the network, support for these BLV and Emergency Interrupt capabilities is

- a. **[Required]** when the "busy line" is an UC EI served by the local UC appliance.
- b. **[Optional]** when the "busy line" is an UC EI served by a remote UC appliance.

SCM-010700 [Required: SC, SS] If the attendant uses BLV on a called line, and that called line (called EI) is busy, the appliance and the attendant console shall give an audible and visual “called line busy” indication back to the attendant.

SCM-010710 [Required: SC, SS] The appliance and the attendant console shall prevent an attendant from activating BLV or Emergency Interrupt to called lines and called numbers that are located in the commercial network (the PSTN).

SCM-010720 [Required: SC, SS] The appliance and the attendant console shall give the attendant the ability to use Emergency Interrupt to interrupt an existing call on a busy line, and inform the busy user of a new incoming call. The appliance shall provide an override tone to the busy user before the attendant enters the conversation, and they shall repeat the tone periodically for as long as the attendant is connected to the busy user. The override tone can either be signaled from the appliance to the busy user’s EI and generated locally by that EI, or generated by the appliance’s media server and injected into the media streams to and from the busy user’s EI.

SCM-010730 [Required: SC, SS] The appliance shall give selected destination EIs the ability to be exempt from Emergency Interrupt and attendant break-in. In particular, it shall be possible for the appliance to preclude the BLV and Emergency Interrupt services from being applied to selected destination EIs (e.g., EIs that provide secure voice service).

2.23.5 Night Service

SCM-010740 [Required: SC, SS] The appliance and the attendant console shall have the ability to route all calls that are normally directed to the console to a separate night service deflection number. The night service deflection number shall be a fixed (preconfigured) or manually-selected DN.

2.23.6 Automatic Recall of Attendant

SCM-010750 [Required: SC, SS] When an attendant redirects an incoming call to a destination station, and that station is either busy or does not answer the call within a preset time, the appliance and the attendant console shall ensure that calling party on the redirected call is recalled automatically to the console.

SCM-010760 [Required: SC, SS] In this case, the appliance shall ensure that that the “recalled” call is returned to the console that originally processed the call. If that console is busy, the appliance shall ensure that the “recalled” calls are placed into the queue for that console. But if that console is out of service, then the appliance shall ensure that the “recalled” call is routed to another console on that appliance, if another console is available.

2.23.7 Calls in Queue to the Attendant

SCM-010770 [Required: SC, SS] The appliance and the attendant console shall have the ability to place calls (both directed to the attendant and diverted to the attendant) into a waiting queue. The appliance and the attendant console shall ensure that calls placed in queue to the attendant are retrieved by the attendant in order of their precedence level (i.e., FLASH OVERRIDE first, ROUTINE last) and the longest holding time within that precedence level.

SCM-010780 [Required: SC, SS] The appliance and the attendant console shall ensure that calls in the attendant queue are not lost when a console is placed out of service or has its calls forwarded to a night service deflection number. When the console is placed out of service or forwarded to night service while calls are in queue, the appliance and the console shall be capable of one of the following solutions to ensure that calls are not lost:

- a. All the existing calls in the queue shall be forwarded first to a separate DN for the centralized attendant (i.e., a different attendant at a different attendant console), and then on to the night service DN (if the centralized attendant activated night service deflection).
- b. All subsequent calls placed to the attendant console shall be forwarded first to the separate DN for the centralized attendant, and then on to the night service DN (if the centralized attendant activated night service deflection). For the existing calls in the queue, the attendant remains at the console and answers all these remaining calls (even though the attendant placed the console out of service or forwarded the console to night service deflection), thereby preventing any of the calls from being lost.

2.24 MSC AND SSC

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

The MSC and SSC requirements in this section apply to MSCs and SSCs in both Strategic (Fixed) networks and MSCSSCTactical (Deployable) networks.

If an SC product can be configured as a Master SC, the MSC requirements in this section apply. If an SC product can be configured as a Subtended SC, the SSC requirements in this section apply. Support for MSC and SSC configurations on an SC product, as specified in [Section 2.10](#), Session Controller, is optional.

SCM-010790 [Required: MSC, SSC] All SC requirements in this section and in all other sections apply to both MSCs and SSCs, unless an individual requirement indicates otherwise.

SCM-010800 [Required: MSC, SSC, PEI, UEI, ATA, IAD] End instruments that are served by an MSC shall be treated just like EIs that are served by SSCs. The MSC shall treat its EIs

(i.e., PEIs, UEIs, ATAs, IADs) in the same way that it would if it were operating as a SSC. The SSC shall treat its EIs (i.e., PEIs, UEIs, ATAs, IADs) in the same way that it would if it were operating as an MSC.

SCM-010810 [Required: MSC] The MSC shall adjudicate the enclave budget (the enclave ASAC budget between the MSC and its primary SS) between its SSCs. The MSC shall adjudicate the enclave ASAC budget in cases where this budget is nondirectional [**Required**] and directional [**Optional**].

SCM-010820 [Required: MSC] The MSC shall support at least one of two methods for adjudicating the enclave ASAC budget between its SSCs: the “Highest Priority Sessions” method and the “Strict Budget for All SCs” method. Support for either of these two methods is acceptable.

2.24.1 Highest Priority Sessions Method

SCM-010830 [Required: MSC] When processing outgoing call requests from its EIs, MGs, and its SSCs, and incoming call requests to its EIs, MGs, and its SSCs, the MSC shall always ensure that the highest precedence level sessions (i.e., P, I, F, FO) are served first over the MSC-to-SS interface. When call requests are received from or directed to the SSCs, the MSC shall always ensure that the highest precedence level sessions (i.e., P, I, F, FO) are served first, regardless of where the SSC is originated or terminated.

For example, assume a MSC with three SSCs, where the MSC-to-SS ASAC budget for voice is 28 voice sessions with no directionalization. Also, assume that each SSC is allowed up to 10 voice sessions (with no directionalization) on its SSC-to-MSC interface. The SSCs could not all simultaneously be allowed up to 10 voice sessions on the MSC-to-SS interface in this case; two requests would be blocked.

SCM-010840 [Required: MSC] When the access link from the MSC to the SS is “full,” the MSC shall allow additional higher precedence sessions (destined for outside of the enclave, or arriving from outside of the enclave) to succeed by preempting existing lower precedence sessions on the access link. The MSC shall preempt the lower precedence sessions and establish the higher precedence sessions, independent of whatever SSC originated these sessions.

SCM-010850 [Required: MSC] In this case, the MSC shall block ROUTINE precedence sessions on the access link that are to or from the following:

- a. End users on the MSC.
- b. End users on any of the SSCs, once the access link session budget (ASAC budget) is met.

2.24.2 Strict Budget for All SCs Method

SCM-010860 [Required: MSC] When processing outgoing call requests from its EIs, MGs, and its SSCs, and incoming call requests to its EIs, MGs, and its SSCs, the MSC shall always ensure

that each SSC is “guaranteed” a fixed subset of the ASAC budget on the MSC-to-SS access link. When call requests are received from or directed to the SSCs, the MSC shall always ensure that calls to or from each SSC are allowed to complete, as long as the source or destination SSC is below its subset of the ASAC budget (its “Strict Budget”) for the access link.

SCM-010870 [Required: MSC] When the source or destination SSC is at or above its Strict Budget for the access link, the MSC shall do the following:

- a. Block all ROUTINE voice session requests on the access link that are to or from end users on that SSC, as long as the SSC is at or above its Strict Budget.
- b. Allow any precedence session requests to or from end users on that SSC, but only if there is an existing session within that SSC’s Strict Budget that is of a lower precedence level and can, therefore be preempted.
- c. If there is no existing lower precedence session that can be preempted, the MSC shall block the precedence session request, even if there are lower precedence sessions established to or from the other SSCs that could be preempted.

For example, assume a MSC with three SSCs, where the MSC-to-SS ASAC budget for voice is 30 voice sessions with no directionalization. Also assume that each SSC is allowed up to 10 voice sessions (with no directionalization) on its SSC-to-MSC interface. Each of the SSCs could also be allowed up to 10 voice sessions on the MSC-to-SS interface in this case. No session requests to or from a SSC would be blocked, unless that SSC was operating at or above its “Strict Budget” of 10 voice sessions for the access link.

SCM-010880 [Required: MSC] When the access link from the MSC to the SS is “full,” the MSC shall allow additional higher precedence sessions (destined for outside of the enclave, or arriving from outside of the enclave) to succeed by preempting existing lower precedence sessions on the access link, but only if the higher and lower precedence sessions are both within the same Strict Budget and associated with the same SSC. If these sessions are associated with the same SSC, then the MSC shall preempt the lower precedence sessions and establish the higher precedence sessions. If these sessions are not associated with the same SSC, then the MSC shall block the higher precedence sessions.

SCM-010890 [Required: MSC] The MSC shall also block ROUTINE precedence voice sessions to or from any SSCs, once the Strict Budget for that SSC is met.

SCM-010900 [Required: MSC] The MSC shall not allow precedence sessions to or from one of the SSCs to complete, if the Strict Budget for that SSC is met, and there are no existing lower precedence sessions within that Strict Budget that can be preempted.

2.24.3 EMS Access, UC SIP Signaling, Enclave Budgets, and MG Connections

SCM-010910 [Required: MSC, SSC] The MSC and the SSCs shall all be capable of directly connecting to both of the following:

- a. Local EMS.
- b. Remote VVoIP EMS.

SCM-010920 [Required: MSC, SSC] The MSC is not required to provide the local or remote EMS with an aggregated NM view of the SSCs. The MSC shall provide the local or remote EMS with an individual NM view of itself. Each SSC shall provide the local or remote EMS with an individual NM view of itself.

SCM-010930 [Required: MSC, SSC] The MSC and the SSCs shall be capable of communicating with each other using an UC SIP protocol per UC SIP 2013.

In cases where the MSC and the SSC are from the same SC vendor, the MSC and the SSCs may communicate with each other using a proprietary signaling protocol.

SCM-010940 [Required: MSC, SSC] All UC SIP signaling that either 1) leaves the enclave for an external destination, or 2) arrives at the enclave from an external source shall pass through the MSC. The SSCs shall not support their own UC SIP or proprietary signaling links to locations outside the enclave. The SSCs shall exchange all UC SIP or proprietary signaling with the MSC within the enclave, and the MSC shall exchange all UC SIP signaling with locations outside the enclave.

This approach allows for both 1) multiple SC vendors within the enclave and 2) a single SC vendor's integrated solution within the enclave.

SCM-010950 [Required: MSC] Each MSC shall maintain two separate enclave budget counts as follows:

- a. Intraenclave Budget Count. This shall be a count of all VVoIP calls traversing the MSC that both originate and terminate within the enclave. This count shall include both calls within the MSC itself (EI-to-EI calls, EI-to-MG calls), and calls to or from all of the SSCs within the enclave.

NOTE: This count shall be based on local traffic engineering for the enclave, and shall not be associated with the access link budget on the MSC-to-SS interface.

- b. Interenclave Budget Count. This shall be a count of all VVoIP calls that either enter the MSC and originated from outside the enclave, or leave the MSC and terminate outside of the enclave. This count shall include incoming and outgoing calls to or from the MSC itself, and incoming and outgoing calls to or from all SSCs within the enclave.

SCM-010960 [Conditional: MSC, SSC] If all connections between the enclave and the local PSTN are made through the MG of the MSC, then all EIs on the MSC, and all EIs on each SSCs shall originate and receive commercial calls from the PSTN PRI/CAS trunk group at the MSC's MG. (This arrangement is desired and simplifies location services that are based on the commercial PSTN numbers of the various EIs in the enclave.)

SCM-010970 [Conditional: MSC, SSC] If connections are made between the enclave and the local PSTN through the MGs of SSCs, then the EIs of a single SSC shall originate and receive calls from the PSTN PRI/CAS trunk group at that SSC's MG.

SCM-010980 [Required: MSC, SSC] The MSC in an enclave shall provide the only TDM connection (T1.619 PRI, CAS, or SS7 trunk group) to the DISN TDM infrastructure (i.e., DSN MFSs, Tandems, EOs, SMEOs, or PBXs) in the enclave. The SSCs in an enclave shall not provide any TDM connections to the DISN TDM infrastructure in the enclave.

2.25 MSC, SSC, AND DYNAMIC ASAC REQUIREMENTS IN SUPPORT OF BANDWIDTH-CONSTRAINED LINKS

This section provides requirements for MSCs, SSCs, and Dynamic Assured Services Admission Control (DASAC), and as such augments the following:

- UC Framework 2013, Section 2.8, Session Controller.
- [Section 2.3](#), ASAC.
- [Section 2.24](#), MSC and SSC.

The SC requirements apply to both MSCs and SSCs unless indicated otherwise.

This section focuses on the Deployable (Tactical) use of the MSC/SSC architecture and the introduction of DASAC. Dynamic ASAC enables an SC to admit, block, or preempt new voice and video calls based on the communications capacity (bps) required for the call and the link capacity available to support the call. Dynamic ASAC will augment the current ASAC approach in which SCs admit calls based on a call budget. Dynamic ASAC will be applied independently to voice and video calls.

The requirements for an MSC and its SSCs in support of bandwidth-constrained links apply to both Deployable (Tactical) SCs and Fixed (Strategic) SCs (i.e., the requirements are not unique to Deployable SCs).

Please note that “bandwidth” has two definitions per the online version of Merriam-Webster's dictionary (<http://www.merriam-webster.com/dictionary/bandwidth>):

“1: a range within a band of wavelengths, frequencies, or energies...

2: the capacity for data transfer of an electronic communications system ... <a bandwidth of 56 kilobits per second>”

The Deployed (Tactical) wireless UC community will be one of the primary audiences for this section. This community generally uses “bandwidth” per the first definition but this section uses “bandwidth” per the second definition according to its usage throughout the rest of this section.

2.25.1 MSC and SSC Architecture

Within Deployable (Tactical) domains, calls typically involve multiple bandwidth constrained links. Each such link must be subject to DASAC. These links typically are wireless (e.g., satellite, radio) in nature. Deployable (Tactical) sites generally exist within a tiered command and control hierarchy.

2.25.1.1 Master/Subtended Architecture Applies to Both Voice and Video

SCM-010990 [Required: Deployable (Tactical) SC – Optional: Fixed (Strategic) SC] A Deployable (Tactical) SC that supports the MSC/SSC functionality shall support both voice and video services.

2.25.1.2 MSC/SSC and DASAC

SCM-011000 [Required: Deployable (Tactical) SC – Optional: Fixed (Strategic) SC] The product shall support DASAC; see [Section 2.25.2](#), Dynamic ASAC.

2.25.1.3 Directionalization Budget Inheritance

SCM-011010 [Optional: Deployable (Tactical) SC, Fixed (Strategic) SC] The product may inherit the voice directionalization ASAC budget requirements (i.e., IPB, IPBi, IPBo) from this entire section and UC SIP 2013, for both voice and video.

2.25.1.4 Minimum Number of Supportable SSCs per MSC

SCM-011020 [Required: Deployable (Tactical) SC – Optional: Fixed (Strategic) SC] A product that supports the MSC functionality shall support DASAC for a minimum of 10 SSCs.

2.25.1.5 MSC Also an SSC

SCM-011030 [Required: Deployable (Tactical) SC – Optional: Fixed (Strategic) SC] A product that acts as an MSC shall be capable of acting simultaneously as an SSC.

2.25.1.6 Two Budgets per Link per Media Type

SCM-011040 [Required: Deployable (Tactical) SC – Optional: Fixed (Strategic) SC, SS] An MSC/SSC pair will apply their respective DASAC budgets to their respective ends of the shared link. Likewise, the SS/MSC pair will apply their respective DASAC budgets to their respective ends of the shared link. During UC SIP call processing a given link and its budget are inferred by the combination of the sender’s CCA-ID and the receiver’s CCA-ID.

2.25.1.7 *Distinct Voice and Video DASAC Budgets*

SCM-011050 [Required: Deployable (Tactical) SC – Optional: Fixed (Strategic) SC] The product shall be able to support an independent DASAC budget for voice and an independent DASAC budget for video.

2.25.1.8 *Long Locals*

SCM-011060 [Optional: Deployable (Tactical) SC] The product may support long locals where the EIs and the SC physically reside at separate sites. The Deployable (Tactical) LAN's SC and SBC also may reside at separate sites.

2.25.1.9 *Logical SCs*

SCM-011070 [Optional: Deployable (Tactical) SC] A single physical product may provide two or more logical SCs supporting two or more Deployable (Tactical) sites. Each logical SC is a software-based partition of the single physical SC asset. Each logical SC will have its own IP address and its own CCA-ID.

2.25.2 *Dynamic ASAC*

This section defines requirements for providing the Dynamic ASAC (DASAC) capability.

SCM-011080 [Required: SS – Required: Deployable (Tactical) SC – Optional: Fixed (Strategic) SC] The product shall manage the DASAC budget in a manner similar to that described in [Section 2.3](#), ASAC, except that the budget shall be based on the amount of bandwidth (bps) available to support a new session.

SCM-011090 [Required: SS – Required: Deployable (Tactical) SC – Optional: Fixed (Strategic) SC] The product shall use a method of establishing and managing the DASAC budget per SC Path. The capacity calculation shall be based on the bottleneck communications link along the SC Path.

The DASAC budget shall be based on the following metrics derived from the parameters shown in [Table 2.25-1](#), EISC Estimation Parameters. A product with DASAC capability shall support an EI Session Capacity (EISC) estimation table for each SC Path and each codec class that operates on the SC Path. A codec class is defined by the codec type PPS produced by the codec.

Table 2.25-1. 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

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

The parameters in each EISC estimation table shall be used to determine the following:

1. EI Session Capacity (EISC). The bandwidth required (in bps) for a session. The EISC shall be computed by the product each time it detects signaling for a new session or a change in codec parameters for an ongoing session.
2. Transmission Link Session Capacity (TLSC). The capacity (bps) of the bottleneck link associated with the SC Path. The TLSC is a pre-provisioned parameter entered for each SC Path link via NM commands. The TLSC does not include an allocation for session signaling.

Session signaling must be provisioned separately as part of traffic engineering for the bottleneck link on the path.

3. Available Link Session Capacity (AVSC). The capacity (bps) currently available for sessions on the SC Path. The AVSC shall be calculated each time during:
 - a. The session establishment UC SIP dialog (specifically the UC SIP message containing the SDP answer).
 - b. Mid-session re-INVITE dialog based on a mid-session codec change (specifically the UC SIP message containing the new SDP answer to the new offer).
 - c. Session teardown (specifically based on SC detecting the UC SIP 200 (OK) for the BYE).

The AVSC is calculated as follows:

AVSC = Transmission Link Session Capacity (TSC). The sum of EISCs for all sessions in progress and in the process of being established on the SC Path.

4. Determination of TSC depends on the following:
 - a. The allocation of capacity to the bottleneck router queue within the SC Path.
 - b. The portion of that capacity that is reserved for voice and video applications that is not under the control of the SC.

Parameters 1 through 3 in [Table 2.25-1](#), EISC Estimation Parameters, are dynamic; the product shall calculate these parameters on a session-by-session basis. Parameters 4 through 9 are preloaded into the product based on traffic engineering analysis of the link.

[Figure 2.25-1](#), UC SIP Triggers for AVSC, illustrates the UC SIP triggers for the AVSC calculations. For reasons of simplification, it assumes the EIs are UC SIP enabled. It is also assumed 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.

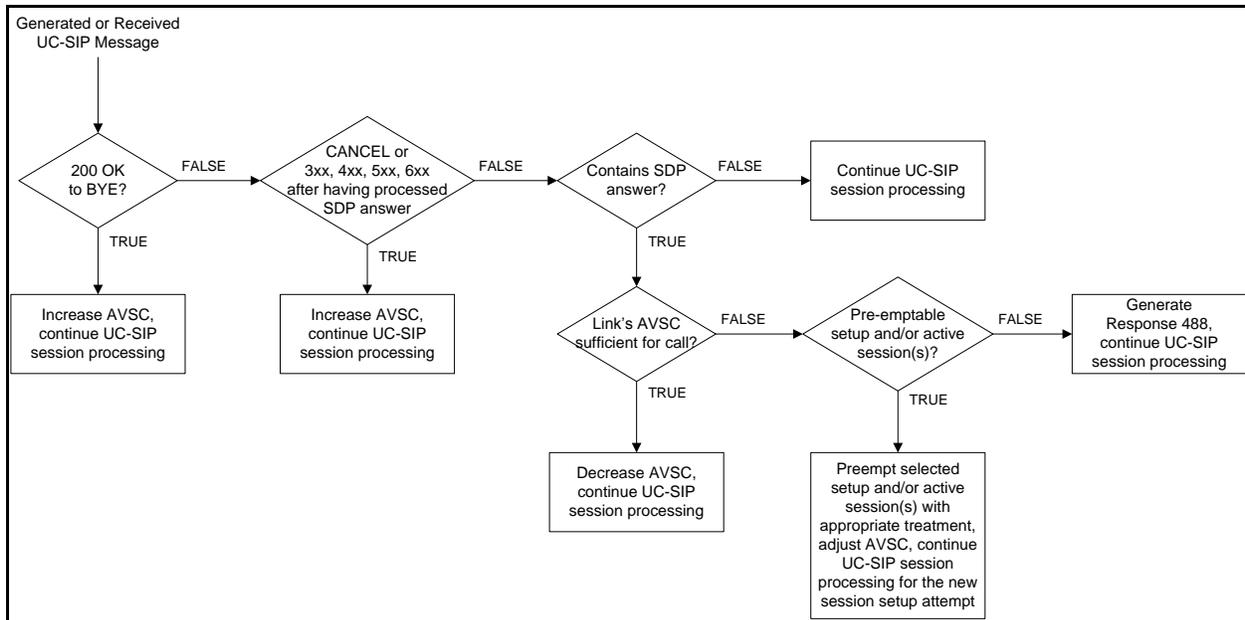


Figure 2.25-1. UC SIP Triggers for AVSC

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 UC 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 \leq 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 preemptible 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.

SCM-011100 [Required: SS – Required: Deployable (Tactical) SC – Optional: Fixed (Strategic) SC] The product shall support DASAC for the following types of session packet flows:

- a. Pass-through flows, where the bearer packets are not modified after they are generated in either an SC or EI.
- b. Voice/Video multiplexed flows where payloads from different flows are combined in a new packet to reduce the effect of IP overhead before transmission on a bottleneck link.

- c. Header compressed flows where all or some of the IP/UDP/RTP headers are compressed before transmission on a bottleneck link.
- d. Tunneled flows, where the packet flows described earlier are also subject to tunneling, for example, using IPsec.

SCM-011110 [Required: SS – Required: Deployable (Tactical) SC – Optional: Fixed (Strategic) SC] The product shall use parameters 1 through 9 in Table 2.25-1, EISC Estimation Parameters, as appropriate, to calculate the total EISC and AVSC. Parameter values 1 through 3 shall be determined by the product (SC or SS). Parameters 4 through 9, as appropriate, shall be determined before operation and loaded into the product (SC or SS) database. These values shall be chosen conservatively to ensure that there is no case where more sessions are admitted than can be supported by the SC Path.

SCM-011120 [Required: SS – Required: Deployable (Tactical) SC – Optional: Fixed (Strategic) SC] The product shall, on a session-by-session basis, scan the SDP messages, extract the EISC codec rate and PPS parameters from each SDP Answer message, and store these parameters in the appropriate DASAC table, for each session in progress.

SCM-011130 [Required: SS – Required: Deployable (Tactical) SC – Optional: Fixed (Strategic) SC] The product shall be able to support all codecs defined in [Section 2.9.1.3](#), Audio Codecs, Voice Instruments, [Section 2.9.3.3](#), Video Codecs (Including Associated Audio Codecs), and Appendix A Section A7.5.4 Codec Translation Functional.

SCM-011140 [Required: SS – Required: Deployable (Tactical) SC – Optional: Fixed (Strategic) SC] If the product does not have an entry for the negotiated audio codec or for the PPS for the session, the product shall set EISC at 110 Kbps.

SCM-011150 [Required: SS – Required: Deployable (Tactical) SC – Optional: Fixed (Strategic) SC] If the product supports an ongoing session in which the EIs can re-negotiate audio or video codec changes at the bearer layer (e.g., modem protocol), the product shall set EISC at the highest bit rate that can be re-negotiated by the EIs mid-session via the bearer layer.

SCM-011160 [Required: SS – Required: Deployable (Tactical) SC – Optional: Fixed (Strategic) SC] If the values of parameters 4 through 7 are not explicitly entered in the table, the product shall use the default parameters listed in [Table 2.25-1](#), EISC Estimation Parameters.

SCM-011170 [Required: SS – Required: Deployable (Tactical) SC – Optional: Fixed (Strategic) SC] The product shall not use silence suppression, also known as voice activity detection, as a factor in calculating EISC for voice sessions.

SCM-011180 [Required: SS – Required: Deployable (Tactical) SC – Optional: Fixed (Strategic) SC] Each DASAC product also shall be provisioned with session budget parameters which provide an absolute limit on the number of voice and video sessions accepted in either direction for each link.

2.26 OTHER UC VOICE

2.26.1 Multilevel Precedence and Preemption

NOTE: In general, the Multilevel Precedence and Preemption (MLPP) requirements in this section apply to IP-based Precedence-Based Assured Services (PBAS), i.e., the use of the term “MLPP” in this section is not meant to restrict these requirements to services provided by TDM-based networks.

SCM-011190 [Required: UEI, SC, SS – Optional: PEI] The MLPP service applies to the MLPP service domain only. Connections and resources that belong to a call from an MLPP subscriber shall be marked with a precedence level and domain identifier (consistent with ANSI Standards T1.619-1992 and T1.619a-1994) and shall only be preempted by calls of higher precedence from MLPP users in the same MLPP service domain

2.26.1.1 Precedence Levels

SCM-011200 [Required: UEI, SC, SS – Optional: PEI] The SC, SS, PEI and UEI shall provide five precedence levels. The precedence levels listed from lowest to highest are ROUTINE, PRIORITY, IMMEDIATE, FLASH, and FLASH OVERRIDE.

2.26.1.2 Invocation and Operation

SCM-011210 [Required: UEI, SC, SS – Optional: PEI] The precedence level of a call is selected by the subscriber on a per call basis. The subscriber may select any precedence level up to and including his or her maximum authorized precedence level. The network at the subscriber’s originating interface ensures that the selected precedence level does not exceed the maximum level assigned to that telephone number. Once set for a call, this precedence level cannot be changed. In addition, a connection between two UC subscribers shall not have different precedence levels. A call will default automatically to the ROUTINE precedence unless a higher precedence is dialed. The DSN Worldwide Numbering and Dialing Plan is described in [Section 2.18.1](#), DSN Worldwide Numbering and Dialing Plan.

During a call setup, if there is a shortage of network resources, the SC or SS shall determine whether resources are held by calls of lower precedence. If there is a shortage, the SC or SS shall release the lowest of these lower precedence call(s) and seize the resources required to set up the higher precedence call. These resources include calls on trunks between an SC and a DSN circuit switch.

The preemption operation depends on whether the SC/SS needs to preempt a common network resource, such as one of the SC to DSN switch trunks that is currently being used by a different subscriber than the intended called subscriber.

If a called user is to be preempted, both the called party and its connected-to parties shall be, at a minimum, audibly notified of the preemption using the preemption tone in [Table 2.9-2](#), UC

Information Signals, and the existing MLPP call shall be cleared immediately. The called party must acknowledge the preemption by going “on-hook” or pressing a feature button, before the higher precedence call is completed. Then the called party is offered the new MLPP call.

After attempting a precedence call, the calling party shall receive an audible ringback precedence call tone when the call is offered successfully to the called party as a precedence call. These alerting tones are provided in [Table 2.9-2](#), UC Information Signals.

The calling party shall receive a BPA, as shown in [Table 2.9-3](#), Announcements, for the following reasons:

- Equal or higher precedence calls have prevented completion.
- No idle network resources are available to make a connection to the dialed number and the called subscriber belongs to a network that does not support preemption.

If the requested precedence level is not subscribed to, the calling party shall receive a UPA, as shown in [Table 2.9-3](#), Announcements.

The calling party shall receive a BNEA, as shown in [Table 2.9-3](#), Announcements, if the called party is assigned as nonpreemptable. Precedence calls (i.e., PRIORITY and above) that are not responded to by the called party (e.g., call unanswered) shall be diverted IAW [Section 2.2.10](#), Precedence Call Diversion. If precedence call waiting has been invoked, these calls shall be handled IAW [Section 2.2.3](#), Precedence Call Waiting. Unanswered calls placed at a ROUTINE precedence level shall continue to ring.

2.26.1.3 Preemption in the Network

SCM-011220 [Required: UEI, TA, IAD, SC, SS – Optional: PEI] The following sections describe the treatment for precedence calls at the called party’s interface and applies to both analog and digital (ISDN and non-ISDN) terminating Customer Premises Equipment (CPE).

2.26.1.3.1 Network Facilities Active with Lower Precedence Calls

SCM-011230 [Required: UEI, SC, SS – Optional: PEI] For PRIORITY precedence calls and above, during call setup, if there is a shortage of a network resource, then the network shall determine whether resources are held by calls of lower precedence. The network shall release the lowest of these lower precedence call(s) and seize the necessary resources that are required to set up the higher precedence call. These resources include calls on trunks between an SC and a DSN circuit switch.

When a common network resource is preempted, all existing parties shall receive a preemption tone (see [Table 2.9-2](#), UC Information Signals) and the existing connection is disconnected. The new higher precedence call is set up using the preempted resource.

2.26.1.3.1.1 CANCEL To/CANCEL From

SCM-011240 [Required: SC, SS] Requirements for the CANCEL to/CANCEL from feature shall be IAW Telcordia Technologies GR 477-CORE, Section 6, NTM Manual Controls.

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

2.26.1.3.2 *Network Facilities Active With Equal or Higher Precedence Call*

SCM-011250 [Required: UEI, SC, SS – Optional: PEI] If all network resources required to complete a precedence call are busy with equal or higher precedence calls, the calling user shall be sent the BPA (see [Table 2.9-3](#), Announcements).

2.26.1.3.3 *MLPP Trunk Selection (Hunting)*

SCM-011260 [Required: SC MG, SS MG] The UC route selections shall be based on Precedence Level/Calling Area (PL/CA) classmarks for both voice-grade and data-grade trunk groups. The UC hunting sequence shall be capable of being varied depending on the route. Hunt sequences shall be capable of scanning data-grade trunk groups for voice-grade calls. The hunting sequence shall be capable of searching all trunks. First, the hunting sequence shall examine the route digit so that, for data calls only, data-grade trunks shall be searched. For voice-grade calls, all trunks shall be searched.

2.26.1.3.3.1 Hunt Sequence for Trunks

SCM-011270 [Required: SC MG, SS MG] The SCs/SSs shall route UC calls to trunks that have classmarks to indicate the maximum PL/CA permitted. Calls shall not be originated over trunk groups when the call attempt exceeds the precedence level or calling area.

2.26.1.3.3.1.1 ROUTINE Precedence Calls

SCM-011280 [Required: SC MG, SS MG] For ROUTINE precedence calls, the SC/SS shall use an idle search on all programmed routes to the call destination. Failing to find an idle trunk, the SC/SS shall provide a trunk busy tone to the caller.

2.26.1.3.3.1.2 Precedence Calls Above ROUTINE Precedence

SCM-011290 [Required: SC MG, SS MG] The SC/SS shall provide for two methods of trunk route selection for precedence level calls above the ROUTINE precedence. Either method can be assigned to a destination route based on the UC Area Code (KXX) and/or UC Switch Code (KXX) of the call. In each method, trunks shall be tested individually for idle or busy conditions. If preemption is required, only a call of the lowest level of precedence, lower than the dialed precedence, shall be preempted.

2.26.1.3.3.1.2.1 Method 1

SCM-011300 [Required: SC MG, SS MG] In method 1, the SC/SS shall perform an idle search on the direct route and all alternative routes, as shown in [Figure 2.26-1](#), Example Hunt Sequence for Method 1.

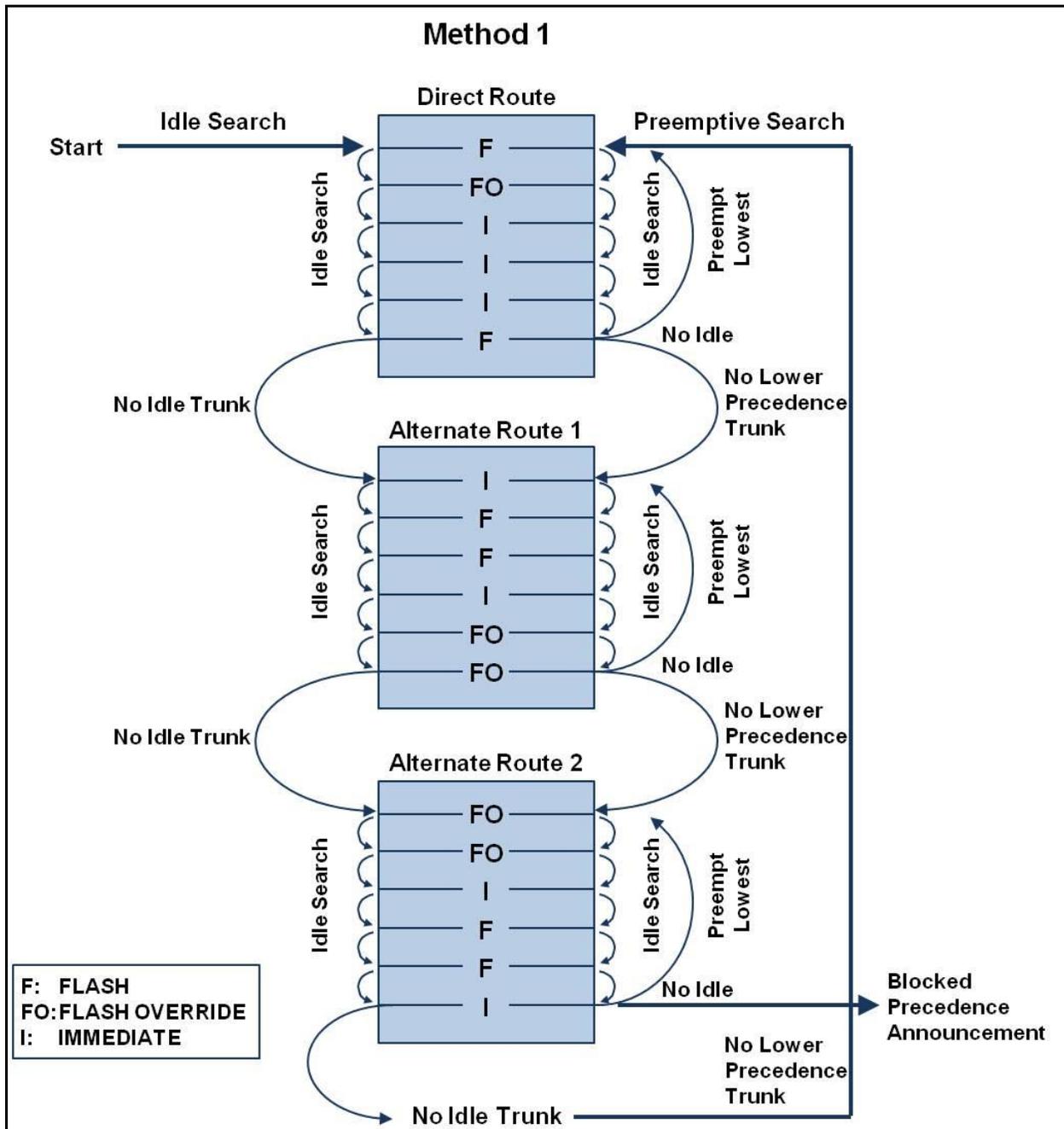


Figure 2.26-1. Example Hunt Sequence for Method 1

Failing to find an idle trunk, the SC/SS shall enter the preemptive search. In the preemptive search, the SC/SS shall search again for an idle trunk in the direct route, and if so, shall select

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

2.26.1.3.3.1.2.2 Method 2

SCM-011310 [Required: SC MG, SS MG] In method 2, the SC/SS shall directly enter a friendly, then a preemptive search of the direct route before searching the next alternate route choice, as shown in [Figure 2.26-2](#), Example Hunt Sequence for Method 2.

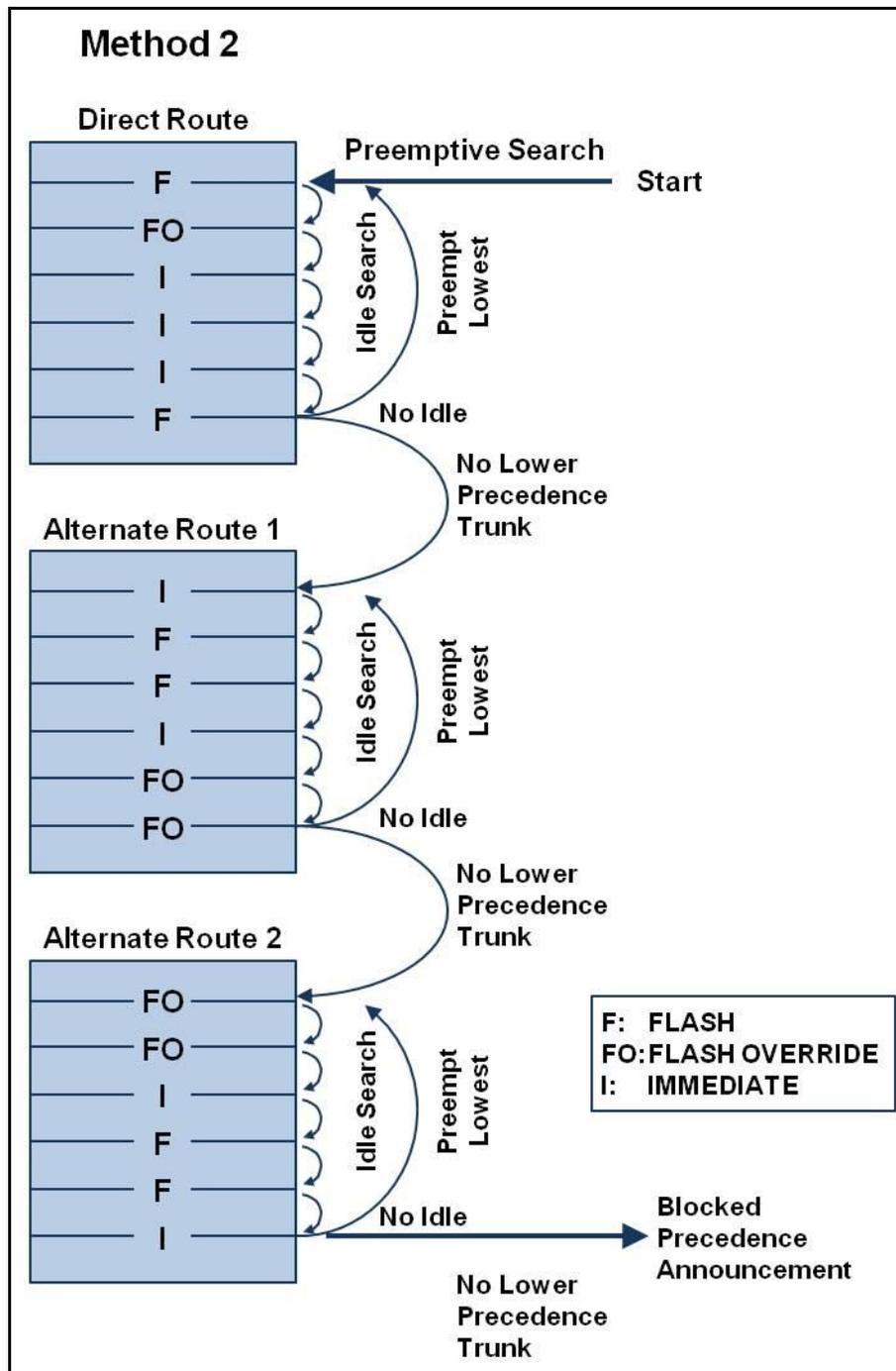


Figure 2.26-2. Example Hunt Sequence for Method 2

In the preemptive search, the SC/SS shall search for an idle trunk in the direct route, and if so, shall select any idle trunk found. If no idle trunk exists in the direct route, the SC/SS shall preempt the call of the lowest precedence in the direct route, provided the precedence of the call selected for preemption is lower than the precedence of the call being processed. Failing to complete the call on the direct route, the SC/SS shall advance the preemptive search to the next alternate route, and repeat the preemptive search process described here. This process will

continue through all possible alternate routes. When the SC/SS is unable to preempt, it shall route the caller to the BPA.

2.26.1.3.4 MLPP Interworking With Other Networks

2.26.1.3.4.1 Calls From Non-MLPP Networks

SCM-011320 [Required: MG, SC, SS] Calls from non-MLPP networks that enter UC shall be assigned the lowest precedence level and the MLPP service domain identification at the network boundary and may be preempted within UC.

2.26.1.3.4.2 Precedence Calls to Non-MLPP Networks

SCM-011330 [Required: SC, SS] When a precedence call leaves the UC network and enters a network (i.e., PSTN, North American Treaty Organization (NATO), Enhanced Mobile Satellite Systems (EMSS), etc.) or a non-MLPP device (e.g., ARD) that does not support the MLPP service, the call is treated as a non-MLPP call. The SC/SS that is directly connected to the non-MLPP network shall send an LOC2 announcement to the call originator as described in [Section 2.9.1.2.2](#), Announcements.

The SC/SS MGs shall be capable of terminating incoming calls above ROUTINE to trunk groups classmarked as non-preemptable (e.g., to a PBX2, PSTN, or other non-UC network). The SC/SS shall be capable of providing the following capabilities:

- a. The SC/SS shall divert the precedence call to an alternate DN or location capable of handling the precedence level of the call.
- b. The SC/SS/MG shall pass the precedence call, including MLPP information element for ISDN, to the distant switch (e.g., PSTN). That call shall be preemptable and maintain its precedence level within its domain of the UC network.

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

- c. The SC/SS/MG shall extend the precedence call as routine (i.e., no T1.619a IEs) to the PBX2 or a non-MLPP network.

2.26.1.4 Preempt Signaling

2.26.1.4.1 Channel-Associated Signaling

SCM-011340 [Optional: SC MG, SS MG] Preemption on CAS trunks shall be accomplished at a UC signaling appliance by sending a measured supervisory signal toward both the calling user and the called user of an established or ringing call connection. The supervisory signal is recognized at the UC signaling appliance, causing the release of the call. Following call release

a, a preempt warning tone of 440 + 620 Hz shall be applied to each end user. The preempt warning tone is introduced by the terminating UC signaling appliance at a composite level of 16 dBm, measured at the zero transmission level point (TLP). The preempt warning tone is maintained until a disconnect signal (“off hook” or feature button on EI) is returned to the UC signaling appliance. The trunk that was selected for Preemption for Reuse shall be reused to serve the waiting precedence call. Four preemption signals exist, depending on the circuit condition and intended disposition. They are Answered Call: Circuit to be Reused, Unanswered Call: Circuit to be Reused, Answered Call: Circuit Not to be Reused, and Unanswered Call: Circuit Not to be Reused, and are illustrated in [Figure 2.26-3](#), UC Preempt Signals (Part 1) and [Figure 2.26-4](#), UC Preempt Signals (Part 2).

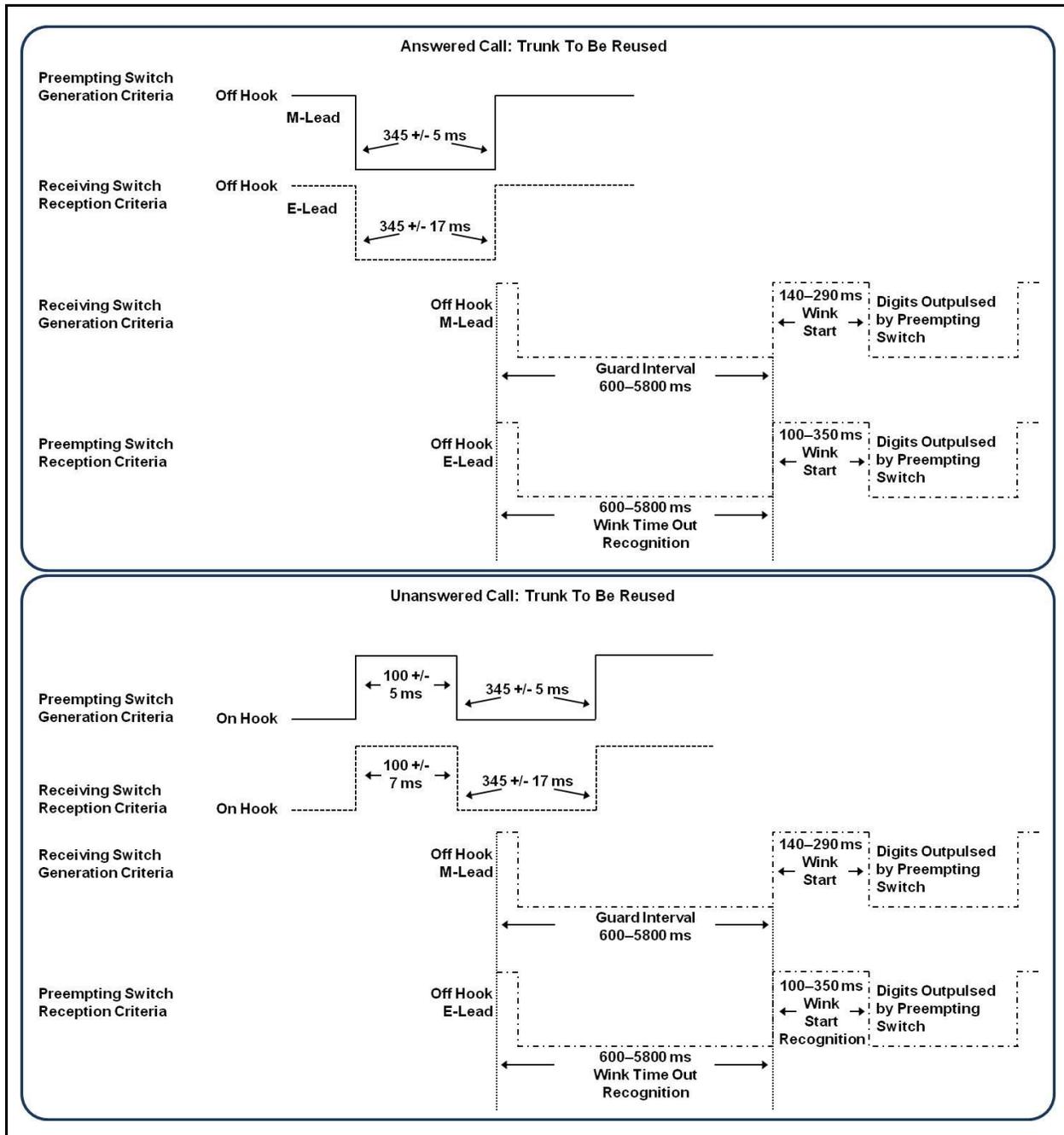


Figure 2.26-3. UC Preempt Signals (Part 1)

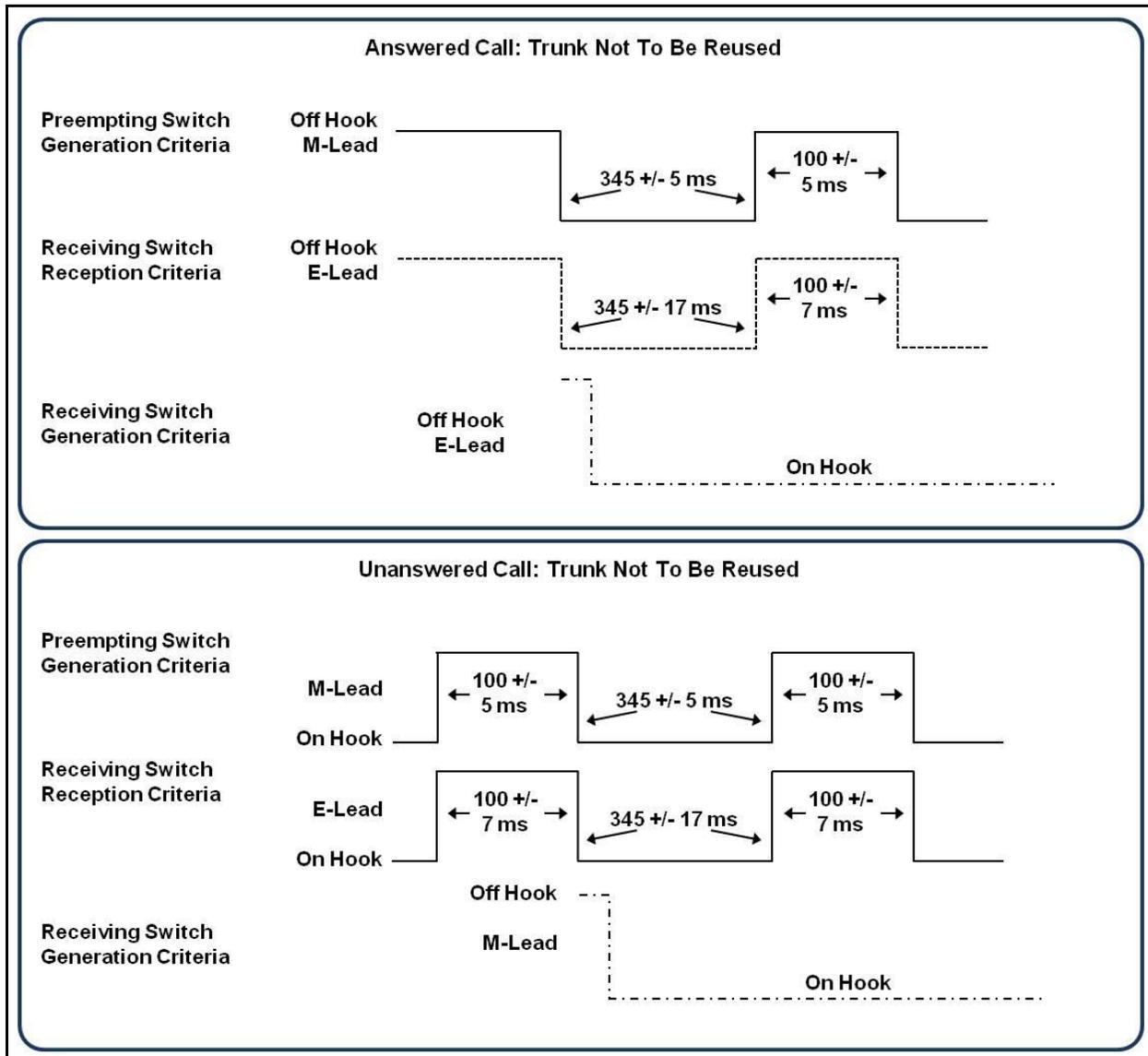


Figure 2.26-4. UC Preempt Signals (Part 2)

Preemption for Reuse shall be exercised only on classmarked trunks in a preemptable group. Preemption Not for Reuse may occur on any classmarked trunk when another link in the established connection is preempted for reuse. The UC signaling appliance MG shall apply a preemption warning tone to dial pulse (DP) and DTMF access trunks that do not use Wink Start signaling for supervision. Trunks that use Wink Start supervision shall conform to the preempt signals, as shown in [Figure 2.26-3](#), UC Preempt Signals (Part 1). Trunks using common channel supervision (i.e., D-channel signaling) shall apply the preemption warning tone to the user that is preempted. The SC/SS that supports MF(R1) signaling shall be capable of interpreting and responding to the four preempt signals, as shown in [Figure 2.26-3](#) and [Figure 2.26-4](#).

2.26.1.4.2 *Primary Rate Interface*

SCM-011350 [Required: SC MG, SS MG] Requirements for MLPP PRI signaling shall be IAW ANSI Standards T1.619-1992 and T1.619a-1994.

2.26.1.5 *Analog Line MLPP*

2.26.1.5.1 *Busy at the Called Party's Interface*

SCM-011360 [Required: TA, IAD, SC, SS] The following busy line treatment at the called party's interface for precedence calls shall apply to analog terminating lines (i.e., lines off of a TA or IAD). The line treatments apply to inter-SC calls or calls between users on the same SC.

2.26.1.5.1.1 Line Active With a Lower Precedence Call

NOTE: The text in this section has been updated and moved to [Section 2.2.3.5](#), Line Active With a Lower Precedence Call.

2.26.1.5.1.2 Line Active With an Equal or Higher Precedence Call Above ROUTINE Precedence

SCM-011370 [Required: TA, IAD, SC, SS] Precedence calls arriving at a party that is busy with an equal or higher precedence call shall be routed to a BPA (see [Table 2.9-3](#), Announcements). If the called party has activated call forwarding, the SC/SS shall attempt to complete the call to the forward destination.

2.26.1.6 *ISDN MLPP BRI*

SCM-011380 [Optional: TA, IAD, SC, SS] The ISDN MLPP BRI allows the simultaneous transmission of voice and circuit-switched (CS) data over a single customer line connecting CPE and a IAD/TA. Specifically, the basic access allows the provision of two 64-Kbps B-channels, which may be used to carry voice or CS data, and a one 16-Kbps D-channel, which can carry signaling and packet information.

The MLPP requirements for this feature shall be IAW ANSI Standard ANSI T1.619-1992 and T1.619a-1994.

2.26.1.6.1 *Single B-Channel, Single Appearance, Single Directory Number*

SCM-011390 [Optional: TA, IAD, SC, SS] The following busy line treatment at the called party's interface for precedence calls shall apply to digital (ISDN and non-ISDN) terminating lines on an IAD or TA. The line treatments also apply to inter-SC calls and calls between users on the same SC.

2.26.1.6.1.1 Line Active With a Lower Precedence Call

SCM-011400 [Optional: TA, IAD, SC, SS] Precedence calls arriving at a busy user that is classmarked as preemptable shall preempt the active lower precedence call. The active busy user shall receive a continuous preemption tone until an “on-hook” signal is received and the other party shall receive a preemption tone for a minimum of 3 seconds (see Table 2.9-2, UC Information Signals). After going “on-hook,” the user to which the precedence call is directed shall be provided precedence ringing (Table 2.9-1, UC Ringing Tones and Cadences). The user shall be connected to the preempting call after going “off-hook.”

If call waiting is invoked by the terminating user, it shall be ignored and the existing lower precedence call shall be preempted (refer to [Section 2.2.3.3](#), Busy With Lower Precedence Call).

2.26.1.6.1.2 Line Active With an Equal or Higher Precedence Call

SCM-011410 [Optional: TA, IAD, SC, SS] Precedence calls arriving at a user that is busy with an equal or higher precedence call shall be routed to a BPA (see Table 2.9-3, Announcements). If the called user has activated call forwarding, the call shall be forwarded to the new number at the same precedence level.

2.26.1.6.2 *Single B-Channel, Multiple Appearances, Single Directory Number*

SCM-011420 [Optional: TA, IAD, SC, SS] This section describes the requirements for processing precedence calls over a single B-channel ISDN interface with a station set that has multiple appearances and one DN.

Incoming precedence calls to a multiple appearance ISDN station set shall provide a precedence ringing tone on the next available button as well as a visual display of the precedence level on the station set. Then the called party shall have the option of either placing the current call on hold and picking up the incoming precedence call, or ignoring the call.

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

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

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

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

2.26.1.6.3 Two B Channels, Multiple Appearances, Single Directory Number

SCM-011430 [Optional: TA, IAD, SC, SS] The requirements for processing precedence calls over a two B-channel ISDN interface, with a station set that has multiple appearances and one DN, shall be identical to that in [Section 2.26.1.6.2](#), Single B-Channel, Multiple Appearances, Single Directory Number (i.e., precedence calls over a single B-channel ISDN interface with a station set that has multiple appearances and one DN).

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

2.26.1.6.4 Two B-Channels, Two Directory Numbers (Data Mode Only)

SCM-011440 [Required: TA, IAD, SC, SS] This section describes the requirements for processing precedence calls over a two B-channel ISDN interface with two DNs.

When an ISDN call appearance is set up as data-mode only (i.e., one or two B-channels equipped for data), preemption by incoming voice calls shall not be permitted. Any incoming higher precedence voice calls placed to a BRI in data-mode shall receive a BNEA or divert IAW [Section 2.2.10](#), Precedence Call Diversion.

2.26.1.7 ISDN MLPP PRI

SCM-011450 [Required: SC MG, SS MG, SC, SS] Requirements for ISDN MLPP PRI shall be IAW ANSI Standards T1.619-1992 and T1.619a-1994.

SCM-011460 [Optional: SC MG, SS MG, SC, SS] Requirements for European Telecommunications Standards Institute (ETSI) ISDN MLPP PRI shall be IAW ITU-T Standard Q.955.3-1993.

2.26.1.7.1 Precedence Level Information Elements

SCM-011470 [Required: SC MG, SS MG, SC, SS] The MLPP ISDN PRI Setup Message shall contain the Precedence Level IE in Code Set 5, as shown in [Table 2.26-1](#).

Table 2.26-1. MLPP ISDN PRI Precedence Level Information Element (Code Set 5)

OCTET 3:								
BIT:	8	7	6	5	4	3	2	1
	Precedence Level Information							
OCTET 1	0	1	0	0	0	0	0	1
	Element Identifier							
2	Length of Precedence Level Contents							
3	1 Ext	Coding Standard		Spare	Precedence Level			
4	0/1 Ext	Spare			Change Value	Spare	LFB Indication	
5	1st Network Identity Digit				2nd Network Identity Digit			
6	3rd Network Identity Digit				4th Network Identity Digit			
7	Most Significant Bit (DSN MLPP Service Domain 1st Octet)							
8	DSN MLPP Service Domain (2nd Octet)							
9	Least Significant Bit (DSN MLPP Service Domain 3rd Octet)							
Bit 8 Set to 1 as an extension bit								
BITS:	7-6 (CODING STANDARD)							
0 0	CCITT standardized coding							
1 0	National Standard*							
*The coding standard for DSN shall be assigned as "National."								
Bits:	4 3 2 1 (PRECEDENCE LEVEL)							
0 0 0 0	(FLASH OVERRIDE – highest)							
0 0 0 1	(FLASH)							
0 0 1 0	(IMMEDIATE)							
0 0 1 1	(PRIORITY)							
0 1 0 0	(ROUTINE – lowest)							
0 1 0 1 to 1 1 1 1	(Spare)							
OCTET 4:								
Bit 8	Set to 0/1 as an extension bit							
Bits 7-6-5	(Spare)							
Bit 4	(Change value)							
0	Precedence level coding privilege may be changed at network boundaries							
1	Precedence level coding privilege may not be changed at network boundaries							
Bit 3	(Spare)							

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

2.26.1.7.2 Disconnect Message Information Cause Values

SCM-011480 [Required: SC MG, SS MG, SC, SS] The MLPP ISDN PRI Q.931 Disconnect message shall contain the following cause values, shown in [Table 2.26-2](#), as defined in the ANSI Standards T1.619-1992 and T1.619a-1994.

Table 2.26-2. Disconnect Message Cause Value

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

2.26.1.7.3 Signal Information Element

SCM-011490 [Required: SC MG, SS MG, SC, SS] For providing tones and announcements, the Signal IE, as described in 4.5.24 of ANSI T1.607, shall be used with the following two U.S. national codepoints for signal values, as shown in [Table 2.26-3](#), U.S. National Codepoints for Signal Values.

Table 2.26-3. U.S. National Codepoints for Signal Values

SIGNAL VALUE	EXPLANATION	NORTH AMERICAN PRACTICE
9	Preemption tone is on	Precise tone is a continuous 440 Hz tone added to a 620 Hz tone
-	Precedence call alerting ringback tone on	Ringback tone (audible ringing tone) is a 440 Hz tone added to a 480 Hz tone repeated in a 1.64 s on, 0.36 s off pattern

SIGNAL VALUE	EXPLANATION	NORTH AMERICAN PRACTICE
66		Precedence call alerting 1.64 s on, 0.36 s off
Note: No signal value is assigned to “precedence call alerting ringback tone on” since the tone is always applied by the destination exchange. This ringback tone is as indicated in the table.		
Signal value (Octet 3) Bits 8 7 6 5 4 3 2 1 0 0 0 0 1 0 0 1 (9) Preemption tone 0 1 0 0 0 0 1 0 (66) Alerting on-pattern 2 (Special/priority alerting)		

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

SCM-011500 [Required: SC MG, SS MG, SC, SS] The ANSI T1.619a ISDN Setup Message called party number format shall be as shown in [Table 2.26-4](#).

Table 2.26-4. ANSI T1.619a ISDN Setup Message Called Party Number Format

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

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

SCM-011510 [Required: TA, IAD, SC MG, SS MG, SC, SS]

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

- b. Trunk-to-EI Calls. The SC/SS shall have the capability to assign a MLPP service domain on a per user basis. The SC/SS shall have the capability to assign a default MLPP service domain to a user that terminates an incoming non-ANSI T1.619a trunk call.
- c. EI-to-Trunk Calls. The SC/SS shall have the capability to assign a default MLPP service domain to an ANSI T1.619a trunk that originates from an EI that is not assigned a MLPP service domain. The SC/SS shall allow calls placed from an EI with or without an assigned MLPP service domain to route over non-ANSI T1.619a trunks.
- d. Interaction between Unlike MLPP Service Domains. The following rules apply for calls placed between unlike MLPP service domains:
 - (1) The SC/SS shall allow connection between unlike MLPP service domains when resources are available.
 - (2) When a call is placed between unlike MLPP service domains, the SC/SS shall classmark the MLPP service domain of the connection based on the MLPP service domain that entered the SC/SS.
 - (a) Example 1: EI-to-EI. If an intra-SC call is placed between two subscribers with different MLPP service domains, the SC shall classmark the connection with the MLPP service domain of the originator.
 - (b) Example 2: Trunk-to-Trunk. If an incoming call is placed to an SC/SS via a non-ANSI T1.619a trunk (i.e., T1/E1 CAS, ISDN PRI) that tandems to an ANSI T1.619a trunk, the SC/SS shall assign the default MLPP service domain to the outbound ANSI T1.619a trunk, and classmark the connection as the SC/SS-assigned default MLPP service domain.
 - (c) Example 3: Trunk-to-EI. If an incoming call is placed to a SC/SS via a non-ANSI T1.619a trunk (i.e., T1/E1 CAS, ISDN PRI) that terminates to an EI, the SC/SS shall assign the default MLPP service domain to the EI and classmark the connection as the SC/SS-assigned default MLPP service domain.
 - (d) Example 4: EI-to-Trunk. If a call is originated from a subscriber over a non-ANSI T1.619a trunk (i.e., T1/E1 CAS, ISDN PRI), the SC/SS shall classmark the MLPP service domain of the connection as the MLPP service domain of the originator.
- e. The MLPP interaction shall not be allowed between unlike MLPP service domains.

2.26.1.8 MLPP Interactions With Common Optional Features and Services

This section describes the requirements for MLPP interactions with other features and services.

2.26.1.8.1 Multiline Hunt Service

SCM-011520 [Optional: PEI, UEI, SC, SS]

- a. **Pilot Line Hunt.** This hunting feature is a group of EIs arranged so that a lead published number, the pilot number is called first. If the first EI (pilot number) is busy, the call goes to the second and subsequent EIs until an idle, or the last EI in the hunt group is called. If all EIs are busy, the calling party will receive a busy tone (unless other forwarding, etc., features are present on the EI).
- b. **Distributed Hunt.** This hunting feature is a group of EIs arranged so that incoming calls are sent to the EI in the group that has been idle the longest.
- c. **Circular Hunt.** This hunt feature is a group of EIs arranged so that if any EI in the hunt group is busy, hunting starts at the next EI, and continues through the rest of the group. This hunting feature will rotate or search the idle status of the EIs in the group at least once (one cycle) before a busy tone is sent.
- d. **MLPP Interactions, EI Hunting.** If no EI is available and one or more existing calls are of lower precedence level than that of the incoming call, an existing call of the lowest precedence level within the group shall be preempted.

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

SCM-011530 [Conditional: PEI, UEI, SC, SS] If Multiline Hunt Service is supported, then it shall be provided in accordance with Telcordia Technologies GR-569-CORE.

2.26.1.9 MLPP Interactions With Electronic Key Telephone Systems Features

2.26.1.9.1 Electronic Key Telephone Systems

SCM-011540 [Optional: TA, IAD, SC, SS] Electronic Key Telephone Systems functions shall be provided by the UC appliance as described in Telcordia Technologies GR 205 CORE. Additional MLPP requirements are listed in the following paragraphs.

2.26.1.9.1.1 Call Appearances

SCM-011550 [Optional: TA, IAD, SC, SS] A call appearance shall be shared by all EKTS users. There shall not be separate call appearances for MLPP calls. All users shall be able to originate the authorized precedence level and receive all levels of precedence on a single call appearance for each directory number. Each EKTS call appearance shall comply with the MLPP functionality specified in [Section 2.26.1](#), Multilevel Precedence and Preemption.

2.26.1.9.1.2 Hold

SCM-011560 [Optional: TA, IAD, SC, SS] The EKTS Hold function shall comply with the requirements of [Section 2.2.5](#), Call Hold.

2.26.1.9.1.3 Directory Number Bridging

SCM-011570 [Optional: TA, IAD, SC, SS] The EKTS Directory Number Bridging function shall comply with the requirements of [Section 2.2.6](#), Three-Way Calling.

2.26.1.9.1.4 Intercom Calling

SCM-011580 [Optional: TA, IAD, SC, SS] The EKTS Intercom Calling feature shall not prevent the offering of an MLPP call to any of the parties involved in an intercom call.

2.26.1.9.1.5 Abbreviated or Delayed Ringing Treatment on Incoming Calls

SCM-011590 [Optional: TA, IAD, SC, SS] Incoming MLPP calls shall be considered as “distinctive alerting” and shall not be affected by the Abbreviated or Delayed Ringing Treatment. Precedence Alerting (see [Table 2.9-1](#), UC Ringing Tones and Cadences) shall be applied to the call DN appearance and the call handled as described in [Section 2.26.1.6](#), ISDN MLPP BRI. If the call is not answered and the EKTS-T1 time expires, the call shall be diverted to an operator. If Call Forwarding-No Reply is invoked by the called DN, then the Call Forwarding procedures of [Section 2.2.2.2](#), Call Forwarding – No Reply at Called Station, apply at the expiration of the EKTS-T1 timer.

2.26.1.9.1.6 Bridged Call Exclusion

SCM-011600 [Optional: TA, IAD, SC, SS] The Bridged Call Exclusion (BCE) feature (automatic or manual) shall not degrade or prevent the MLPP interactions described in this section.

2.26.1.9.1.7 Non-ISDN Users

SCM-011610 [Optional: TA, IAD, SC, SS] Non-ISDN users (analog telephone) can be assigned as members of the EKTS group. The non-ISDN user will share a call appearance with other members of the EKTS group and shall be able to originate the authorized precedence level and receive all levels of precedence on that shared appearance.

2.26.1.10 Network Management Manual Controls

SCM-011620 [Required: SC, SS] Call gapping shall not apply to FLASH and FLASH OVERRIDE calls. In addition, FLASH and FLASH OVERRIDE calls shall be exempt from Cancel to (CANT) and Cancel from (CANF)..

2.26.2 Signaling

2.26.2.1 Introduction

This section covers the signaling requirements for UC signaling appliance systems. The requirements are based on Telcordia Technologies GR-506-CORE; ANSI T1.619 (1992); ANSI T1.619a (1994); ANSI T1.110 (1999); ANSI T1.116 (1996); ANSI T1.116a (1998); ANSI T1.111 (1996); ANSI T1.114 (2000); ANSI T1.112 (1996); and ANSI 1.113 (1995).

Requirements for analog signaling also apply to digital circuits using CAS.

2.26.2.2 Network Power Systems for External Interfaces

SCM-011630 [Required: TA, IAD, SC, SS – Optional: MG] The UC signaling appliance systems shall meet the network power systems requirements specified in the Telcordia Technologies GR-506-CORE, Paragraph 2.1.

2.26.2.3 Line Signaling

2.26.2.3.1 Loop Start Line

SCM-011640 [Required: TA, IAD] In a loop start line arrangement, the IAD/TA supplies battery between the ring and the tip conductors. The IAD/TA detects a loop closure from the customer station as a seizure, after which it provides dial tone on the tip and ring conductors as a start dial signal.

The UC signaling appliance systems shall meet this requirement in accordance with the “R” requirements in Telcordia Technologies GR-506-CORE, Paragraphs 3 through 3.4.7, 6.2.1, 6.3.1, 13.6.1.1, 13.6.2.1, 13.6.3.1, and 13.7.1.

2.26.2.3.2 Ground Start Line

SCM-011650 [Required: TA, IAD] In a ground start line arrangement, the IAD/TA provides battery through a ground detector to the ring conductor and leaves the tip conductor open. The customer station seizes the line by applying a ground to the ring conductor. The IAD/TA responds by returning ground on the tip conductor and dial tone across the tip and ring as start dial signals. When the tip ground is detected from the IAD/TA, the customer station changes to loop closure for the off-hook state. Alerting the customer is done by connecting 20-Hz ringing to the ring conductor and ground to the tip conductor.

The UC signaling appliance systems shall meet this requirement in accordance with the “R” requirements in Telcordia Technologies GR-506-CORE, Paragraphs 4 through 4.4.8, 13.2.2, 13.6.1.1, 13.6.2.2, 13.6.3.2, and 13.7.2.

2.26.2.4 *Trunk Supervisory Signaling*

2.26.2.4.1 *Reverse Battery*

SCM-011660 [Optional: SC MG, SS MG] The trunk circuit at one end of a variety of loop signaling trunks applies battery and ground through suitable resistances to the tip and ring conductors. One polarity on the tip and ring leads is used for the on-hook state, and the reverse is used for the off-hook state.

The UC signaling appliance systems may meet this requirement in accordance with the “R” requirements in Telcordia Technologies GR-506-CORE, Paragraphs 7 and 8.

2.26.2.4.2 *Immediate Start*

SCM-011670 [Optional: SC MG, SS MG] Immediate start (by-link) is a feature that provides intersystem address signaling between the MG and a system that transmits and/or receives address signals without special address control signals. For the reception of digits from offices requiring immediate start, the system shall be prepared to recognize the first dial pulse promptly after the connect signal is received. For transmission of address information to an office requiring immediate start, the system shall delay outpulsing after sending the connect signal to ensure that the distant office is ready. It is desirable that the transmitting office verifies that battery and ground are of the proper polarity at the time of seizure. Failure to detect the proper condition may result in a retry of the call and a failure recorded.

The UC signaling appliance systems may meet this requirement in accordance with the “R” requirements in Telcordia Technologies GR-506-CORE, Paragraph 11.2.2.

2.26.2.4.3 *Normal and Abnormal Wink Start Operation*

2.26.2.4.3.1 Normal Operation

2.26.2.4.3.1.1 Normal Wink Start Operation

SCM-011680 [Optional: SC MG, SS MG] Wink start is a feature that provides control for address signaling between systems arranged with wink start as a special address control signal. The wink start signal is applicable to specified incoming, outgoing, and two-way trunks and is used to inform the calling office that the called office is prepared to receive address signals. For wink start operation, the transmitting office may test for the detection of the brief off-hook as a signaling integrity check.

The UC signaling appliance systems may provide wink start operation in accordance with the requirements in Telcordia Technologies GR-506-CORE, Paragraph 11.2.1.

2.26.2.4.3.1.2 Glare Operation

SCM-011690 [Optional: SC MG, SS MG] Glare occurs when both interfaces of switching systems connected to the same inter-switching-system facility (trunk) apply a seizure signal at approximately the same time.

The UC signaling appliance systems may provide glare detection and resolution IAW the requirements in Telcordia Technologies GR-506-CORE, Paragraph 11.5.

2.26.2.4.3.2 Abnormal Operation

2.26.2.4.3.2.1 Wink Start

SCM-011700 [Optional: SC MG, SS MG] After the connect signal is sent over the trunk, the originating office can normally expect to receive a wink start (timed off-hook) signal indicating that the terminating office is ready to receive address signaling. When the end of the wink start signal is received, the originating office may begin outpulsing. The duration of the off-hook wink returned by the terminating office will be 140 to 290 ms. However, because of distortion in the trunk facilities, the duration of the wink received by the originating office may vary (refer to [Figure 2.26-3](#), UC Preempt Signals (Part 1) and [Figure 2.26-4](#), UC Preempt Signals (Part 2)). If the wink is shorter than the minimum allowable interval, it shall be ignored. If it is greater than the maximum interval, the call may be considered to be in a glare condition as described in [Section 2.26.2.4.3.2.2](#), Glare Resolution.

2.26.2.4.3.2.2 Glare Resolution

SCM-011710 [Optional: SC MG, SS MG] The UC signaling appliances may meet the glare resolutions requirements defined in Telcordia Technologies GR-506-CORE, Paragraph 11.5 and subparagraphs.

2.26.2.4.4 *Delay Dial*

SCM-011720 [Conditional: SC MG, SS MG] If this feature is provided, it shall be in accordance with Telcordia Technologies GR-506-CORE.

2.26.2.4.5 *Call for Service Timing*

SCM-011730 [Optional: SC MG, SS MG] The MG shall ignore as a “hit” any transient off-hook signal whose duration is less than 35 ms on an incoming trunk. Off-hook signals greater than 60 ms may be considered as a valid seizure. Signals that are 15 to 60 ms in length are considered invalid seizures.

2.26.2.4.6 *Guard Timing*

SCM-011740 [Optional: SC MG, SS MG] The UC signaling appliance systems may meet guard requirements in accordance with Telcordia Technologies GR-506-CORE.

2.26.2.4.7 *Satellite Interface*

SCM-011750 [Optional: SC MG, SS MG] The UC signaling appliance system may accommodate the use of single satellite-derived trunk facilities. The only interface parameter that shall be modified is the guard timing. This interval may be extended from 1050 to 1250 ms to compensate for propagation delay.

2.26.2.4.8 *Disconnect Control*

SCM-011760 [Optional: SC MG, SS MG] The UC signaling appliance systems may meet the Disconnect Control requirements in Telcordia Technologies GR-506-CORE, Paragraph 13 and all subparagraphs.

2.26.2.4.9 *Reselect or Retrial*

SCM-011770 [Optional: SC MG, SS MG] The actions that may be taken by the MG are summarized in the following table based on the direction of the circuit (outgoing or two-way), the method of controlled outpulsing (wink start or delay dial), and the method of glare resolution on two-way circuit (hold or release). The MG may reselect or retry on circuit supervision faults as shown in [Table 2.26-5](#).

Table 2.26-5. Reselect or Retrial

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

2.26.2.4.10 Off-Hook Supervision Transitions (Unexpected Stop)

SCM-011780 [Optional: SC MG, SS MG] The UC signaling appliances may detect and react to unexpected off-hook supervisory transitions while outpulsing on trunks, after receipt of the start-dial indication and until completion of the outpulsing. An unexpected stop is defined as an off-hook supervision transition whose duration exceeds the “hit” timing interval. When an unexpected stop is detected, the system may reselect another trunk.

2.26.2.5 Control Signaling

Control signaling is used for the reception and outpulsing of address, precedence, and routing information. Three types of outpulsing are DP, DTMF, and Multifrequency 2/6. The UC signaling appliances shall support as applicable the following signaling combinations: DTMF 2way, DP 2way, DTMF in-DP out, DP in-DTMF out, MF(R1) 2/6 2way. Audible tones shall be IAW Telcordia Technologies GR-506-CORE, Paragraph 17.

2.26.2.5.1 Dial-Pulse Signals

SCM-011790 [Required: TA, IAD] The UC DP signaling requirements are the same as those specified in Telcordia Technologies GR-506-CORE, Paragraph 10.

2.26.2.5.2 DTMF Signaling

SCM-011800 [Required: TA, IAD – Optional: SC MG, SS MG] The UC signaling appliance system shall be capable of outpulsing and interpretation of DTMF digits on outgoing or two-way trunks as specified in Telcordia Technologies GR-506-CORE, Paragraph 15, and [Table 2.26-6](#).

Table 2.26-6. DTMF Generation and Reception From Users and Trunks

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

2.26.2.5.2.1 Standard Digit Format for Precedence

SCM-011810 [Required: TA, IAD – Optional: SC MG, SS MG] In addition, the UC signaling appliance system shall be capable of outpulsing and interpretation of DTMF precedence digits in digit 0 through 4 format (i.e., 0=FLASH OVERRIDE, 1=FLASH, 2=IMMEDIATE, 3=PRIORITY, and 4=ROUTINE).

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

SCM-011820 [Optional: SC MG, SS MG] The UC signaling appliance system may be capable of outpulsing and reception of multifrequency (MF)(R1) 2/6 signaling requirements IAW Telcordia Technologies GR-506-CORE, Paragraph 16 and its subparagraphs, and [Table 2.26-7](#), MF(R1) 2/6 Generation and Reception for Trunks.

Table 2.26-7. MF(R1) 2/6 Generation and Reception for Trunks

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

2.26.2.6 Alerting Signals and Tones

Alerting signals are applied by an EI or IAD/TA to inform the end-user of an incoming call. [Section 2.9.1.2.1](#) defines ringing and information signal requirements.

2.26.2.7 ISDN Digital Subscriber Signaling System No. 1 Signaling

2.26.2.7.1 UC ISDN User-to-Network Signaling

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

- Circuit-switched calls (both data and voice).
- Supplementary services that include unique UC features.

- Future UC access signaling requirements for other network services, including public and private network interworking in intracountry and intercountry environments, as applicable, and interoperability with other DOD Networks.

2.26.2.7.1.1 Application

SCM-011830 [PRI: Required: MG, SC, SS – BRI: Optional: TA, IAD, SC, SS] This section is the UC signaling appliance requirements for user-to-network signaling over an ISDN interface. It specifies the interface signaling protocol for application throughout the UC network and defines the requirements of the UC user-to-network signaling for exchanging information between CPE, including terminal equipment (TE) and PBXs, and UC network signaling appliances. The exchange of signaling information between CPE and UC network signaling appliances shall be over the D-channel of the ISDN interface. The D-channel may be used either for associated signaling or non-associated signaling as defined in ANSI T1.607, Annex F. In-band information and tones sent over the B-channel shall be allowed, when applicable. In the UC host countries, UC connections may be made with public, private, and military CPE and networks. Protocol and/or SG conversions shall be required in some instances to provide the desired UC connections. Such translations shall be handled on a case-by-case basis as detailed in site-specific contracts.

2.26.2.7.1.2 Physical Layer

SCM-011840 [PRI: Required: MG, SC, SS – BRI: Optional: TA, IAD, SC, SS] The UC user-to-network signaling physical layer specification for the BRI shall be ANSI T1.605 and ANSI T1.601 or ITU Recommendation I.430, as required, for OCONUS applications. The UC user-to-network signaling physical layer specification for the PRI operating at 1.544 Mbps shall be ANSI T1.408. The UC user-to-network signaling specification for the PRI operating at 2.048 Mbps shall be ITU Recommendation I.431.

2.26.2.7.1.2.1 S/T Reference Point

SCM-011850 [Optional: TA, IAD] For the BRI at the S/T reference point, B-channels shall have the capability of either restricted or unrestricted operation. The restricted capability is necessary for backward compatibility with networks that support the restricted 64 Kbps operation. The D channel shall have unrestricted capability.

2.26.2.7.1.3 Data-Link Layer

SCM-011860 [PRI: Required: MG, SC, SS – BRI: Optional: TA, IAD, SC, SS] The UC user-to-network signaling data-link layer shall be as specified in the ANSI T1.602, which is a pointer document completely aligned with the ITU-T Recommendations Q.920 and Q.921.

2.26.2.7.1.3.1 Data-Link Connections

SCM-011870 [PRI: Required: MG, SC, SS – BRI: Optional: TA, IAD, SC, SS] Point-to-point, broadcast, and multipoint data-link connections shall be provided for UC applications. The ANSI T1.602 depicts examples of point-to-point and broadcast data-link connections. Other point-to-point applications of this specification shall be allowed, such as the support of multiple terminals at the user-to-network interface. A data-link layer management entity shall be provided to support UC management.

2.26.2.7.1.3.2 Peer-to-Peer Procedures of Data-Link Layer

SCM-011880 [PRI: Required: MG, SC, SS – BRI: Optional: TA, IAD, SC, SS] Within the UC network, peer-to-peer procedures of the data-link layer shall follow the procedures described in the ANSI T1.602, with the additions provided in this paragraph. The network administration shall have the responsibility to determine the system parameter values on the UC user-to-network interface. These parameters shall initially be set to the default values of the ANSI standard. A means is available in ITU-T Recommendation Q.921, Appendix IV to change the assignment of the system parameters within the range of values specified by the ANSI standard. The UC TE shall support other values of T200 to allow for multiple terminals on the user side, together with satellite connections, in UC user-to-network transmission.

2.26.2.7.1.4 Layer 3 UC User-to-Network Signaling

SCM-011890 [PRI: Required: MG, SC, SS – BRI: Optional: TA, IAD, SC, SS] The Layer 3 protocols specify the messages and IEs, coding and formats, and procedures used on the user-to-network interface to establish, maintain, and terminate network connections across an ISDN.

2.26.2.7.1.4.1 Overview of Layer 3

The overview of Layer 3 of the UC user-to-network signaling layer 3 shall be as specified in ANSI T1.615. The ANSI standard is consistent with the seven-layer model described in ITU Recommendation I.320. ANSI T1.615 describes, in general terms, the D-channel Layer 3 DSS1 functions and protocol used across an ISDN user-to-network interface.

2.26.2.7.1.4.2 RTS User-to-Network Signaling for Circuit-Switched Bearer Service

SCM-011900 [PRI: Required: MG, SC, SS – BRI: Optional: TA, IAD, SC, SS] The UC user-to-network signaling Layer 3 specification for CS bearer service (or CS-Basic Call) shall be as specified in the ANSI T1.607 for ISDN PRI and BRI. ANSI T1.607 is aligned with the ITU Recommendation Q.931 (to the extent possible), and it covers U.S. unique requirements for CS-Basic Call.

2.26.2.7.1.4.3 Sequence of Messages for UC CS Calls

SCM-011910 [PRI: Required: MG, SC, SS – BRI: Optional: TA, IAD, SC, SS] Call establishment involves SETUP, SETUP ACK, CALL PROCEEDING, ALERTING, CONNECT, and CONNECT ACK messages. The PROGRESS message shall be used with interworking or with in-band information and patterns to indicate the progress of a call. A three-step call clearing phase shall use the DISCONNECT, RELEASE, and RELEASE COMPLETE messages. The miscellaneous messages—INFORMATION, STATUS ENQUIRY (and STATUS), and NOTIFY—shall be used for the purposes described in ANSI T1.607.

2.26.2.7.1.4.4 Message Functional Definitions and Content

SCM-011920 [PRI: Required: MG, SC, SS – BRI: Optional: TA, IAD, SC, SS] The Layer 3 messages used by the UC user-to-network signaling for CS connections shall be as specified by the ANSI T1.607, except for messages modified in the following paragraph.

SETUP Message. The SETUP message is sent by the calling user to the network or by the network to the called user to initiate call establishment. The UC calls shall use the SETUP message specified in ANSI T1.607. The Channel Identification, Calling Party Number (when available), and Called Party Number are mandatory IEs. For an MLPP call (invoking an MLPP feature) on the UC user-to-network interface, the SETUP message shall include the Precedence Level IE. It also shall contain other IEs, when such unique UC features are required and the call identity IE (as defined in ITU Recommendation Q.931) for the MLPP feature. The Precedence Level and MLPP service domain (both contained in the Precedence Level IE) and Calling Party Number (contained in the Calling Party Number IE), shall be used to mark the circuit (identified in the Channel Identification IE) to be preempted as “reserved” for reuse by the preempting call when the LFB option is exercised on the UC user-to-network interface. [Table 2.26-8](#), SETUP Message for MLPP Call, shows the SETUP message content for an MLPP call; important differences from the SETUP message in ANSI T1.607 are specified in the following paragraphs.

Table 2.26-8. SETUP Message for MLPP Call

MESSAGE TYPE: SETUP SIGNIFICANCE: GLOBAL DIRECTION: BOTH			
INFORMATION ELEMENT	ANSI T1.607 REFERENCE	DIRECTION	TYPE
Protocol Discriminator	4.2	both	M
Call Reference	4.3	both	M
Message Type	4.4	both	M
Repeat Indicator	4.5	both	O (Note 1)
Bearer Capability	4.5	both	M (Note 2)
Channel Identification	4.5	both	M (Note 3)

MESSAGE TYPE: SETUP SIGNIFICANCE: GLOBAL DIRECTION: BOTH			
INFORMATION ELEMENT	ANSI T1.607 REFERENCE	DIRECTION	TYPE
Progress Indicator	4.5	both	O (Note 4)
Network Specific Facilities	4.5	both	O (Note 5)
Display	4.5	n-u	O (Notes 6 & 7)
Keypad Facility	4.5	u-n	O (Note 8)
Signal	4.5	n-u	O (Note 9)
Calling Party Number	4.5	both	M (Note 10)
Calling Party Subaddress	4.5	both	O (Note 11)
Called Party Number	4.5	both	M (Note 12)
Called Party Subaddress	4.5	both	O (Note 13)
Transit Network Selection	4.5	u-n	O (Note 14)
Lower Layer Compatibility	4.5	both	O (Note 15)
High Layer Compatibility	4.5	both	O (Note 16)
User-User	4.5	both	O (Notes 17 & 18)
Locking Shift (Note1)	4.5	u-n	O (Note 19)
Operator System Access	4.6	u-n	O (Note 20)
Precedence Level	Note2	both	M
NOTE: Notes 1 through 20 and references of the ANSI T1.607 IE are not repeated for this table but still apply. Refer to ANSI T1.607 IE for detailed notes and references.			
1. The Locking Shift IE to identify IEs in U.S. National Codeset 5.			
2. The Precedence Level IE is in U.S. National Codeset 5 and is defined in ANSI T1.619 (1992) and T1-619a (1994).			
LEGEND			
M: Mandatory		O: Optional Elements	

2.26.2.7.1.4.5 General Message Format and Information Elements Coding

SCM-011930 [PRI: Required: MG, SC, SS – BRI: Optional: TA, IAD, SC, SS] The guidelines specified in the ANSI T1.607 shall be followed in this specification.

- a. Application of Codesets Within UC. UC unique IEs, if any, shall use the following order of preference in using the codesets:
 - (1) Codeset 0 – highest.
 - (2) Codeset 5.
 - (3) Codeset 6 – lowest.

- b. Application of IEs in UC. The UC user-to-network signaling protocol shall maximize the use of codeset “00” (ITU standardized coding) and codeset “10” (national standard) IEs (when codeset “00” is not possible). Following are guidelines for the specific use of such IEs in the UC network:
- (1) Called Party Number IE. The Called Party Number IE, which identifies one called party of a call, shall accommodate the DSN numbering plan. The variable length number digits parameter in the IE may carry the area code, switch code, and line number from the DSN numbering plan.
 - (2) Calling Party Number IE. The Calling Party Number IE, which identifies the origin of a call, shall accommodate the DSN Worldwide Numbering and Dialing Plan (WWNDP) as stated for the Called Party Number IE.
 - (3) Keypad Facility IE. The Keypad Facility IE, which conveys ASCII characters entered by means of a terminal keypad (when used), shall contain the digits entered by a UC user.
 - (4) Channel Identification IE. The Channel Identification IE identifies a channel within the interface(s) controlled by the signaling procedures. The channel number/slot map parameter within it identifies the B-channel controlled by a particular message. The following two methods of B-channel identification are available for use in the UC network: 1) binary channel number assigned to the channel and 2) a slot map that identifies the time slots used by the channel. The parameter shall be coded exclusively for one method depending on the number/map parameter information. Both PRIs, 1.544 Mbps and 2.048 Mbps, shall be supported IAW the slot map in ITU-T Q.931.
 - (5) Transit Network Selection IE. The Transit Network Selection IE identifies one requested transit network. It may be repeated in a message to select a sequence of transit networks through which a call must pass. For example, the element may be used in a SETUP message to specify one or a sequence of transit networks (other than the user-assigned transit network) through which a call must pass. In the case of UC user-to-network signaling, this IE shall be used to specify the UC network or a network other than the UC network as a transit network. (DOD networks and foreign PTTs are examples.)
 - (6) Cause IE. The Cause IE shall be IAW ANSI T1.619a.
 - (7) Signal IE. The Signal IE shall be IAW ANSI T1.619a. The signal shall be included in the DISCONNECT, PROGRESS, and SETUP messages, as appropriate, for the MLPP feature.
 - (8) Notification Indicator IE. The Notification Indicator IE, which indicates information pertaining to a call, shall contain the notification description code of “0 0 0 0 1 0 0” (value 4) for the MLPP feature to indicate to the calling user a possible call completion delay when an LFB query is invoked in response to an MLPP call setup.

2.26.2.7.1.4.6 Supplementary Services

SCM-011940 [Optional: TA, IAD, MG, SC, SS] If provided, Supplementary Services shall be IAW the following standards:

- a. ANSI T1.607-1998.
- b. ANSI T1.613-1992.
- c. ANSI T1.616-1992.
- d. ANSI T1.621-1992.
- e. ANSI T1.632-1993.
- f. ANSI T1.642-1993.
- g. ANSI T1.643-1995.
- h. ANSI T1.647-1995.

2.26.3 ISDN

SCM-011950 [Required] The UC signaling appliance systems shall provide the ISDN BRI and PRI capabilities shown in Tables 2.26-9 through 2.26-13 that are marked with an R. The UC signaling appliance systems may provide the ISDN BRI and PRI capabilities shown in [Tables 2.26-9](#) through [2.26-13](#) that are marked with an O, indicating Optional.

Tables 3-1 through 3-5 of Telcordia Technologies SR 3476 provide the specific requirements for features and capabilities listed in [Tables 2.26-9](#) through [2.26-13](#). The MLPP interactions with ISDN are identified in [Section 2.26.1](#), Multilevel Precedence and Preemption.

Table 2.26-9. BRI Access, Call Control, and Signaling

IAD/TA	SC MG	SS MG	SC	SS	FEATURE OR CAPABILITY
O			O	O	ISDN BRI Layer 1
O			O	O	4:1 Time Division Multiplex Method for ISDN Basic Access
O			O	O	ISDN BRI Layer 2
O			O	O	BRI Circuit-Mode Call Control Basic Call Control
O			O	O	BRI Terminal initialization
O			O	O	Service Profile Identifier
O			O	O	Parameter Downloading
O			O	O	Default Services for Terminals

Table 2.26-10. Uniform Interface Configurations for BRIs

TA/ IAD	SC MG	SS MG	SC	SS	FEATURE OR CAPABILITY
O			O	O	Uniform Interface Configurations for BRIs. Single User with Multiple Applications Two Users Sharing a BRI
O			O	O	More than two B-Channel Terminals on a BRI (Passive Bus)
O			O	O	Associated Group Indicator
O			O	O	DN Sharing over Multiple Call Types on an Integrated Terminal
O			O	O	Non-Initializing Terminals

Table 2.26-11. BRI Features

TA/ IAD	SC MG	SS MG	SC	SS	FEATURE OR CAPABILITY
O			O	O	Electronic Key Telephone Systems Multiple DNs per Terminal Analog Member of an EKTS Group Multiple DN Appearances per Call Appearance Call Handling Hold/Retrieve Bridging/DN-Bridging Intercom Calling Membership in a Multiline Hunt Group Abbreviated and Delayed Ringing Automatic and/or Manual Bridged Call Exclusion
O			O	O	Call Forwarding
O			O	O	Call Forwarding Variable Courtesy Call Reminder Notification Call Forwarding Interface Busy Call Forwarding Don't Answer Call Forwarding Intragroup Only Call Forwarding Interface Busy Incoming Only Call Forwarding Don't Answer Incoming Only
O			O	O	ISDN Call Hold Hold and Retrieve
O			O	O	Flexible Calling Three-Way and Six-Way Calling Consultation Hold Conference Hold and Retrieve
O			O	O	ISDN Display Service Protocol and Procedures Uniform Text (for NI-2 Uniform Services)
O			O	O	Basic Business Group

TA/ IAD	SC MG	SS MG	SC	SS	FEATURE OR CAPABILITY
					Denied Originating Denied Terminating Distinctive Alerting Indication
O			O	O	Business Group Dial Access Features
O			O	O	Dial Access to Automatic Flexible Routing
O			O	O	Customer Access Treatment Code Restriction
O			O	O	Code Restriction and Diversion
O			O	O	Direct Outward Dialing
O			O	O	Direct Inward Dialing
O			O	O	ISDN Call Pickup
O			O	O	ISDN Directed Call Pickup
O			O	O	Access To Analog Attendant Access Station Message Detail Recording Tracing of Terminating Calls Tandem Call Tracing Trace of a Call In Progress Bulk Calling Line Identification Selective Call Acceptance Selective Call Forwarding Selective Call Rejection
O			O	O	Limitations and Restrictions for 911 PSAP – Call Hold Not Allowed for a 911 Call

Table 2.26-12. PRI Access, Call Control, and Signaling

TA/ IAD	SC MG	SS MG	SC	SS	FEATURE OR CAPABILITY
	R	R	R	R	PRI Layer 1
	R	R	R	R	PRI Layer 2 (Circuit)
	R	R	R	R	PRI Call Control and Signaling
	R	R	R	R	Basic Call Control for Circuit Mode Calls
	R	R	R	R	Multiple DS1 Facilities Controlled by a Single D-Channel
	R	R	R	R	Access to Selected Primary Rate Services on a Per-Call Basis

Table 2.26-13. PRI Features

TA/ IAD	SC MG	SS MG	SC	SS	FEATURE OR CAPABILITY
	O	O	O	O	Call-by-Call Service Selection FX Non-ISDN Tie IN WATS

TA/ IAD	SC MG	SS MG	SC	SS	FEATURE OR CAPABILITY
					OUT WATS Non-ISDN ETN
	O	O	O	O	Interworking with Private Networks

2.26.4 Backup Power

SCM-011960 [Required: TA, IAD, MG, SC, SS] UC shall have backup power to maintain continuous operation whenever the primary source of power is disrupted. Back-up power design and implementation shall be incorporated into the design to assure that UC meets the reliability requirements of UCR 2013, Section 15, Reliability. General power requirements are described in Telcordia Technologies GR-513-CORE. Following the risk avoidance guidance in Telcordia Technologies GR-513-CORE, the backup power design shall minimize the probability of a complete loss of UC appliance system power.

2.26.4.1 UPS

The requirements for UPS in the following paragraphs are bare minimum essential requirements and may not assure the design goal of continuous operation.

2.26.4.1.1 UPS Load Capacity

SCM-011970 [Required: TA, IAD, MG, SC, SS] The Uninterruptible Power Supply (UPS) shall provide greater than 8 hours of mission busy hour current load requirements (rated in Ampere hours) plus at least 10 percent for UC equipment to include ancillary equipments.

2.26.4.2 Backup Power (Environmental)

SCM-011980 [Required: SC, SS] The backup power system shall have the capacity to operate environmental systems required to sustain continuous operation of UC appliance systems equipment to include ancillary equipments. Power to the environmental systems may not need to be continuous.

2.26.4.3 Alarms

SCM-011990 [Required: TA, IAD, MG, SC, SS] Power system alarms shall be generated to an attended monitoring location whenever there is a loss of power and shall remain until the power is restored. Power alarms shall remain active until the condition that activated the alarm is corrected.

2.26.5 Echo Cancellor

This section provides the requirements for echo control equipment in the UC network. All MG EC devices are required to meet the requirements in the following paragraphs.

2.26.5.1 EC Functionality

SCM-012000 [Required: SC MG, SS MG] The EC shall meet the requirements of ITU T Recommendation G.165, ITU-T Recommendation G.168, and Telcordia Technologies Special Report, SR-2275, Section 7, Transmission.

SCM-012010 [Required: SC MG, SS MG] The EC shall support at least 64 ms echo tail length.

SCM-012020 [Required: SC MG, SS MG] The MOS technique, if applicable, and the perceptual evaluation of speech quality (PESQ) measurement, ITU-T Recommendation P.862 shall be used to assess the clarity of end-to-end voice circuits on which ECs are installed. The voice quality shall have an MOS of 4.0 or better, as measured IAW DOD Information Technology Standards Registry (DISR) voice quality standards.

SCM-012030 [Required: SC MG, SS MG] The MG EC shall be able to determine when a new call is being established and apply echo cancellation IAW this section.

SCM-012040 [Required: SC MG, SS MG] The EC shall have, at a minimum, the following two operational states and they shall be settable by the NMS (see [Section 2.26.5.1.5](#), Device Management), local control interface, or front/back control panel on a per DS0 basis:

- a. Normal. Echo cancellation will remain in the enabled state between calls and during calls unless it is disabled as defined in this section.
- b. Forced Off. In this state the echo canceller shall not enable echo cancellation until the forced-off state has been changed.

2.26.5.2 2100-Hertz EC Disabling Tone Capability

SCM-012050 [Required: SC MG, SS MG] On a per-channel basis, a 2100 Hertz (Hz) disabling tone shall be recognized by the EC, causing the EC to disable, as specified in ITU-T Recommendation G.168.

SCM-012060 [Required: SC MG, SS MG] Re-enabling the EC, after the echo cancellation function has been disabled by the tone, it shall remain in a disabled state until one of the following events occurs.

- a. No single-frequency sinusoid is present as defined in ITU-T Recommendation G.168, Section 7.
- b. The end of the call is detected.
- c. The end of data transmission is detected. This may be detected either by the lack of modem or fax tones on the channel, or by some proprietary method.

SCM-012070 [Required: SC MG, SS MG] Echo cancellers shall be capable of determining when a channel is in use (i.e., a call is active on the channel) or not. This function shall not interfere in any manner with an active call.

SCM-012080 [Required: SC MG, SS MG] The 2100 Hz disabling tone shall override all other control functions and shall disable echo cancellation for that particular call.

2.26.5.3 EC Hardware

SCM-012090 [Required: SC MG, SS MG] The EC shall be able to be connected to either analog and/or digital transmission facilities.

SCM-012100 [Optional: SC MG, SS MG] An analog trunk interface shall be able to provide echo cancellation on a per-trunk basis.

SCM-012110 [Optional: SC MG, SS MG] A digital trunk interface shall be implemented on a digital basis without conversion to analog. The digital EC shall treat all DS0 channels (PCM-24, PCM-30, or more for SONET) independently.

2.26.5.4 Echo Cancellation on PCM Circuits

SCM-012120 [Required: SC MG, SS MG] The PCM-24 or PCM-30 interfaces shall be IAW the requirements in ANSI T1.102, "Digital Hierarchy – Electrical Interfaces" (for PCM-25) and ITU-T Recommendations G.703 and G.732 (for PCM-30).

SCM-012130 [Required: SC MG, SS MG] When the bearer channel is used for 56 or 64 Kbps digital data or submultiples of 64 Kbps, the digital ECs shall not cause a loss of bit integrity.

SCM-012140 [Required: SC MG, SS MG] Echo cancellers inserted in a PCM-24 path using CAS (i.e., "robbed bit") shall have a selectable setting to exclude the signaling bits from the cancellation process.

SCM-012150 [Required: SC MG, SS MG] The EC shall be capable of performing echo cancellation for speech and audio bearer capability calls on the full 64 Kbps signal.

2.26.5.5 Device Management

SCM-012160 [Required: SC MG, SS MG] All UC EC devices will be monitored and managed by the remote VVoIP EMS, as described in [Section 2.19.2](#), Requirements for FCAPS Management.

SCM-012170 [Required: SC MG, SS MG] Echo cancellers shall be capable of performing a self-test diagnostic function on nonactive and active channels on a noninterference basis and report any failures to the assigned EMS.

SCM-012180 [Required: SC MG, SS MG] The EC shall program its echo cancellation capability based on input via a direct connection to the external communications port, or using the front/ back programming panel, or by MG datafill.

2.26.5.6 Reliability

SCM-012190 [Required: SC MG, SS MG] The EC reliability and availability shall conform to Section 5 of Telcordia Technologies GR-512-CORE, as specified for individual devices. The vendor shall provide a reliability model for the system, showing all calculations along with how the overall availability will be met, if requested.

2.26.6 VoIP System Latency for MG Trunk Traffic

The System defined for the requirements in this section is the combination of the SC/SS and its MGs, PEIs and UEIs, IADs, and ATAs. The requirements in this section apply to the system as a whole and not to the individual components of the system.

SCM-012200 [Required: SC, SS] When bearer traffic exits the system via a TDM MG trunk interface, the one-way system latency shall not be greater than 65 ms averaged over any 5-minute period. The latency shall be measured from the EI handset to egress from the system via a TDM trunk. This latency shall be measured for all types of EIs offered by the System.

SCM-012210 [Required: SC, SS] When bearer traffic enters the system via a TDM MG trunk interface, the one-way system latency shall not be greater than 85 ms averaged over any 5-minute period. The latency shall be measured from the system TDM ingress to the EI handset. This latency shall be measured for all types of EIs offered by the System.

2.27 RTS STATEFUL FIREWALL

2.27.1 Introduction

An RTS Stateful Firewall (RSF) is discussed in other UCR sections. For example, the placement of the RSF within the local area network topology is displayed in Figure 4.5-2, Notional Example of Voice, Video, Softphone, Videophone, and Data ASLAN Segmentation. However, the RSF requirements are not specified. The purpose of this section is to specify these requirements.

2.27.2 Role of the RSF

The UCR contains the specifications for a voice and video firewall called an SBC. The SBC is placed at the edge of the enclave B/P/C/S and sits between the LANs and the WAN. The SBC protects voice and video devices from attacks that originate outside of the enclave. The SBC requirements are presented in [Section 2.17](#), SBC.

The role of the RSF is to protect an SC or SS from attacks that originate from inside of the enclave. The Joint Interoperability Test Command (JITC) has validated that SCs and SSs have acceptable Information Assurance risks for most deployments. Therefore, the use of the RSF is not a mandatory requirement. However, some sites may determine that additional protection is required because of the risks associated with their unique scenario. When this occurs, the RSF may be deployed to provide additional protection.

The RSF is considered a UC Approved Products List (APL) product. UC APL products are also called Systems Under Test (SUTs). The RSF is a standalone APL product and therefore a standalone SUT. The RSF SUT is not part of the SC SUT or the SS SUT.

2.27.3 Detailed RSF

2.27.3.1 RSF General

SCM-012220 [Required: RSF] The RSF shall meet all SBC requirements with the exception of the requirements specified in [Section 2.27.3.2](#), RSF Shall Not.

SCM-012230 [Required: RSF] The RSF shall maintain a persistent TLS session with the SBC within the RSF's enclave. Persistent means that the TLS session is established when the RSF system joins the signaling network and is not established on a VVoIP/UC SIP session-by-session basis.

SCM-012240 [Required: RSF] The RSF shall fulfill the same availability requirements as the SC that the RSF is protecting. If the SC's availability requirement is 99.999, then the RSF's availability requirement is also 99.999.

NOTE: With a few exceptions, the RSF and the SBC perform the same functions. The functions performed by the RSF are a very large subset of the functions performed by the SBC. These functions are performed by the same hardware and software on both the RSF and the SBC. Although the software is the same, the RSF's software configuration is a little different from the SBC's software configuration.

The hardware configuration used at a specific site is determined by the site's specific availability requirements, as defined in [Section 2.17.6](#), Availability. At a specific site, both the RSF and the SBC are subject to the same availability requirements. Although the availability requirements are the same, appliances from different vendors may be used. Using the same vendor's appliance for the RSF and the SBC is not required.

The SBC functions that the RSF shall not perform are presented in [Section 2.27.2](#), Role of the RSF. Because the RSF is not part of the SC or SS SUT, the RSF shall not participate in the SS failover process and shall not perform NAT/NAPT.

2.27.3.2 RSF Shall Not

SCM-012250 [Shall Not: RSF] The RSF shall not take any corrective actions upon the SC failover from the primary SS to the secondary SS. The SBC-required actions upon failover from the primary SS to the secondary SS are described in [Section 2.6](#). The RSF shall not perform these actions.

SCM-012260 [Shall Not: RSF] The RSF shall not bidirectionally anchor (NAT and/or NAPT) the media associated with a voice or video session that originates or terminates within its enclave. The SBC requirements for bidirectionally anchoring the media are described in Sections 2.17.1-1a, 1b, and 1c. The RSF shall not perform these actions.

SCM-012270 [Shall Not: RSF] The RSF shall not maintain a persistent TLS session with SBCs that are outside of the RSF's enclave. The SBC's requirements for maintaining persistent TLS connections with SBCs that are outside of the local enclave are described in Sections 2.17.1-6a and 6b. The RSF shall not perform these actions.