DEFENSE INFORMATION SYSTEMS AGENCY
P. O. BOX 549
FORT MEADE, MARYLAND 20755-0549

IN REPLY REFER TO: Joint Interoperability Test Command (JTE) **9 Sep 13**

MEMORANDUM FOR DISTRIBUTION Errata 1.1 (Enclosure 4)

SUBJECT: Joint Interoperability Certification of the Microsoft Lync Release 2013

References: (a) Department of Defense Instruction 8100.04, "DoD Unified Capabilities (UC)," 9 December 2010
(b) DoD CIO, Memorandum, "Interim Guidance for Interoperability of Information Technology (IT) and National Security Systems (NSS)," 27 March 2012
(c) through (e), see Enclosure 1

1. **Certification Authority.** References (a) and (b) establish the Joint Interoperability Test Command (JITC) as the Joint Interoperability Certification Authority for the Unified Capabilities (UC) products.

2. **Conditions of Certification.** Microsoft Lync Release 2013; hereinafter referred to as the System Under Test (SUT), meets all of the critical requirements of the Unified Capabilities Requirements (UCR), Reference (c), and is certified for joint use as a UC Collaboration Product over a Local Area Network (LAN) or Wide Area Network (WAN). In addition, the SUT is certified for non-assured services voice and video over internet protocol (VVoIP) between SUT Lync clients and non-assured services voice over internet protocol (VoIP) between the SUT Lync clients and VoIP end instruments within the UC Network with the conditions described in Table 1. This certification expires upon changes that affect interoperability, but no later than three years from the date of this memorandum.

Table 1. Conditions

Condition	Operational Impact	Remarks
UCR Waivers		
None.		
Conditions of Fielding		
Due to limitations with IPv6 via the SUT SBC, the SUT is certified for IPv4 only via the SBC to the UC network	None	
Open Test Discrepancies		
The SUT SBC partially complies with IA-004010 requirement.	Minor	See note 1.
The SUT SBC does not meet the IP infrastructure requirements.	Minor	See note 2.

Table 1. Conditions (continued)

NOTES:
1. The SUT SBC supports real-time logging; however, it does not get to the port level. DISA accepted the vendor's POA&M and adjudicated this as minor.
2. The SUT SBC is not capable of sending an automated alert when installed certificates corresponding to trust chains, OCSP responder certificates, or any other certificates are nearing expiration. DISA accepted the vendor's POA&M and adjudicated this as minor.

LEGEND:

DISA	Defense Information Systems Agency	POA&M	Plan of Actions and Milestones
IA	Information Assurance	SBC	Session Border Controller
IP	Internet Protocol	SUT	System Under Test
IPv4	Internet Protocol version 4	UC	Unified Capabilities
IPv6	Internet Protocol version 6	UCR	Unified Capabilities Requirements
OCSP	Online Certificate Status Protocol		

3. **Interoperability Status.** Table 2 provides the SUT interface interoperability status and Table 3 provides the Capability Requirements (CR) and Functional Requirements (FR) status. Table 4 provides a Unified Capabilities (UC) Approved Products List (APL) product summary.

Table 2. Interface Status

Interface	Threshold CR/FR Requirements (See note 1.)	Status	Remarks
Network Management Interfaces			
IEEE 802.3i (10BaseT UTP) (C) (See note 2.)	1	Met	
IEEE 802.3u (100BaseT UTP) (C) (See note 2.)	1	Met	
IEEE 802.3ab (1000BaseT UTP) (C) (See note 2.)	1	Met	
UC Network Interfaces			
IEEE 802.3i (10BaseT UTP) (C) (See note 2.)	1, 2, 3, and 4	Partially Met	See note 3.
IEEE 802.3u (100BaseT UTP) (C) (See note 2.)	1, 2, 3, and 4	Partially Met	See note 3.
IEEE 802.3ab (1000BaseT UTP) (C) (See note 2.)	1, 2, 3, and 4	Partially Met	See note 3.
DISN Legacy Interfaces			
North American ISDN PRI (C)	1 and 2	Not Tested	
European ISDN (C)	1 and 2	Not Tested	
2-wire analog (C)	1 and 2	Not Tested	
Client Interfaces			
IEEE 802.3i (10BaseT UTP) (C) (See note 2.)	1, 2, 3, and 4	Partially Met	See note 3.
IEEE 802.3u (100BaseT UTP) (C) (See note 2.)	1, 2, 3, and 4	Partially Met	See note 3.

NOTES:
1. The SUT high-level CR and FR ID numbers depicted in the Threshold CRs/FRs column can be cross-referenced in Table 3. These high-level CR/FR requirements refer to a detailed list of requirements provided in Enclosure 3.
2. The SUT must provide a minimum of one of the listed interfaces.
3. The SUT partially meets the interoperability requirements related to SUT Information Assurance detailed in UCR 2013 section 4.2.3 and 4.2.7. The SUT SBC does not support real-time logging at the port level. The SUT SBC does not send an alert when installed certificates are nearing expiration. DISA accepted the vendor's POA&M and adjudicated these as minor.

LEGEND:

802.3i	10BaseT Mbps over twisted pair	DISN	Defense Information Systems Network
802.3u	Standard for 100 Mbps Ethernet	FR	Functional Requirement
802.3ab	1000BaseT Gbps Ethernet over twisted pair at 1 Gbps (125 Mbps)	Gbps	Gigabits per second
		IEEE	Institute of Electrical and Electronics Engineers
10BaseT	10 Mbps (Baseband Operation, Twisted Pair) Ethernet	ISDN	Integrated Services Digital Network
100BaseT	100 Mbps (Baseband Operation, Twisted Pair) Ethernet	POA&M	Plan of Actions and Milestones
		PRI	Primary Rate Interface
1000BaseT	1000 Mbps (Baseband Operation, Twisted Pair) Ethernet	R	Required
		SBC	Session Border Controller
C	Conditional	UC	Unified Capabilities
CR	Capability Requirement	UCR	Unified Capabilities Requirements
DISA	Defense Information Systems Agency	UTP	Unshielded Twisted Pair

Table 3. SUT Capability Requirements and Functional Requirements Status

CR/FR ID	UCR Requirement (High-Level) (See note 1.)	UCR 2013 Reference	Status
1	Voice and Video Collaboration Tool Requirements (R)	3.9.2	Met
2	Optional Voice and Video Collaboration Tool Requirements (O)	3.9.3	Partially Met (See note 2.)
3	IM/Chat/Presence Collaboration Product Requirements (CRe)	3.9.4	Partially Met (See note 3.)
4	Information Assurance (CRe)	4	Partially Met (See note 4.)

NOTES:
1. The annotation of 'required' refers to a high-level requirement category. The applicability of each sub-requirement is provided in Enclosure 3.
2. The SUT was not tested for inter-enclave video over IP via the SBC and therefore, it is not covered under this certification. The SUT does not support the optional Session Admission Control requirements.
3. The SUT offers an XMPP Gateway; however, this was not tested and it is not covered under this certification. This is an optional requirement.
4. The interoperability requirements related to Information Assurance are verified by the vendor's LoC. The SUT partially meets the interoperability requirements related to SUT Information Assurance detailed in UCR 2013 section 4.2.3 and 4.2.7. The SUT SBC does not support real-time logging at the port level. The SUT SBC does not send an alert when installed certificates are nearing expiration. DISA accepted the vendor's POA&M and adjudicated these as minor.

LEGEND:

CR	Capability Requirement	O	Optional
CRe	Conditionally Required	R	Required
DISA	Defense Information Systems Agency	SBC	Session Border Controller
FR	Functional Requirement	SUT	System Under Test
ID	Identification	UCR	Unified Capabilities Requirements
IP	Internet Protocol	XMPP	Extensible Messaging and Presence Protocol
LoC	Letters of Compliance		

Table 4. UC APL Product Summary

Product Identification			
Product Name	Microsoft Lync		
Software Release	Server 2013		
UC Product Type(s)	UC Collaboration Product		
Product Description	The Microsoft Lync Rel. 2013 is a UC Collaboration Product (CP) that supports collaboration between other Microsoft Lync IP-based end users using Voice and Video over IP sessions, Presence/Instant Messaging (IM)/Chat sessions, and other collaborative sessions such as Whiteboard Sharing, Document Sharing, and Virtual meetings.		
Product Components (See note 1.)	**Component Name**	**Version**	**Remarks**
Microsoft Lync Server	Lync 2013 Server	5.0.8308 64-bit	
Microsoft Lync Client	Lync 2013 Client	15.0.4481.1000 MSO 64-bit	
SBC	Acme Packet Net-Net 4500 SD EBC	S-CX6.3.0.MR-5 GA (Build 573)	See note 2.
Workstation	Dell Latitude E6430	Windows 7 Enterprise SP1 64-bit	
Phone	Polycom CX 300	01.20.7.03	

NOTES:
1. The detailed component and subcomponent list is provided in Enclosure 3.
2. The SUT was tested with the Acme Packet Net-Net 4500 SD. However, the 3820 utilizes the same software and similar hardware and JITC analysis determined it to be functionally identical for interoperability certification purposes and the 3820 is also covered under this certification for use with the SUT. In addition, the SUT is certified with any 4500 or 3820 with this release or later that is on the UC APL.

LEGEND:

APL	Approved Products List	JITC	Joint Interoperability Test Command
EBC	Edge Boundary Controller	UC	Unified Capabilities
IP	Internet Protocol		

4. **Test Details.** This finding is based on interoperability testing, DISA adjudication of open test discrepancy reports (TDRs), review of the vendor's Letters of Compliance (LoC), and DISA Certifying Authority (CA) Recommendation for inclusion on the UC APL. Testing was conducted at JITC's Global Information Grid Network Test Facility at Fort Huachuca, Arizona,

from 13 through 24 May 2013 using test procedures derived from Reference (d). Additional testing was conducted 16 August 2013. DISA adjudication of outstanding TDRs was completed on 13 August 2013. Review of the vendor's LoC was completed on 17 May 2013. The DISA CA provided a positive Recommendation on 16 July 2013 based on the security testing completed by DISA-led IA test teams and the results published in a separate report, Reference (e). Enclosure 2 documents the test results and describes the tested network and system configurations. Enclosure 3 provides a detailed list of the interface, capability, and functional requirements. Enclosure 4 provides a list of errata changes to this certification since the original signature date.

5. **Additional Information.** JITC distributes interoperability information via the JITC Electronic Report Distribution (ERD) system, which uses Sensitive but Unclassified IP Data (formerly known as NIPRNet) e-mail. Interoperability status information is available via the JITC System Tracking Program (STP). STP is accessible by .mil/.gov users at https://stp.fhu.disa.mil/. Test reports, lessons learned, and related testing documents and references are on the JITC Joint Interoperability Tool (JIT) at https://jit.fhu.disa.mil/. Due to the sensitivity of the information, the Information Assurance Accreditation Package (IAAP) that contains the approved configuration and deployment guide must be requested directly from the Unified Capabilities Certification Office (UCCO), e-mail: disa.meade.ns.list.unified-capabilities-certification-office@mail.mil. All associated information is available on the DISA UCCO website located at http://www.disa.mil/Services/Network-Services/UCCO.

6. **Point of Contact (POC).** The JITC point of contact is CPT James Torres, commercial telephone (520) 538-5575, DSN telephone 879-5575, FAX DSN 879-4347; e-mail address james.m.torres.mil@mail.mil; mailing address Joint Interoperability Test Command, ATTN: JTE (CPT James Torres) P.O. Box 12798, Fort Huachuca, AZ 85670-2798. The UCCO tracking number for the SUT is 1303201.

FOR THE COMMANDER:

3 Enclosures a/s

for RICHARD A. MEADOR
Chief
Battlespace Communications Portfolio

Distribution (electronic mail):
DoD CIO
Joint Staff J-6, JCS
USD(AT&L)
ISG Secretariat, DISA, JTA
U.S. Strategic Command, J665
US Navy, OPNAV N2/N6FP12
US Army, DA-OSA, CIO/G-6 ASA(ALT), SAIS-IOQ
US Air Force, A3CNN/A6CNN
US Marine Corps, MARCORSYSCOM, SIAT, A&CE Division
US Coast Guard, CG-64
DISA/TEMC
DIA, Office of the Acquisition Executive
NSG Interoperability Assessment Team
DOT&E, Netcentric Systems and Naval Warfare
Medical Health Systems, JMIS IV&V
HQUSAISEC, AMSEL-IE-IS
UCCO

ADDITIONAL REFERENCES

(c) Office of the Department of Defense Chief Information Officer, "Department of Defense Unified Capabilities Requirements 2013," January 2013
(d) Joint Interoperability Test Command, "Unified Capabilities Test Plan (UCTP)," Draft
(e) Joint Interoperability Test Command, "Information Assurance (IA) Assessment of Microsoft Lync Release (Rel.) 2013 (Tracking Number: 1303201)," Draft

CERTIFICATION SUMMARY

1. SYSTEM AND REQUIREMENTS IDENTIFICATION. The Microsoft Lync Release 2013 is hereinafter referred to as the System Under Test (SUT). Table 2-1 depicts the SUT identifying information and requirements source.

Table 2-1. System and Requirements Identification

System Identification	
Sponsor	Defense Information System Agency
Sponsor Point of Contact	Louis Schmuckler, Address: P.O. Box 549, Fort Meade, Maryland 20755-0549, e-mail: Louis.a.schmuckler.civ@mail.mil
Vendor Point of Contact	Victor Akinnagbe, Microsoft, 12012 Sunset Hills Road, Reston, VA 20190, e-mail: victor.a@microsoft.com
System Name	Microsoft Lync
Increment and/or Version	Server 2013
Product Category	Unified Capabilities (UC) Collaboration Product
System Background	
Previous certifications	None.
Tracking	
UCCO ID	1303201
System Tracking Program ID	4286
Requirements Source	
Unified Capabilities Requirements	Unified Capabilities Requirements 2013
Remarks	
Test Organization(s)	Joint Interoperability Test Command, Fort Huachuca, Arizona
LEGEND: ID Identification UCCO Unified Capabilities Connection Office	

2. SYSTEM DESCRIPTION. Unified Capabilities (UC) Collaboration Products (CP) are an enterprise-ready UC product that provide one or more collaborative services (e.g., voice, video, chat, etc…). These products connect Department of Defense (DoD) users via their desktop collaboration software as part of their everyday productivity experience. These collaboration products provide a consistent, single client experience for presence, instant messaging, voice, video and data sharing. The SUT supports collaboration between Internet Protocol (IP)-based end users using voice and video over Internet protocol (VVoIP) sessions, presence/Instant Messaging (IM)/chat sessions, and other collaborative sessions such as whiteboard sharing, document sharing, and virtual meetings.

The Microsoft Lync 2013 SE Server is the CP Server component of the SUT. It supports the system's access to the enterprise infrastructure and provides IM, presence, file transfer, and multiparty voice and video calling, ad hoc and structured conferences (audio and video) to Lync Clients. The SUT connectivity to the Public Switched Telephone Network, as well as the enterprise Session Initiation Protocol network, functions through the Microsoft Lync Rel. 2013 SE Server.

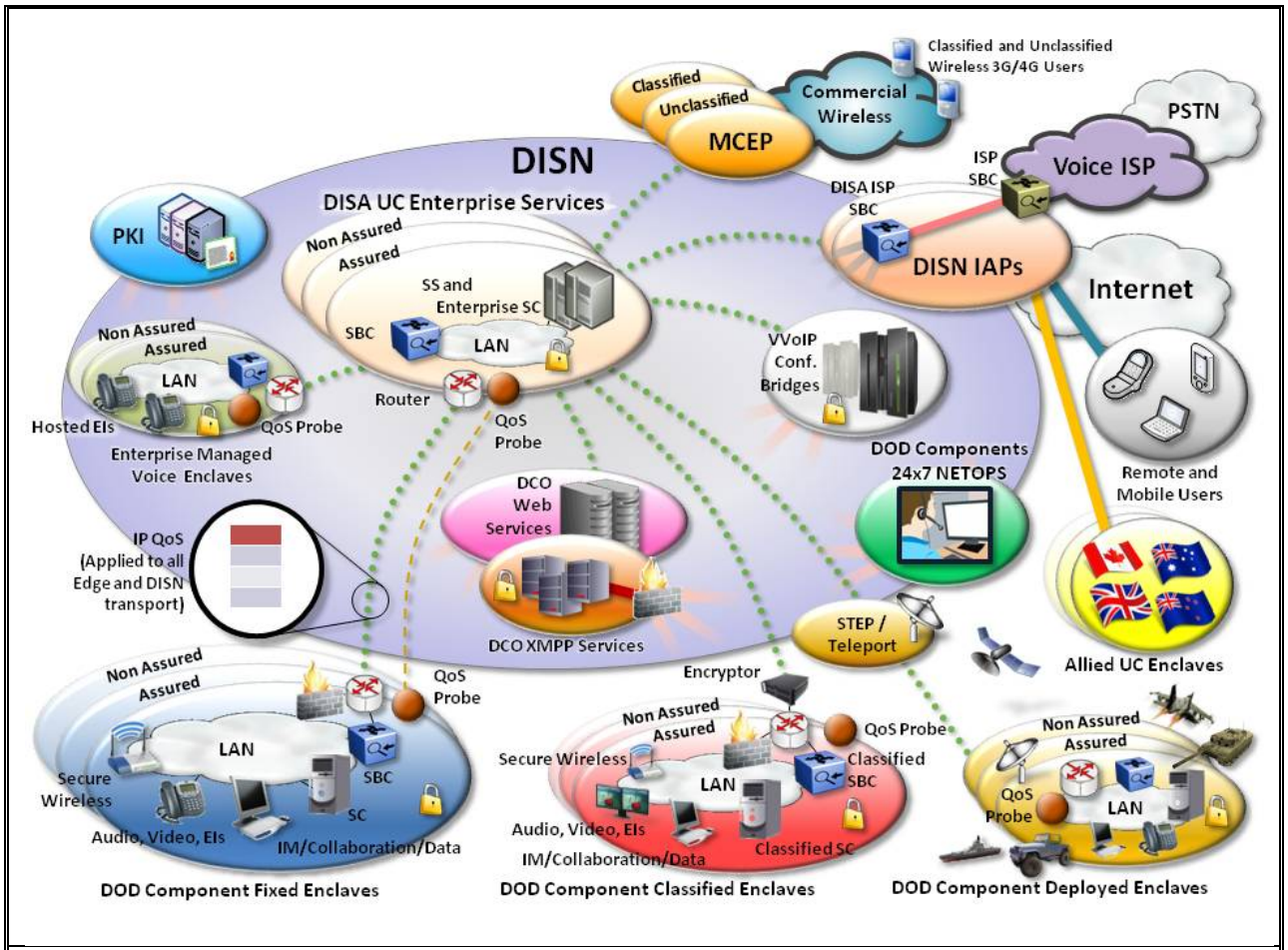
The Lync Client is the CP Client component of the SUT. The Lync Client is a site-provided Security Technical Implementation Guides (STIG)-compliant and Common Access Card (CAC)-enabled Windows 7 Service Pack 1 workstation or laptop with the Microsoft Lync Rel. 2013 client software installed. The Lync Client software provides users Instant Messaging, Presence, file transfer, and multiparty voice and video calling, ad hoc and structured conferences (audio and video). Use of many adjunct devices such as Universal Serial Bus (USB) handsets and headsets are provided by the Lync Client. The system was tested with a Polycom CX300 USB handset device. However, the SUT is certified for use with any USB phones identified on the Microsoft website as Microsoft-certified with the Lync.

The CP Session Border Controller (SBC) gives the CP clients and CP server access to a Session Controller in the UC Network by providing the SIP to AS-SIP conversion. The SUT SBC is an Acme Packet Net-Net 4500 SD Edge Boundary Controller (EBC) with a unique software release. The SBC includes the ETC card, which supports both single- and dual-side rekeying. The SUT was tested with the Acme Packet Net-Net 4500 SD with release S-CX6.3.0.MR-5 GA (Build 573). However, the 3820 utilizes the same software and similar hardware and JITC analysis determined it to be functionally identical for interoperability certification purposes and the 3820 is also covered under this certification for use with the SUT. In addition, the SUT is certified with any 4500 or 3820 with this release or later that is on the UC Approved Products List (APL).

3. OPERATIONAL ARCHITECTURE. The UC architecture is a two-level network hierarchy consisting of Defense Information Systems Network (DISN) backbone switches and Service/Agency installation switches. The Department of Defense (DoD) Chief Information Officer (CIO) and Joint Staff policy and subscriber mission requirements determine which type of switch can be used at a particular location. The UC architecture, therefore, consists of several categories of switches. Figure 2-1 depicts the notional operational UC architecture that the SUT may be used in and Figure 2-2 the UC CP functional model.

4. TEST CONFIGURATION. The test team tested the SUT at JITC, Fort Huachuca, Arizona in a manner and configuration similar to that of a notional operational environment. Testing of the system's required functions and features was conducted using the test configuration depicted in Figure 2-3. Testing was conducted after Information Assurance (IA) testing using the same configuration.

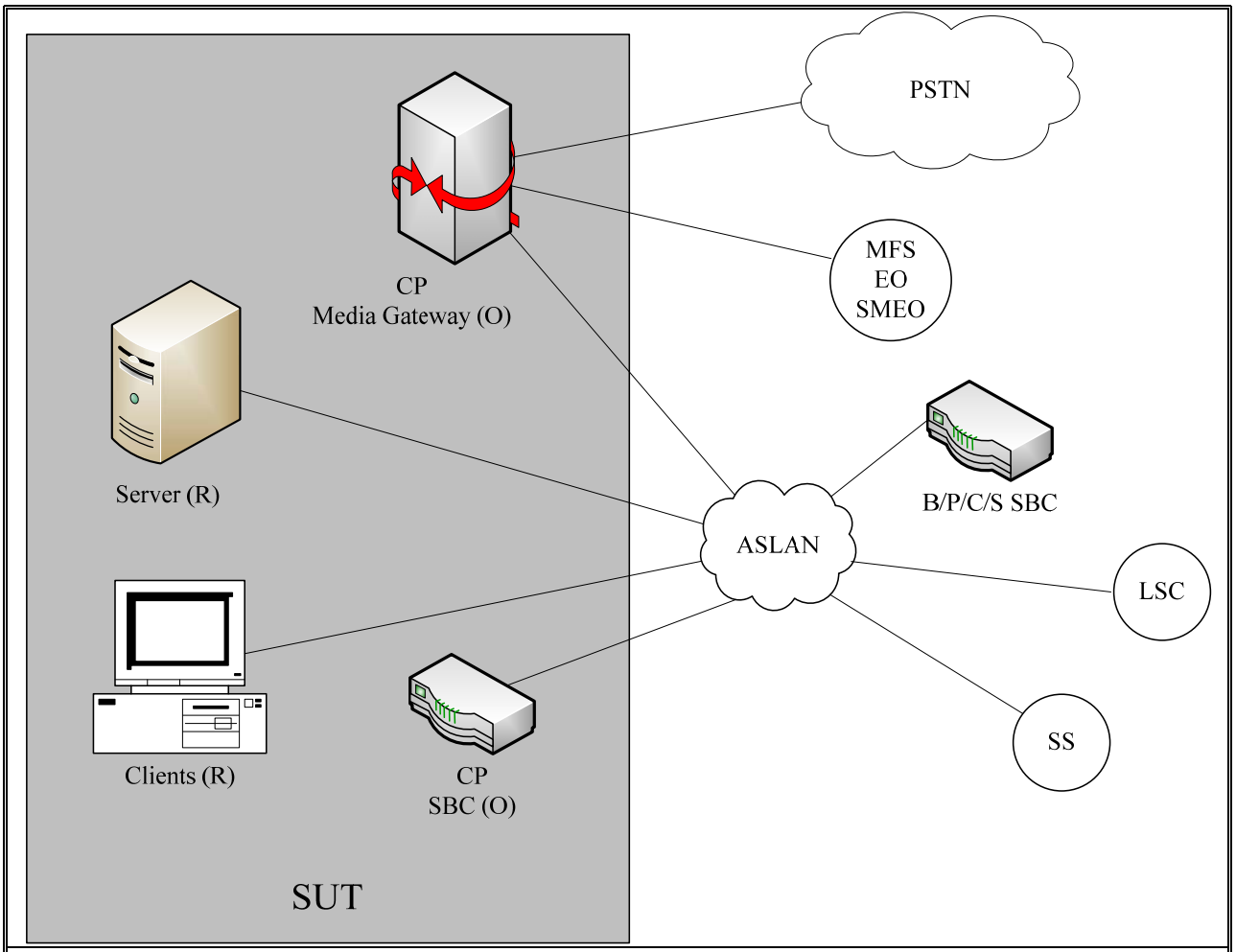
5. METHODOLOGY. Testing was conducted using UC Collaboration Tool (CP) requirements derived from the Unified Capabilities Requirements (UCR) 2013, Reference (c), and UC Collaboration Tool test procedures, Reference (d). Any discrepancies noted were written up in Test Discrepancy Reports (TDRs). The vendor submitted Plan of Action and Milestones (POA&M) as required. The remaining open TDRs were adjudicated by DISA as minor. Any new discrepancy noted in the operational environment will be evaluated for impact on the existing certification. These discrepancies will be adjudicated to the satisfaction of DISA via a vendor POA&M, which will address all new critical TDRs within 120 days of identification.



LEGEND:

DCO	Defense Connection Online	NETOPS	Network Operations
DISA	Defense Information Systems Agency	PKI	Public Key Infrastructure
DISN	Defense Information Systems Network	PSTN	Public Switched Telephone Network
DoD	Department of Defense	QoS	Quality of Service
EI	End Instrument	SBC	Session Border Controller
IAP	Internet Access Point	SC	Session Controller
IM	Instant Messaging	SS	Softswitch
IP	Internet Protocol	STEP	Standardized Tactical Entry Point
ISP	Internet Service Provider	UC	Unified Capabilities
LAN	Local Area Network	VVoIP	Voice and Video over IP
MCEP	Multi Carrier Entry Point	XMPP	Extensible Messaging and Presence Protocol

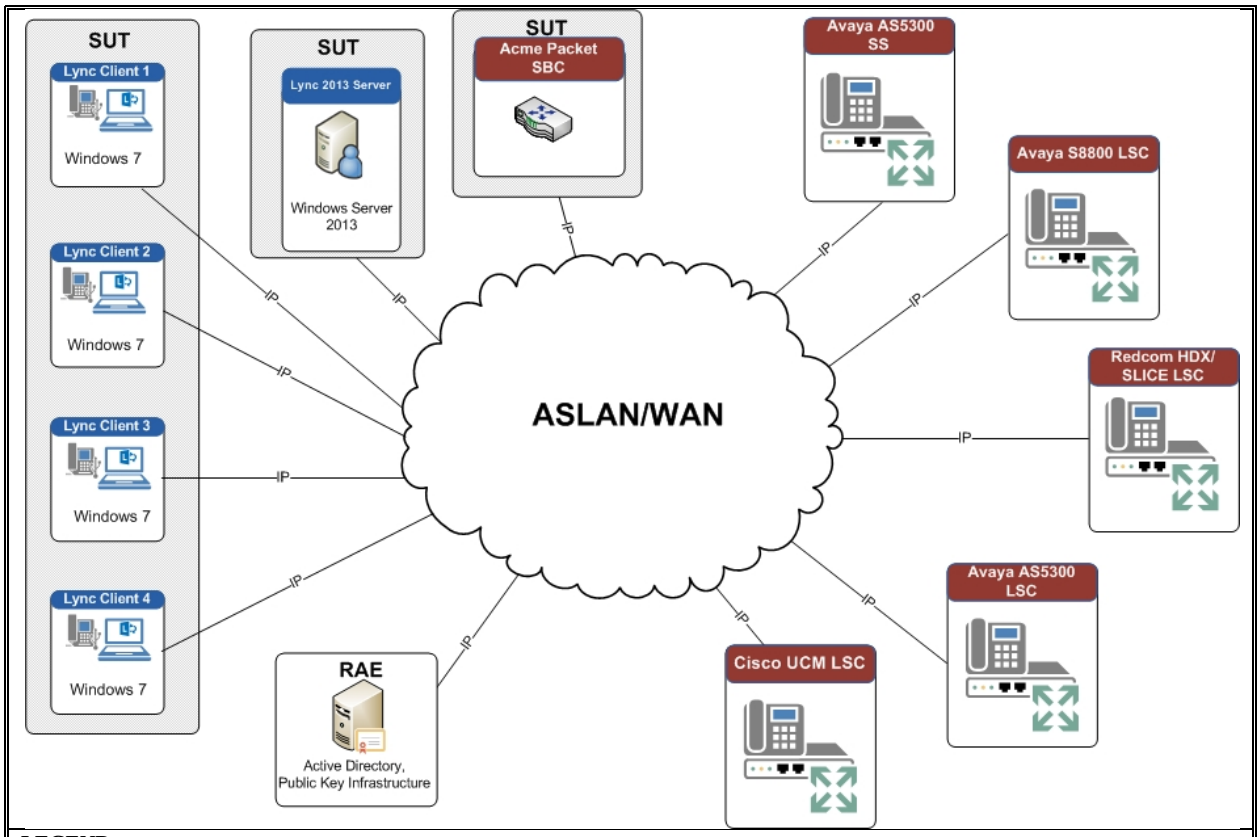
Figure 2-1. Notional UC Network Architecture



LEGEND:

ASLAN	Assured Services Local Area Network	PSTN	Public Switched Telephone Network
B/C/P/S	Base/Camp/Post/Station	R	Required
CP	Collaboration Product	SBC	Session Border Controller
EO	End Office	SMEO	Small End Office
LSC	Local Session Controller	SS	SoftSwitch
MFS	Multifunction Switch	SUT	System Under Test
O	Optional		

Figure 2-2. UC Collaboration Tool Functional Reference Model



LEGEND:

ASLAN	Assure Service Local Area Network	SC	Session Controller
LSC	Local Session Controller	SS	Soft Switch
HDX	High Density Exchange	SUT	System Under Test
IP	Internet Protocol	UCM	Unified Communications Manager
RAE	Required Ancillary Equipment	WAN	Wide Area Network
SBC	Session Border Controller		

Figure 2-3. SUT Test Configuration

6. INTEROPERABILITY REQUIREMENTS, RESULTS, AND ANALYSIS. The interface, Capability Requirements (CR) and Functional Requirements (FR), IA, and other requirements for the UC CP are established by UCR 2013, sections 3.9.2, 3.9.3, 3.9.4, 4 and 5.

a. Voice and Video Collaboration Tool Requirements. Section 3.9.2 provides the detailed requirements for voice and video features.

(1) **Point-to-Point Voice Calls Between Collaboration Tool Clients.** Section 3.9.2.1 provides the point-to-point voice requirements. The CP shall support the establishment of point-to-point Voice over IP (VoIP) calls between clients that are served by the server. The CP shall allow one client to set up a point-to-point VoIP call with another CP client. The CP shall allow the first CP to call the second CP client by entering the second client's phone number, by entering the second client's username, or by looking up the second client in a User Directory on the CP server. The SUT met this requirement with testing.

(2) **Add Voice Call to Existing Collaboration Session.** Section 3.9.2.2 states that when two CP clients have an existing collaboration session established through the CP server (e.g., a Presence/IM/Chat session, a whiteboard session, or a document sharing session), the CP shall allow either one of the CP clients to add a VoIP call with the other CP client to that existing session. The CP shall also allow either of the CP clients to later drop the VoIP call from that session, returning the session to its original type (e.g., Presence/IM/Chat, whiteboard, or document sharing). The SUT met this requirement with testing.

(3) Point-to-Point Video Calls Between Collaboration Tool Clients. Section 3.9.2.3 states that the CP shall support the establishment of point-to-point video over IP calls between CP clients that are served by the CP server. The CP shall allow one CP client to set up a point-to-point video over IP call with another CP client. The CP shall allow the first CP client to call the second CP client by entering the second client's phone number, entering the second client's username, or looking up the second client in the User Directory on the CP server. The SUT met this requirement with testing for intra-enclave point-to-point video over IP between the SUT CP Clients.

(4) Add Video Call to Existing Collaboration Session. Section 3.9.2.4 states that when two CP clients have an existing collaboration session established through the CP server (e.g., a Presence/IM/Chat session, a whiteboard session, or a document sharing session), the CP shall allow either one of the CP clients to add a video over IP call with the other CP client to that existing session. The CP shall also allow either of the CP clients to later drop the video over IP call from that session, returning the session to its original type (e.g., Presence/IM/Chat, whiteboard, or document sharing). The SUT met this requirement with testing.

(5) Proprietary Client <->Server Signaling and Client <->Client Media. Section 3.9.2.5, includes requirements for client and server signaling.

(a) For VoIP sessions between CP clients, the CP client and the CP server shall support the establishment and tear-down of the VoIP sessions, using signaling messages that are proprietary to the CP. The SUT met this requirement with testing.

(b) For video over IP sessions between CP clients, the CP client and the CP server shall support the establishment and tear-down of video over IP sessions, using signaling messages that are proprietary to the CP. The SUT met this requirement with testing.

(c) For voice calls that traverse the CP MG, the CP server and the CP MG shall support the establishment and tear-down of the VoIP sessions, using signaling messages that are proprietary to the CP. The SUT does not offer a CP MG.

(d) For voice calls that traverse the CP SBC, the CP server and the CP SBC shall support the establishment and tear-down of the VoIP sessions, using signaling messages that are proprietary to the CP. The SUT met this requirement with testing. The SUT includes the Acme packet SBC for this functionality.

(e) For video calls that traverse the CP SBC, the CP server and the CP SBC shall support the establishment and tear-down of the video over IP sessions, using signaling messages that are proprietary to the CP. Support for AS-SIP signaling over TLS within the CP (i.e., between one product component and another) is not required. Support for commercial SIP signaling over TLS within the CP is allowed but is not required. Since different product vendors generally support different versions of commercial SIP signaling, commercial SIP signaling is considered proprietary signaling. The SUT was not tested for inter-enclave video over IP via the SBC and therefore, it is not covered under this certification.

(f) For VoIP sessions between CP clients, the clients shall support the exchange of VoIP media packets, using media protocols that are proprietary to the CP. Support of industry-standard media protocols is also allowed. The SUT met the requirement through testing with proprietary media protocols.

(g) For video over IP sessions between CP clients, the clients shall support the exchange of video over IP media packets, using media protocols that are proprietary to the CP. Support of industry-standard media protocols is also allowed. The SUT does not offer a MG interface, therefore this interface is not covered under this certification.

(h) For voice calls that traverse the CP MG, the CP client and the CP MG shall support the exchange of VoIP media packets, using media protocols that are proprietary to the CP. Support of industry-standard media protocols is also allowed. The SUT does not offer a CP MG.

(i) For voice calls that traverse the CP SBC, the CP Client and the CP SBC shall support the exchange of video over IP media packets, using media protocols that are proprietary to the CP. Support of industry-standard media protocols is also allowed. The SUT was not tested for inter-enclave video over IP via the SBC and therefore, it is not covered under this certification.

(j) For video calls that traverse the CP SBC, the CP client and the CP SBC shall support the exchange of video over IP media packets, using media protocols that are proprietary to the CP. Support of industry-standard media protocols is also allowed. Support for SRTP-based media within the CP (i.e., between one product component and another) is allowed, but is not required. Examples of SRTP-based media are G.711 over SRTP and G.729 over SRTP for VoIP sessions, and H.263 over SRTP and H.264 over SRTP for video sessions. The SRTP-based media within the CP can be either industry-standard media (such as the aforementioned G.7XX and H.26X media), or non-standard media that is proprietary to the CP. The SUT was not tested for inter-enclave video over IP via the SBC and therefore, it is not covered under this certification.

(6) Local Directory Service for CP Users. Section 3.9.2.6 contains requirements for Local Directory Service (LDS) for CP users.

(a) The CP shall provide a LDS for the CP users (the end users of the CP clients and the CP server). The LDS shall allow the CP users to look up information about each other

based on the users' Name, Phone Number, and E-mail Address values. The SUT met this requirement with testing.

(b) The CP LDS shall support the following functions:

1. The CP shall support a Directory Look-Up function that shall allow a user assigned to a CP to look up the telephone numbers of other users assigned to (i.e., served by) that CP. This function is referred to as "white pages" service. The SUT met this requirement with testing.

2. For security reasons, the Directory Look-Up function shall be available only from a user's CP client and not from other user devices outside the CP. The SUT met this requirement with testing.

3. The CP shall allow the system administrator to update the directory database in response to subscriber data changes (i.e., subscriber adds, modifications, or removals). The CP shall update the white pages data automatically whenever the subscriber information is updated. The SUT met this requirement with testing.

(7) IPv6 Support. Section 3.9.2.7 states that the source for the IPv6 Support Requirements for CP clients and servers is Section 5, IPv6. This was met with testing and the vendor's LoC. However, due to limitations with IPv6 via the SUT SBC, the SUT is certified for IPv4 only via the SBC to the UC network.

(a) The CP client shall meet all of the IPv6 protocol requirements for End Instrument (EI) products in Section 5, IPv6, including the requirements in Table 5.2-3, UC EIs. This includes EI Conditional Requirements, when the Condition specified for the EI also applies to the CP client. This was met with testing and the vendor's LoC.

(b) The CP server shall meet all the IPv6 protocol requirements for Network Appliances and Simple Servers (NA/SS) products in Section 5, IPv6, including the requirements in Table 5.2-4, UC Network Appliances and Simple Servers (NA/SS). This includes NA/SS Conditional Requirements, when the Condition specified for the NA/SS also applies to the CP server. This was met with testing and the vendor's LoC.

(8) QoS for Video over IP and VoIP Sessions. Section 3.9.2.8 states that the CP client, server, MG, and SBC shall provide Quality of Service (QoS) for VoIP sessions and video over IP Sessions, through the setting of Differentiated Services Code Points (DSCPs) in VVoIP signaling streams and VVoIP media streams. Additionally, CP support for the VVoIP Signaling and Media DSCPs, specified in Section 6.3.2 and Table 6.3.2 for precedence voice is optional. The SUT met this requirement with testing.

(9) Information Assurance. Section 3.9.2.9 states that the CP and its components shall meet the Information Assurance requirements of all applicable DISA STIGs. Security is tested by DISA-led Information Assurance test teams and the results published in a separate report, Reference (e). Additional IA requirements are addressed in subparagraph "6.d." below.

(10) SNMPv3 Alarms for Remote Monitoring. Section 3.9.2.10 states that the CP must support Simple Network Management Protocol (SNMP) version 3 (SNMPv3) alarms for remote monitoring. The SUT met the requirements with testing and the vendor's LoC for a CP server and SBC. The SUT does not offer a CP MG, and therefore, the MG requirements do not apply.

(a) The CP server, MG, and SBC shall support generation and transmission of SNMPv3 alarms for remote monitoring.

(b) The CP server, MG, and SBC shall generate alarm messages that are distinguishable from administrative log messages.

(c) The CP server, MG, and SBC shall detect their own fault (alarm) conditions.

(d) The CP server, MG, and SBC shall generate alarm notifications.

(e) The CP Server, MG, and SBC shall send the alarm messages in Near-Real Time (NRT). More than 99 percent of alarms shall be detected and reported in NRT. NRT is defined as event detection and alarm reporting within 5 seconds of the event, excluding transport time.

(f) The CP server, MG, and SBC shall send the alarm messages in SNMPv3 format.

b. Optional Voice and Video Collaboration Tool Requirements. Section 3.9.3 outlines the optional voice and video requirements that a CP may support. The paragraphs below specify the optional requirements.

(1) Section 3.9.3.1 specifies the optional voice call features (call forwarding, call transfer, call hold, three way calling, and calling number delivery) requirements.

(a) Section 3.9.3.1.1 states that three types of CF features are applicable for UC CPs: Call Forwarding Variable (CFV), Call Forwarding Busy Line (CFBL), and Call Forwarding – Don't Answer – All Calls (CFDA). Reminder Ring for all call forwarding features, as specified in Telcordia Technologies GR-217-CORE, GR-580-CORE, and GR-586-CORE, shall be supported. CFV shall be supported IAW Telcordia Technologies GR-580-CORE. CFBL shall be supported IAW Telcordia Technologies GR-586-CORE. CFDA shall be supported IAW Telcordia Technologies GR-586-CORE. The SUT met the requirements with testing and the vendor's LoC.

(b) Section 3.9.3.1.2 states that the collaboration product shall support two types of call transfers for voice calls: normal and explicit. A normal call transfer is a transfer of an incoming voice call from a CP end user to another party (another CP end user, a DSN phone number, or a commercial phone number). An explicit call transfer is the CP end user's transfer of two existing calls together, when both of these calls were originated by the CP end user. The SUT met this requirement with testing.

(c) Section 3.9.3.1.3 states that the CP shall support the Call Hold feature for voice calls. Call Hold shall support the capabilities in the following subparagraphs. The SUT met the following requirements with testing.

1. End user can place an active voice call on hold.

2. End user can retrieve a held voice call, making it an active voice call again.

3. End user can have multiple voice calls on hold at the same time.

4. Notifications from the CP to the end user that their held call is still on hold. (e.g., when a user's active call ends and the user's held call is still on hold, the CP should notify the user that the held call is still established and is still on hold).

(d) Section 3.9.3.1.4 states that the CP shall support the Three-Way Calling feature for voice calls. Three-Way Calling shall support the following capabilities:

1. End user can place an active voice call on hold, launch an outgoing voice call, and merge the two voice calls together into a three-way call. The SUT met this requirement with testing.

2. End user can place an active voice call on hold, answer an incoming voice call, and merge the two voice calls together into a three-way call. The SUT met this requirement with testing.

3. Place a three-way call on hold and retrieve a three-way call from hold. The SUT met this requirement with testing.

4. If the CP uses SIP for voice call establishment, then the product shall support the Three-Way Calling feature consistent with sections 2.10 and 2.11 of Request for Comment (RFC) 5359. The SUT met this requirement with testing and the vendor's LoC.

(e) Section 3.9.3.1.5 states that the CP shall support the Calling Number Delivery feature for voice calls. Calling Number Delivery shall support the capabilities in the following subparagraphs. The SUT met the following requirements with testing.

1. Delivery of the calling party's number to the CP end user on incoming voice calls to that user from other CP end users, from UC network and DSN end users, and from PSTN end users.

2. Delivery of "Calling Number Private" indications to the CP end user on incoming voice calls to that user in which the calling party's identity is marked "Private.".

3. Delivery of "Calling Number Unavailable" indications to the CP end user on incoming voice calls to that user in which the calling party's identity is not available.

4. The CP shall determine the calling number provided to the called party based on the dialing plan used by the calling party:

a. If the incoming call is from another CP end user, then the calling number shall be delivered to the called party in a format that allows the called party to "call back" the calling party at a later time. A calling party address (such as a Calling Party Username) can be used instead of a calling party number in this case. The SUT met the following requirements with testing.

b. If the incoming call is from a UC network or DSN user, then the calling number shall be delivered to the called party in a 10-digit DSN number format. The SUT met the following requirements with testing.

c. If the incoming call is from a PSTN (commercial) user, then the calling number shall be delivered to the called party in a national or international calling number format. The SUT does not offer a direct PSTN interface.

5. Support the Calling Name Delivery feature for voice calls. Calling Number Delivery shall support the following capabilities:

a. Delivery of the calling party's name to the CP end user on incoming voice calls to that user from other CP users, from UC network and DSN end users, and from PSTN end users. The SUT does not offer a direct PSTN interface.

b. Delivery of "Calling Name Private" indications to the CP end user on incoming voice calls to that user in which the calling party's identity is marked "Private". The SUT met this requirement with testing.

c. Delivery of "Calling Name Unavailable" indications to the CP end user on incoming voice calls to that user in which the calling party's identity is not available. The SUT met this requirement with testing.

(2) Section 3.9.3.2 includes requirements for outgoing voice calls to DSN and commercial numbers (via CP MG or SBC).

(a) The CP shall support the establishment of point-to-point VoIP calls from CP end users to DSN numbers, and point-to-point VoIP calls from CP end users to commercial numbers. When a voice call's called address includes a DSN number from the DSN numbering plan, the CP shall determine whether the called DSN number is local to the CP or external to the CP. If the called DSN number is local to the CP, then the CP shall complete the voice call request to the destination end user on that CP. If the called DSN number is external to the CP, then the CP shall route the session request outside of the CP, using one of the following:

1. A DSN PRI on the CP MG (i.e., a PRI connected to a DSN EO). The SUT did not offer a CP MG.

2. An AS-SIP "trunk group" on the CP SBC (i.e., an AS-SIP "trunk group" that is linked with another UC network element such as an SC or an SC SBC). The SUT met this requirement.

(b) The CP shall support outgoing voice call requests from CP end users, containing called addresses that are DSN numbers from the DSN numbering plan and called addresses that are E.164 numbers from the E.164 numbering plan. When a voice call's called address includes an E.164 number from the E.164 numbering plan, the CP shall determine whether the called E.164 number is local to the CP or external to the CP. If the called E.164 number is local to the CP, then the CP shall complete the voice call request to the destination end user on that CP. If the called E.164 number is external to the CP, then the CP shall route the session request outside of the CP, using one of the following:

1. A PSTN PRI on the CP MG (that is, a PRI connected to a PSTN EO). For North American PRIs, the CP MG shall support both the Facility Associated Signaling (FAS) and Non-Facility Associated Signaling (NFAS) options. The SUT does not offer a CP MG.

2. An AS-SIP "trunk group" on the CP SBC (i.e., an AS-SIP "trunk group" that is linked with another UC network element such as an SC or an SC SBC). The SUT met this requirement with testing via the CP SBC.

(c) For outgoing voice calls, the CP MG shall support access to DSN EOs and PSTN EOs using the following types of ISDN PRIs: North American ISDN PRI or European (ETSI) ISDN PRI. The SUT does not offer a CP MG.

(d) For outgoing voice calls, the CP SBC shall support access to UC SCs and UC SC SBCs using AS-SIP trunk groups, per the SBC AS-SIP requirements in Section 2.17, SBC, and the AS-SIP 2013 document. The SUT met this requirement with testing and the vendor's LoC.

(3) Section 3.9.3.3 includes requirements for incoming voice calls from DSN and commercial numbers (via CP MG or SBC). The SUT met the following requirements for incoming voice calls via the SBC. The SUT does not offer a direct PSTN interface.

(a) The CP shall support the establishment of point-to-point VoIP calls to CP end users from DSN numbers, and of point-to-point VoIP calls to CP end users from COM numbers as shown in the subparagraphs below. The SUT does not offer a direct PSTN interface.

1. A DSN PRI on the CP MG (i.e., a PRI connected to a DSN EO). The SUT does not offer a CP MG interface.

2. An AS-SIP "trunk group" on the CP SBC (i.e., an AS-SIP "trunk group" that is linked with another UC network element such as an SC or an SC SBC). The SUT met this requirement with testing.

(b) The CP shall support incoming voice call requests to the CP end users, containing the following:

1. Called addresses that are DSN numbers from the DSN numbering plan. When a voice call's called address includes a DSN number from the DSN numbering plan, the CP shall determine whether the called DSN number is local to the CP or external to the CP. If the called DSN number is local to the CP, then the CP shall complete the voice call request to the destination end user on that CP. If the called DSN number is external to the CP, then the CP may route the session request back outside the CP, using one of the following: a DSN PRI on the CP MG or An AS-SIP "trunk group" on the CP SBC. The SUT met this requirement via the CP SBC. The SUT does not offer a CP MG interface.

2. Called addresses that are E.164 numbers from the E.164 numbering plan. When a voice call's called address includes an E.164 number from the E.164 numbering plan, the CP shall determine whether the called E.164 number is local to the CP or external to the CP. If the called E.164 number is local to the CP, then the CP shall complete the voice call request to the destination end user on that CP. If the called E.164 number is external to the CP, then the CP may route the session request back outside the CP, using one of the following: a PSTN PRI on the CP MG or an AS-SIP "trunk group" on the CP SBC. The SUT met this requirement with testing.

(c) For incoming voice calls, the CP MG shall support access from DSN EOs and PSTN EOs using North American ISDN PRI or European (ETSI) ISDN PRI. For North American PRIs, the CP MG shall support both the Facility Associated Signaling (FAS) and Non-Facility Associated Signaling (NFAS) options. The SUT does not offer a CP MG interface.

(d) For incoming voice calls, the CP SBC shall support access from UC SCs and UC SC SBCs using AS-SIP trunk groups, per the SBC AS-SIP requirements in Section 2.17, SBC, and the AS-SIP 2013 document. The SUT met this requirement with testing and the vendor's LoC.

(4) Section 3.9.3.4 includes requirements for video call features (call forwarding, call transfer, call hold, three-way calling, calling number delivery). UCR 2013, section 3.9.3.1, requirements are extended to video calls by replacing the term "voice call" with the term "video call" in each of these requirements. On video call requests to CP end users, the CP Client and the CP Server shall not allow the automatic enabling of the user's video camera when the video call request is negotiated or answered. The SUT met this requirement with testing.

(5) Section 3.9.3.5, states the CP shall support the establishment of point-to-point video over IP calls from CP end users to DSN numbers. The CP shall route calls to DSN numbers to an AS-SIP "trunk group" on the CP SBC. The CP can also route a call to a DSN number to another end user served by that CP, if that DSN number is associated with that other end user in the CP's internal routing tables. The CP shall support outgoing video call requests from CP end users containing called addresses that are DSN numbers from the DSN numbering plan. The SUT was not tested for inter-enclave video via the CP SBC and it is not covered under this certification.

(6) Section 3.9.3.6, states the CP shall support the establishment of point-to-point video over IP calls to CP end users from DSN numbers. The CP shall allow incoming video call requests to the CP end users containing called addresses that are DSN numbers from the DSN numbering plan. The SUT met this requirement with the testing. For incoming video calls, the CP SBC shall support access from UC SCs and UC SC SBCs using AS-SIP trunk groups, per the SBC AS-SIP requirements in Section 2.17, SBC, and the AS-SIP 2013 document. The SUT does not offer video via the CP SBC and it is not covered under this certification.

(7) Section 3.9.3.7, states the CP shall have a product availability state of 0.99999 (a non-availability state of no more than 5 minutes per year). The CP vendor shall provide an availability model for the product, showing all availability calculations and showing how the overall availability will be met. The product components shall have no single point of failure that could cause an outage of more than 96 VoIP and Video over IP subscribers. The SUT met this requirement with the vendor's LoC. The CP shall meet the following maximum downtime requirements:

(a) IP (10/100 Ethernet) network links (CP Server to CP MG connections, CP Server to CP SBC connections, and CP SBC connections to external SCs and SC SBCs): No more than 35 minutes of downtime per year. The SUT met this requirement with the vendor's LoC.

(b) IP End User connections (CP Client to CP Server connections): No more than 12 minutes of downtime per year. The SUT met this requirement with the vendor's LoC.

(8) Section 3.9.3.8, states the CP shall support Emergency Services Access services for CP end users. The CP shall allow the end user to dial an Emergency Services number as part a voice call request (e.g., 911 in the United States and Canada, and 112 in European countries), in order to place an emergency call and reach an ESB/PSAP.

(a) Once the emergency services call is answered at the ESB, the CP shall prevent the CP calling party from ending the call (i.e., a disconnect request from that caller shall be rejected). The CP shall allow the CP MG or the CP SBC to end the call in this case, provided that the CP MG or CP SBC receives a disconnect request from the destination PSAP indicating that the call can be disconnected. This supports the ESB/PSAP "Emergency Call Hold" feature described previously. The optional requirement was not tested.

(b) The CP shall provide Calling Party Number (CPN) information with the Emergency call request (911 or 112 call) to signal to the destination PSAP where the emergency call is being originated from. The CP shall include this CPN information in the ISDN PRI signaling when the call leaves the CP via the CP MG. The CP shall include this CPN information in the AS-SIP signaling when the call leaves the CP via the CP SBC. The SUT met this requirement with testing.

(c) The CP shall allow the CP System Administrator to associate a calling user with a calling physical location on the base, and a CPN value that points to that calling physical

location. The CP should use this configured CPN value to identify the calling location on outgoing Emergency call requests, through the CP MG and CP SBC. The SUT met this requirement with testing.

(d) The CP shall allow the CP end user to place a 911 Emergency Services call without having to dial a PSTN access code (e.g., 9+9) or a DSN access code (e.g., 9+4). The CP is not required to support a 911 Emergency Services call using the PSTN Access Code (e.g., by dialing 9+9+911) or a DSN Access Code (e.g., by dialing 9+4+911). The SUT met this requirement with testing. The SUT does not offer a direct PSTN interface.

(e) When the CP provides the Emergency Service feature using the 911 number, the feature's operation shall also be IAW Telcordia Technologies GR-529-CORE. The SUT met this requirement with testing.

(9) Basic Session Admission Control. Section 3.9.3.9 states the CP shall implement call counts and call thresholds for VoIP sessions, and call counts and call thresholds for video over IP sessions, in order to perform Session Admission Control (SAC). SAC refers to the CP's enforcement of voice and video call thresholds for the requirements in the subparagraphs below. The SUT does not fully support this optional requirement.

(a) Outgoing voice calls from CP end users to UC network and DSN end users, via the CP Server and the CP SBC.

(b) Incoming voice calls to CP end users from UC network and DSN end users, via the CP SBC and the CP Server.

(c) Outgoing video calls from CP end users to UC network end users, via the CP Server and the CP SBC.

(d) Incoming video calls to CP end users from UC network end users, via the CP SBC and the CP Server.

(e) Section 3.9.3.9 states the CP shall support configuration of total voice call thresholds and total video call thresholds. The CP shall also support configuration of outbound voice call thresholds, inbound voice call thresholds, outbound video call thresholds, and inbound video call thresholds in the subparagraphs below. The SUT does not support this optional requirement.

1. The CP shall apply SAC and enforce the configured voice and video call thresholds in the following cases:

2. Reject outbound voice call requests from the CP to the UC Network that would exceed the configured voice call threshold (or the configured outbound voice call threshold, when directionalization is supported).

3. Reject inbound voice call requests from the UC Network to the CP that would exceed the configured voice call threshold (or the configured inbound voice call threshold, when directionalization is supported).

4. Reject outbound video call requests from the CP to the UC Network that would exceed the configured video call threshold (or the configured outbound video call threshold, when directionalization is supported).

5. Reject inbound video call requests from the UC Network to the CP that would exceed the configured video call threshold (or the configured inbound video call threshold, when directionalization is supported).

6. If commercial SIP is used between the CP Server and the CP SBC, then the CP shall treat new SIP INVITE requests (outbound or inbound) as new CP call requests, for both voice and video calls. But the CP shall not treat SIP re-INVITE requests (outbound or inbound) as new CP call requests, for either voice or video calls, because the SIP re-INVITE requests are updates to previously accepted SIP INVITE requests.

c. IM/Chat/Presence Collaboration Tool Requirements.

(1) Section 3.9.4.1 intra-system capabilities between clients hosted off a single collaboration system requirements are provided in the following text:

(a) Section 3.9.4.1.1, states the CP shall use TLS to enable secure client-to-server connections between the host server and its clients. The SUT met this requirement with testing.

(b) Section 3.9.4.1.2, states the CP shall provide the ability for end users to subscribe to another user's presence (i.e., end user availability status) and to be notified when that state changes. Before the subscribing end user is permitted to see a contact's presence information, the contact must authorize the subscription. The CP shall support the ability for end users to cancel a subscription/unsubscribe to an end user's presence. The SUT met this requirement with testing.

(c) Section 3.9.4.1.3, states the CP shall enable end users to send presence information to the host server, and the host server shall in turn propagate that information to all the user's contacts who have an active subscription to that user's presence information. The CP shall permit end users to update their presence (i.e., Availability Status), and the host server shall in turn broadcast the updated presence information to all the user's contacts who have an active subscription to that user's presence information. With regard to the exchange of presence, the CP shall support the ability to block and unblock communications with selected users. The SUT met this requirement with testing.

(d) Section 3.9.4.1.4, states the CP shall store an end user's roster and shall permit end users to retrieve their roster upon login into the host server. The CP shall enable end users to add, modify, or delete items in their roster. For example, adding or deleting a group to a roster. The SUT met this requirement with testing.

(e) Section 3.9.4.1.5, states the CP shall enable a one-to-one chat (near real-time, text-based messaging) conversation between two parties. The CP shall communicate chat state notifications (i.e., the ability to communicate when a chat partner is actively engaged in composing/typing a message). With regard to one-to-one chat, the CP shall support the ability to block and unblock communications with selected end users. The SUT met this requirement with testing. Section 3.9.4.1.5, states the CP shall enable groups of end users to participate and maintain ongoing discussions within the context of a real-time, text-based conference. The CP shall permit end users to create a chat room (i.e., a virtual space for a real-time, text-based conference). The end user who creates the room is designated as the owner of the room with moderator privileges. The CP shall permit the owner/moderator to define a name for the room. The CP shall permit an end user to "enter" a room by becoming an "occupant within the room" with the privilege to participate in the ongoing discussions. The CP shall permit an end user to "exit" a room by ceasing to be an "occupant within the room." The CP shall permit the room owner/moderator to ban a user from a room or to remove a participant from a room. The CP shall permit an end user to create a members only room and to grant or revoke membership to other end users. The SUT met this requirement with testing.

(2) Section 3.9.4.2, states the optional requirements between clients hosted off different Collaboration Systems are provided in UCR 2013, Table 3.9-1. The SUT offers an XMPP Gateway; however, this was not tested and it is not covered under this certification.

d. Information Assurance (IA) Requirements. Security testing is accomplished by DISA-led Information Assurance test teams and the results published in a separate report, Reference (e). Additional security requirements specific to the SUT SBC and documented in the subparagraphs below were verified by the vendor's LoC with any exceptions noted.

(1) Section 4.2.3 provided the IA requirements for user roles. The SUT SBC supports real-time logging; however, it does not support real-time logging at the port level. DISA accepted the vendor's POAM and adjudicated this as minor.

(2) Section 4.2.4 provided the IA requirements for ancillary equipment.

(3) Section 4.2.5 provided the IA requirements for Voice and Video over IP (VVoiP) authentication.

(4) Section 4.2.6 provided the IA requirements for VVoIP authorization.

(5) Section 4.2.7 provided the IA requirements for Public Key Infrastructure (PKI). The SUT SBC is not capable of sending an alert when installed certificates corresponding to trust chains, OCSP responder certificates, or any other certificates installed on the device that cannot be renewed in an automated manner are nearing expiration. DISA accepted the vendor's POAM and adjudicated this as minor.

(6) Section 4.2.8 provided the IA requirements for integrity.

(7) Section 4.2.9 provided the IA requirements for confidentiality.

(8) Section 4.2.10 provided the IA requirements for non-repudiation.

e. Hardware/Software/Firmware Version Identification. Table 3-3 provides the SUT components' hardware, software, and firmware tested. The JITC tested the SUT in an operationally realistic environment to determine its interoperability capability with associated network devices and network traffic. Table 3-4 provides the hardware, software, and firmware of the components used in the test infrastructure.

7. TESTING LIMITATIONS. JITC test teams noted the following testing limitation including the impact they may have on interpretation of the results and conclusions. Any untested requirements are also included in the testing limitations. Although the SUT supports IPv6, it was not tested inter-enclave via the CP SBC because of test limitations within the network infrastructure. Therefore, inter-enclave IPv6 via the CP SBC is not covered under this certification, but intra-enclave use of IPv6 is authorized for use. The fielding of the SUT is limited to IPv4 across the DISN between the SUT CP Server and CP Clients. There is no impact because DoD is not fielding IPv6 across the DISN in the near future.

8. CONCLUSION(S). The SUT meets the critical interoperability requirements for a UC Collaboration Product in accordance with the UCR and is certified for joint use with other UC Products listed on the APL. The SUT meets the interoperability requirements for the interfaces listed in Table 3-1.

DATA TABLES

Table 3-1. Interface Status

Interface	Threshold CR/FR Requirements (See note 1.)	Status	Remarks
Network Management Interfaces			
IEEE 802.3i (10BaseT UTP) (C) (See note 2.)	1	Met	
IEEE 802.3u (100BaseT UTP) (C) (See note 2.)	1	Met	
IEEE 802.3ab (1000BaseT UTP) (C) (See note 2.)	1	Met	
UC Network Interfaces			
IEEE 802.3i (10BaseT UTP) (C) (See note 2.)	1, 2, 3, and 4	Partially Met	See note 3.
IEEE 802.3u (100BaseT UTP) (C) (See note 2.)	1, 2, 3, and 4	Partially Met	See note 3.
IEEE 802.3ab (1000BaseT UTP) (C) (See note 2.)	1, 2, 3, and 4	Partially Met	See note 3.
DISN Legacy Interfaces			
North American ISDN PRI (C)	1 and 2	Not Tested	
European ISDN (C)	1 and 2	Not Tested	
2-wire analog (C)	1 and 2	Not Tested	
Client Interfaces			
IEEE 802.3i (10BaseT UTP) (C) (See note 2.)	1, 2, 3, and 4	Partially Met	See note 3.
IEEE 802.3u (100BaseT UTP) (C) (See note 2.)	1, 2, 3, and 4	Partially Met	See note 3.

NOTES:

1. The SUT high-level CR and FR ID numbers depicted in the Threshold CRs/FRs column can be cross-referenced in Table 3. These high-level CR/FR requirements refer to a detailed list of requirements provided in Enclosure 3.
2. The SUT must provide a minimum of one of the listed interfaces.
3. The SUT partially meets the interoperability requirements related to SUT Information Assurance detailed in UCR 2013 section 4.2.3 and 4.2.7. The SUT SBC does not support real-time logging at the port level. The SUT SBC does not send an alert when installed certificates are nearing expiration. DISA accepted the vendor's POA&M and adjudicated these as minor.

LEGEND:

802.3i	10BaseT Mbps over twisted pair	DISN	Defense Information Systems Network
802.3u	Standard for 100 Mbps Ethernet	FR	Functional Requirement
802.3ab	1000BaseT Gbps Ethernet over twisted pair at 1 Gbps (125 Mbps)	Gbps	Gigabits per second
		IEEE	Institute of Electrical and Electronics Engineers
10BaseT	10 Mbps (Baseband Operation, Twisted Pair) Ethernet	ISDN	Integrated Services Digital Network
100BaseT	100 Mbps (Baseband Operation, Twisted Pair) Ethernet	POA&M	Plan of Actions and Milestones
		PRI	Primary Rate Interface
1000BaseT	1000 Mbps (Baseband Operation, Twisted Pair) Ethernet	R	Required
		SBC	Session Border Controller
C	Conditional	UC	Unified Capabilities
CR	Capability Requirement	UCR	Unified Capabilities Requirements
DISA	Defense Information Systems Agency	UTP	Unshielded Twisted Pair

Table 3-2. Capability and Functional Requirements and Status

CR/FR ID	Capability/Function	Applicability (See note 1.)	UCR Reference	Status
1	**Voice and Video Collaboration Tool Requirements**			
	Point-to-Point Voice Calls Between Collaboration Tool Clients	Required	3.9.2.1	Met
	Add Voice Call to Existing Collaboration Session	Required	3.9.2.2	Met
	Point-to-Point Video Calls Between Collaboration Tool Clients	Required	3.9.2.3	Met (See note 2.)
	Add Video Call to Existing Collaboration Session	Required	3.9.2.4	Met
	Proprietary Client <->Server Signaling and Client <->Client Media	Required	3.9.2.5	Met
	Local Directory Service for Collaboration Product Users	Required	3.9.2.6	Met
	IPv6 Support	Required	3.9.2.7	Met (See note 3.)
	QoS for Video over IP and VoIP Sessions	Required	3.9.2.8	Met
	Information Assurance	Required	3.9.2.9	See note 4.
	SNMPv3 Alarms for Remote Monitoring	Required	3.9.2.10	Met
2	**Optional Voice and Video Collaboration Tool Requirements**			
	Voice Call Features (Call Forwarding, Call Transfer, Call Hold, Three Way Calling, Calling Number Delivery)	Optional	3.9.3.1	Met
	Outgoing Voice Calls to DSN and COM Numbers (via CP MG or SBC)	Optional	3.9.3.2	
	Incoming Voice Calls from DSN and COM Numbers (via CP MG or SBC)	Optional	3.9.3.3	Met (See note 5.)
	Video Call Features (Call Forwarding, Call Transfer, Call Hold, Three-Way Calling, Calling Number Delivery)	Optional	3.9.3.4	Met
	Outgoing Video Calls to DSN Numbers (via SBC)	Optional	3.9.3.5	Not Tested
	Incoming Video Calls from DSN Numbers (via SBC)	Optional	3.9.3.6	Met
	High Availability (Five 9s) for Collaboration Tool Products	Optional	3.9.3.7	Met
	Emergency Service (911) for Voice Calls	Optional	3.9.3.8	Met
	Basic Session Admission Control	Optional	3.9.3.9	Not Met (See note 6.)
3	**IM/Chat/Presence Collaboration Product Requirements**			
	Intra-System	Conditionally Required	3.9.4.1	Met
	Inter-System	Conditionally Required	3.9.4.2	Not Tested
4	**IA Requirements**			
	User Roles	Conditionally Required	4.2.3	Partially Met (See note 7.)
	Ancillary Equipment	Conditionally Required	4.2.4	Met
	VVoIP Authentication	Conditionally Required	4.2.5	Met
	VVoIP Authorization	Conditionally Required	4.2.6	Met
	Public Key Infrastructure	Conditionally Required	4.2.7	Partially Met (See note 8.)
	Integrity	Conditionally Required	4.2.8	Met
	Confidentiality	Conditionally Required	4.2.9	Met
	Non-Repudiation	Conditionally Required	4.2.10	Met

Table 3-2. Capability and Functional Requirements and Status (continued)

NOTES:
1. The annotation of 'required' refers to a high-level requirement category. The applicability of each sub-requirement is provided in Enclosure 3. The system under test does not need to provide conditional requirements. However, if a capability is provided, it must function according to the specified requirements.
2. The SUT met this requirement with testing for intra-enclave point-to-point video over IP between the SUT CP clients.
3. The SUT met this requirement with testing and the vendor's LoC. However, due to limitations with IPv6 via the SUT SBC, the SUT is certified for IPv4 only via the SBC to the UC network.
4. Security is verified by the vendor's LoC and testing accomplished by DISA-led Information Assurance test teams and the results published in a separate report, Reference (e).
5. The SUT does not offer a direct PSTN interface.
6. The SUT does not fully support the optional Session Admission Control requirements.
7. The SUT SBC supports real-time logging; however, it does not get to the port level. DISA accepted the vendor's POA&M and adjudicated this as minor.
8. The SUT is not capable of sending an alert when installed certificates corresponding to trust chains, OCSP responder certificates, or any other certificates installed on the device that cannot be renewed in an automated manner are nearing expiration. DISA accepted the vendor's POA&M and adjudicated this as minor.

LEGEND:

COM	Commercial	MG	Media Gateway
CP	Collaboration Product	OCSP	Online Certificate Status Protocol
CR	Capability Requirement	PoA&M	Plan of Actions and Milestones
DISA	Defense Information Systems Agency	PSTN	Public Switched Telephone Network
DSN	Defense Switched Network	QoS	Quality of Service
FR	Functional Requirement	SBC	Session Border Controller
IA	Information Assurance	SNMPv3	Simple Network Management Protocol version 3
ID	Identification	SUT	System Under Test
IM	Instant Messaging	UC	Unified Capabilities
IP	Internet Protocol	UCR	Unified Capabilities Requirements
IPv4	Internet Protocol version 4	VoIP	Voice over IP
IPv6	Internet Protocol version 6	VVoIP	Voice and Video over IP
LoC	Letters of Compliance		

Table 3-3. SUT Hardware/Software/Firmware Version Identification

Component	Release	Sub-component	Function
Acme Packet Net-Net 4500 SD (See note 1.	S-CX6.3.0.MR-5 GA (Build 573)	ETC Card (See note 2.)	SBC
Lync 2013 Server	5.0.8308 64-bit	None	Microsoft Lync Server
Lync 2013 Client	15.0.4481.1000 MSO 64-bit	None	Microsoft Lync Client
Dell Latitude E6430	Windows 7 Enterprise SP1 64-bit	None	Workstation
Polycom CX 300	N/A		USB Phone (See note 3.)

NOTES:
1. The SUT was tested with the Acme Packet Net-Net 4500 SD. However, the 3820 utilizes the same software and similar hardware and JITC analysis determined it to be functionally identical for interoperability certification purposes and the 3820 is also covered under this certification for use with the SUT. In addition, the SUT is certified with any 4500 or 3820 with this release or later that is on the UC APL.
2. The SUT SBC was originally tested with the HIFN card installed; however, there were one-way audio anomalies. The SUT was retested with the ETC card installed in the SBC and the anomalies were no longer present. The SBC ETC card supports both single- and dual-side rekeying. The SUT SBC is not certified for use with the HIFN card installed.
3. JITC analysis determined the SUT is certified for use with any USB phones identified on the Microsoft website as Microsoft-certified with the Lync.

LEGEND:

APL	Approved Products List	SUT	System Under Test
ETC	Enhanced Traffic Controller	UC	Unified Capabilities
JITC	Joint Interoperability Test Command	USB	Universal Serial Bus
SBC	Session Border Controller		

Table 3-4. Test Infrastructure Hardware/Software/Firmware Version Identification

System Name	Software Release	Function
Required Ancillary Equipment		
Active Directory		
Public Key Infrastructure		
Test Network Components		
Avaya CS2100 with AS5300	CS2100 Release SE09.1/ AS5300 Release 2.0	MFSS
Avaya CS2100 with AS5300	CS2100 Release SE09.1/ AS5300 Release 3.0	MFSS
Avaya AS5300	Release 2.0	LSC
Avaya AS5300	Release 3.0	LSC
REDCOM High Density Exchange (HDX)	4.0AR3P9	LSC
Avaya	Communication Manager (CM) 6.0.1 (00.1.510.1 Service Pack [SP] 20554) with Security Service Pack 1 (SSP1)	LSC
Cisco Unified Communications Manager	8.0(2)	LSC
Cisco Unified Communications Manager	8.6.1	LSC
LEGEND: LSC Local Session Controller MFSS Multifunction Softswitch		

Table 3-5. UC Collaboration Tool Capability/Functional Requirements

CR/FR ID	Requirement	UCR Ref (UCR 2013)	LoC/ TP ID	CP R/O/C
1	**3.9.2 - Voice and Video Collaboration Tool Requirements**			
1-1	**3.9.2.1 - Point-to-Point Voice Calls Between Collaboration Tool Clients**			
1	The CP shall support the establishment of point-to-point Voice over IP (VoIP) calls between CP Clients that are served by the CP Server. The CP shall allow one CP Client to set up a point-to-point VoIP call with another CP Client. The CP shall allow the first CP Client to call the second CP Client by entering the second Client's phone number, by entering the second Client's username, or by looking up the second Client in a User Directory on the CP Server.	3.9.2.1 AUX-006330	T IO-3A IO-3B	CP (R)
1-2	**3.9.2.2 - Add Voice Call to Existing Collaboration Session**			
1	When two CP Clients have an existing Collaboration session established through the CP Server (e.g., a Presence/IM/Chat session, a whiteboard session, or a document sharing session), the CP shall allow either one of the CP Clients to add a VoIP call with the other CP Client to that existing session. The CP shall also allow either of the CP clients to later drop the VoIP call from that session, returning the session to its original type (e.g., Presence/IM/Chat, whiteboard, or document sharing).	3.9.2.2 AUX-006340	T IO-3C	CP (R)
1-3	**3.9.2.3 - Point-to-Point Video Calls Between Collaboration Tool Clients**			
1	The CP shall support the establishment of point-to-point Video over IP calls between CP Clients that are served by the CP Server. The CP shall allow one CP Client to set up a point-to-point Video over IP call with another CP Client. The CP shall allow the first CP Client to call the second CP Client by entering the second Client's phone number, entering the second Client's username, or looking up the second Client in the User Directory on the CP Server.	3.9.2.3 AUX-006350	T IO-6A IO-6B	CP (R)
1-4	**3.9.2.4 - Add Video Call to Existing Collaboration Session**			
1	When two CP Clients have an existing Collaboration Session established through the CP Server (e.g., a Presence/IM/Chat session, a whiteboard session, or a document sharing session), the CP shall allow either one of the CP Clients to add a Video over IP call with the other CP Client to that existing session. The CP shall also allow either of the CP clients to later drop the Video over IP call from that session, returning the session to its original type (e.g., Presence/IM/Chat, whiteboard, or document sharing).	3.9.2.4 AUX-006360	T IO-6C	CP (R)
1-5	**3.9.2.5 - Proprietary Client <->Server Signaling and Client <->Client Media**			
1	For VoIP sessions between CP Clients, the CP Client and the CP Server shall support the establishment and tear-down of the VoIP sessions, using signaling messages that are proprietary to the CP product.	3.9.2.5 AUX-006370	T IO-3	CP Client (R) CP Server (R)
2	For Video over IP sessions between CP Clients, the CP Client and the CP Server shall support the establishment and tear-down of Video over IP sessions, using signaling messages that are proprietary to the CP product	3.9.2.5 AUX-006380	T IO-4	CP Client (R) CP Server (R)
3	For Voice calls that traverse the CP MG, the CP Server and the CP MG shall support the establishment and tear-down of the VoIP sessions, using signaling messages that are proprietary to the CP product.	3.9.2.5 AUX-006390	T IO-5	CP Server (R) CP MG (R)
4	For Voice calls that traverse the CP SBC, the CP Server and the CP SBC shall support the establishment and tear-down of the VoIP sessions, using signaling messages that are proprietary to the CP product.	3.9.2.5 AUX-006400	T IO-5	CP Server (R) CP SBC (R)
5	For Video calls that traverse the CP SBC, the CP Server and the CP SBC shall support the establishment and tear-down of the Video over IP sessions, using signaling messages that are proprietary to the CP product. Support for AS-SIP signaling over TLS within the CP product (i.e., between one product component and another) is not required. Support for commercial SIP signaling over TLS within the CP product is allowed but is not required. Since different product vendors generally support different versions of commercial SIP signaling, commercial SIP signaling is treated as proprietary signaling here.	3.9.2.5 AUX-006410	T IO-8	CP Server (R) CP SBC (R)
6	For VoIP sessions between CP Clients, the Clients shall support the exchange of VoIP media packets, using media protocols that are proprietary to the CP product. Support of industry-standard media protocols is also allowed.	3.9.2.5 AUX-006420	T IO-3	CP Client (R)

Table 3-5. Collaboration Tool Capability/Functional Requirements (continued)

CR/FR ID	Requirement	UCR Ref (UCR 2013)	LoC/ TP ID	CP R/O/C
1-5	**3.9.2.5 - Proprietary Client <->Server Signaling and Client <->Client Media**			
7	For Video over IP sessions between CP Clients, the Clients shall support the exchange of Video over IP media packets, using media protocols that are proprietary to the CP product. Support of industry-standard media protocols is also allowed.	3.9.2.5 AUX-006430	T IO-4	CP Client (R)
8	For Voice calls that traverse the CP MG, the CP Client and the CP MG shall support the exchange of VoIP media packets, using media protocols that are proprietary to the CP product. Support of industry-standard media protocols is also allowed.	3.9.2.5 AUX-006440	T IO-5	CP Client (R) CP MG (R)
9	For Voice calls that traverse the CP SBC, the CP Client and the CP SBC shall support the exchange of Video over IP media packets, using media protocols that are proprietary to the CP product. Support of industry-standard media protocols is also allowed.	3.9.2.5 AUX-006450	T IO-5	CP Client (R) CP SBC (R)
10	For Video calls that traverse the CP SBC, the CP Client and the CP SBC shall support the exchange of Video over IP media packets, using media protocols that are proprietary to the CP product. Support of industry-standard media protocols is also allowed. Support for SRTP-based media within the CP product (i.e., between one product component and another) is allowed, but is not required. Examples of SRTP-based media are G.711 over SRTP and G.729 over SRTP for VoIP sessions, and H.263 over SRTP and H.264 over SRTP for Video sessions. The SRTP-based media within the CP product can be either industry-standard media (such as the aforementioned G.7XX and H.26X media), or non-standard media that is proprietary to the CP product.	3.9.2.5 AUX-006460	T IO-8	CP Client (R) CP SBC (R)
1-6	**3.9.2.6 - Local Directory Service for Collaboration Product Users**			
1	The CP product shall provide a Local Directory Service (LDS) for the CP users (the end users of the CP Clients and the CP Server). The LDS shall allow the CP users to look up information about each other based on the users' Name, Phone Number, and E-mail Address values.	3.9.2.6 AUX-006470	T IO-1	CP (R)
2	The CP LDS shall support the following functions: AUX-006480.a [Required: CP] The CP shall support a Directory Look-Up function that shall allow a user assigned to a CP to look up the telephone numbers of other users assigned to (i.e., served by) that CP. This function is referred to as "white pages" service, and it should not be confused with the CP routing tables, which are used for handling collaboration requests. AUX-006480.b [Required: CP] For security reasons, the Directory Look-Up function shall be available only from a user's CP Client and not from other user devices outside the CP product. AUX-006480.c [Required: CP] The CP shall allow the system administrator to update the directory database in response to client data changes (i.e., client adds, modifications, or removals). The CP shall update the white pages data automatically whenever the client information is updated.	3.9.2.6 AUX-006480	T IO-1 IO-12A	CP (R)
1-7	**3.9.2.7 - IPv6 Support**			
1	The CP Client shall meet all of the IPv6 protocol requirements for End Instrument (EI) products in Section 5, IPv6, including the requirements in Table 5.2-3, UC EIs. This includes EI Conditional Requirements, when the Condition specified for the EI also applies to the CP Client.	3.9.2.7 AUX-006490	L/T IO-3 IO-6	CP Client (R)
2	The CP Server shall meet all the IPv6 protocol requirements for Network Appliances and Simple Servers (NA/SS) products in Section 5, IPv6, including the requirements in Table 5.2-4, UC Network Appliances and Simple Servers (NA/SS). This includes NA/SS Conditional Requirements, when the Condition specified for the NA/SS also applies to the CP Server.	3.9.2.7 AUX-006500	L	CP Server (R)

Table 3-5. Collaboration Tool Capability/Functional Requirements (continued)

CR/FR ID	Requirement	UCR Ref (UCR 2013)	LoC/ TP ID	CP R/O/C
1-8	**3.9.2.8 - QoS for Video over IP and VoIP Sessions**			
1	The CP Client, CP Server, CP MG, and CP SBC shall provide Quality of Service (QoS) for VoIP sessions and Video over IP Sessions, through the setting of Differentiated Services Code Points (DSCPs) in VVoIP signaling streams and VVoIP media streams.	3.9.2.8 AUX-006510	T IO-2A	CP Client (R) CP Server (R) CP MG (R) CP SBC (R)
2	CP support for the VVoIP Signaling and Media DSCPs, specified in Section 6.3.2 and Table 6.3.2, Traffic Conditioning Specification, is optional but not required. Examples of VVoIP Signaling and Media DSCPs follow: • User Signaling DSCP 40 (Base 10). • Non-Assured Voice DSCP 46 (Base 10). • Broadcast Video DSCP 24 (Base 10). CP support for Table 6.3.2 DSCPs associated with Priority and Precedence is not required.	3.9.2.8 AUX-006520	T IO-2B	CP Client (O) CP Server (O) CP MG (O) CP SBC (O)
1-9	**3.9.2.9 - Information Assurance**			
1	The CP and its components shall meet the Information Assurance requirements of all applicable DISA STIGs. NOTE: The number of STIGs that would apply to a vendor's CP is dependent on the architecture of the CP System Under Test (SUT) that the vendor submits for certification.	3.9.2.9 AUX-006530	T (see IA TPs)	CP (R)
1-10	**3.9.2.10 - SNMP v3 Alarms for Remote Monitoring**			
1	The CP Server, CP MG, and CP SBC shall support generation and transmission of Simple Network Management Protocol (SNMP) version 3 (SNMPv3) alarms for remote monitoring.	3.9.2.10 AUX-006540	L/T IO-12B	CP Server (R) CP MG (R) CP SBC (R)
2	The CP Server, CP MG, and CP SBC shall generate alarm messages that are distinguishable from administrative log messages.	3.9.2.10 AUX-006550	T IO-12C	CP Server (R) CP MG (R) CP SBC (R)
3	The CP Server, CP MG, and CP SBC shall detect their own fault (alarm) conditions.	3.9.2.10 AUX-006560	T IO-12D	CP Server (R) CP MG (R) CP SBC (R)
4	The CP Server, CP MG, and CP SBC shall generate alarm notifications.	3.9.2.10 AUX-006570	T IO-12D	CP Server (R) CP MG (R) CP SBC (R)
5	The CP Server, CP MG, and CP SBC shall send the alarm messages in Near-Real Time (NRT). More than 99 percent of alarms shall be detected and reported in NRT. NRT is defined as event detection and alarm reporting within 5 seconds of the event, excluding transport time.	3.9.2.10 AUX-006580	T IO-12D	CP Server (R) CP MG (R) CP SBC (R)
6	The CP Server, CP MG, and CP SBC shall send the alarm messages in SNMPv3 format.	3.9.2.10 AUX-006590	L/T IO-12B	CP Server (R) CP MG (R) CP SBC (R)

Table 3-5. Collaboration Tool Capability/Functional Requirements (continued)

CR/FR ID	Requirement	UCR Ref (UCR 2013)	LoC/ TP ID	CP R/O/C
2	**3.9.3 - Optional Voice and Video Collaboration Tool Requirements**			
2-1	**3.9.3.1 - Voice Call Features (Call Forwarding, Call Transfer, Call Hold, Three Way Calling, Calling Number Delivery)**			
1	Reminder Ring for all call forwarding features, as specified in accordance with (IAW) Telcordia Technologies GR-217-CORE, GR-580-CORE, and GR-586-CORE, shall be supported.	3.9.3.1.1 AUX-006600	L/T IO-4	CP Client (O) CP Server (O) CP MG (O) CP SBC (O)
2	CFV shall be supported IAW Telcordia Technologies GR-580-CORE.	3.9.3.1.1.1 AUX-006610	L/T IO-4A	CP Client (O) CP Server (O) CP MG (O) CP SBC (O)
3	CFBL shall be supported IAW Telcordia Technologies GR-586-CORE.	3.9.3.1.1.2 AUX-006620	L/T IO-4B	CP Client (O) CP Server (O) CP MG (O) CP SBC (O)
4	CFDA shall be supported IAW Telcordia Technologies GR-586-CORE.	3.9.3.1.1.3 AUX-006630	L/T IO-4C	CP Client (O) CP Server (O) CP MG (O) CP SBC (O)
5	The CP product shall support two types of call transfers for voice calls: normal and explicit.	3.9.3.1.2 AUX-006640	T IO-4D	CP Client (O) CP Server (O) CP MG (O) CP SBC (O)
6	The CP product shall support the Call Hold feature for Voice calls. Call Hold shall support the following capabilities: • End user can place an active voice call on hold. • End user can retrieve a held voice call, making it an active voice call again. • End user can have multiple voice calls on hold at the same time. • Notifications from the CP product to the end user that their held call is still on hold. (e.g., when a user's active call ends and the user's held call is still on hold, the CP should notify the user that the held call is still established and is still on hold).	3.9.3.1.3 AUX-006650	T IO-4E	CP Client (O) CP Server (O) CP MG (O) CP SBC (O)
7	The CP product shall support the Three-Way Calling feature for Voice calls. Three-Way Calling shall support the following capabilities: • End user can place an active voice call on hold, launch an outgoing voice call, and merge the two voice calls together into a three-way call. • End user can place an active voice call on hold, answer an incoming voice call, and merge the two voice calls together into a three-way call. • Place a three-way call on hold and retrieve a three-way call from hold.	3.9.3.1.4 AUX-006660	T IO-4F	CP Client (O) CP Server (O) CP MG (O) CP SBC (O)
8	If the CP product uses SIP for voice call establishment, then the product shall support the Three-Way Calling feature consistent with the following sections of Request for Comment (RFC) 5359: • Section 2.10, Three-Way Conference – Third Party Is Added. • Section 2.11, Three-Way Conference – Third Party Joins.	3.9.3.1.4 AUX-006670	L/T IO-4G	CP Client (O) CP Server (O) CP MG (O) CP SBC (O)
9	The CP product shall support the Calling Number Delivery feature for Voice calls. Calling Number Delivery shall support the following capabilities: • Delivery of the calling party's number to the CP end user on incoming voice calls to that user from other CP end users, from UC network and DSN end users, and from PSTN end users. • Delivery of "Calling Number Private" indications to the CP end user on incoming voice calls to that user in which the calling party's identity is marked "Private." • Delivery of "Calling Number Unavailable" indications to the CP end user on incoming voice calls to that user in which the calling party's identity is not available.	3.9.3.1.5 AUX-006680	L/T IO-4H	CP Client (O) CP Server (O) CP MG (O) CP SBC (O)

Table 3-5. Collaboration Tool Capability/Functional Requirements (continued)

CR/FR ID	Requirement	UCR Ref (UCR 2013)	LoC/ TP ID	CP R/O/C
2-1	**3.9.3.1 - Voice Call Features (Call Forwarding, Call Transfer, Call Hold, Three Way Calling, Calling Number Delivery)**			
10	The CP product shall determine the calling number provided to the called party based on the dialing plan used by the calling party: • If the incoming call is from another CP end user, then the calling number shall be delivered to the called party in a format that allows the called party to "call back" the calling party at a later time. A calling party address (such as a Calling Party Username) can be used instead of a calling party number in this case. • If the incoming call is from a UC network or DSN user, then the calling number shall be delivered to the called party in a 10-digit DSN number format. • If the incoming call is from a PSTN (commercial) user, then the calling number shall be delivered to the called party in a national or international calling number format. Aside from the above requirements, the methods used to provide the Calling Number Delivery capabilities at the CP Client, CP Server, CP MG, and CP SBC, are up to the CP product vendor.	3.9.3.1.5 AUX-006690	T IO-4H	CP Client (O) CP Server (O) CP MG (O) CP SBC (O)
11	The CP product shall support the Calling Name Delivery feature for Voice calls. Calling Number Delivery shall support the following capabilities: • Delivery of the calling party's name to the CP end user on incoming voice calls to that user from other CP users, from UC network and DSN end users, and from PSTN end users. • Delivery of "Calling Name Private" indications to the CP end user on incoming voice calls to that user in which the calling party's identity is marked "Private." • Delivery of "Calling Name Unavailable" indications to the CP end user on incoming voice calls to that user in which the calling party's identity is not available.	3.9.3.1.5.1 AUX-006700	T IO-4H	CP Client (O) CP Server (O) CP MG (O) CP SBC (O)
2-2	**3.9.3.2 - Outgoing Voice Calls to DSN and COM Numbers (via CP MG or SBC)**			
1	The CP product shall support the establishment of point-to-point VoIP calls from CP end users to DSN numbers, and point-to-point VoIP calls from CP end users to Commercial (COM) numbers. • The CP shall route calls to DSN numbers to either a DSN PRI on the CP MG, or to an AS-SIP "trunk group" on the CP SBC, depending on the value of the called DSN number. • The CP can also route a call to a DSN number to another end user served by that CP, if that DSN number is associated with that other end user in the CP's internal routing tables. • The CP shall route calls to COM numbers to either a PSTN PRI on the CP MG, or to an AS-SIP "trunk group" on the CP SBC, depending on the value of the called COM number. • The CP can also route a call to a COM number to another end user served by that CP, if that COM number is associated with that other end user in the CP's internal routing tables.	3.9.3.2 AUX-006710	T IO-5A	CP Client (O) CP Server (O) CP MG (O) CP SBC (O)
2	The CP product shall support outgoing Voice call requests from CP end users, containing the following: • Called addresses that are DSN numbers from the DSN numbering plan. • Called addresses that are E.164 numbers from the E.164 numbering plan.	3.9.3.2 AUX-006720	L/T IO-5B	CP Client (O) CP Server (O) CP MG (O) CP SBC (O)
3	When a Voice call's called address includes a DSN number from the DSN numbering plan, the CP product shall determine whether the called DSN number is local to the CP or external to the CP. If the called DSN number is local to the CP, then the CP shall complete the Voice call request to the destination end user on that CP. If the called DSN number is external to the CP, then the CP shall route the session request outside of the CP, using one of the following: • A DSN PRI on the CP MG (i.e., a PRI connected to a DSN EO). • An AS-SIP "trunk group" on the CP SBC (i.e., an AS-SIP "trunk group" that is linked with another UC network element such as an SC or an SC SBC).	3.9.3.2 AUX-006730	L/T IO-5C	CP Client (O) CP Server (O) CP MG (O) CP SBC (O)

Table 3-5. Collaboration Tool Capability/Functional Requirements (continued)

CR/FR ID	Requirement	UCR Ref (UCR 2013)	LoC/ TP ID	CP R/O/C
2-2	**3.9.3.2 - Outgoing Voice Calls to DSN and COM Numbers (via CP MG or SBC)**			
4	When a Voice call's called address includes an E.164 number from the E.164 numbering plan, the CP product shall determine whether the called E.164 number is local to the CP or external to the CP. If the called E.164 number is local to the CP, then the CP shall complete the Voice call request to the destination end user on that CP. If the called E.164 number is external to the CP, then the CP shall route the session request outside of the CP, using one of the following: • A PSTN PRI on the CP MG (that is, a PRI connected to a PSTN EO). • An AS-SIP "trunk group" on the CP SBC (i.e., an AS-SIP "trunk group" that is linked with another UC network element such as an SC or an SC SBC).	3.9.3.2 AUX-006740	L/T IO-5D	CP Client (O) CP Server (O) CP MG (O) CP SBC (O)
5	For outgoing Voice calls, the CP MG shall support access to DSN EOs and PSTN EOs using the following types of ISDN PRIs: • North American ISDN PRI. • European (ETSI) ISDN PRI.	3.9.3.2 AUX-006750	L	CP MG (O)
6	For North American PRIs, the CP MG shall support both the Facility Associated Signaling (FAS) and Non-Facility Associated Signaling (NFAS) options.	3.9.3.2 AUX-006760	L	CP MG (O)
7	For outgoing Voice calls, the CP SBC shall support access to UC SCs and UC SC SBCs using AS-SIP trunk groups, per the SBC AS-SIP requirements in Section 2.17, SBC, and the AS-SIP 2013 document.	3.9.3.2 AUX-006770	L/T IO-5E	CP SBC (O)
2-3	**3.9.3.3 - Incoming Voice Calls from DSN and COM Numbers (via CP MG or SBC)**			
1	The CP product shall support the establishment of point-to-point VoIP calls to CP end users from DSN numbers, and of point-to-point VoIP calls to CP end users from COM numbers. • The CP shall accept calls to DSN numbers from a DSN PRI on the CP MG, and from an AS-SIP "trunk group" on the CP SBC. • The CP can also accept a call to a DSN number from another end user served by that CP, if that DSN number is associated with an end user in the CP's internal routing tables. • The CP shall accept calls to COM numbers from a PSTN PRI on the CP MG, and from an AS-SIP "trunk group" on the CP SBC. • The CP can also accept a call to a COM number to another end user served by that CP, if that COM number is associated with an end user in the CP's internal routing tables.	3.9.3.3 AUX-006780	L/T IO-5A	CP Client (O) CP Server (O) CP MG (O) CP SBC (O)
2	The CP product shall support incoming Voice call requests to the CP end users, containing the following: • Called addresses that are DSN numbers from the DSN numbering plan. • Called addresses that are E.164 numbers from the E.164 numbering plan.	3.9.3.3 AUX-006790	L/T IO-5B	CP Client (O) CP Server (O) CP MG (O) CP SBC (O)
3	When a Voice call's called address includes a DSN number from the DSN numbering plan, the CP product shall determine whether the called DSN number is local to the CP or external to the CP. If the called DSN number is local to the CP, then the CP shall complete the Voice call request to the destination end user on that CP. If the called DSN number is external to the CP, then the CP may route the session request back outside the CP, using one of the following: • A DSN PRI on the CP MG. • An AS-SIP "trunk group" on the CP SBC. In these cases, it is recommended that the route which the call leaves the CP on be different from the route which the call entered the CP on (e.g., if the call came in on a DSN PRI, then the call should go out on an AS-SIP trunk group).	3.9.3.3 AUX-006800	L/T IO-5C	CP Client (O) CP Server (O) CP MG (O) CP SBC (O)
4	When a Voice call's called address includes an E.164 number from the E.164 numbering plan, the CP product shall determine whether the called E.164 number is local to the CP or external to the CP. If the called E.164 number is local to the CP, then the CP shall complete the Voice call request to the destination end user on that CP. If the called E.164 number is external to the CP, then the CP may route the session request back outside the CP, using one of the following: • A PSTN PRI on the CP MG. • An AS-SIP "trunk group" on the CP SBC.	3.9.3.3 AUX-006810	L/T IO-5D	CP Client (O) CP Server (O) CP MG (O) CP SBC (O)

Table 3-5. Collaboration Tool Capability/Functional Requirements (continued)

CR/FR ID	Requirement	UCR Ref (UCR 2013)	LoC/ TP ID	CP R/O/C
2-3	**3.9.3.3 - Incoming Voice Calls from DSN and COM Numbers (via CP MG or SBC)**			
5	For incoming Voice calls, the CP MG shall support access from DSN EOs and PSTN EOs using the following types of ISDN PRIs: • North American ISDN PRI. • European (ETSI) ISDN PRI.	3.9.3.3 AUX-006820	L	CP MG (O)
6	For North American PRIs, the CP MG shall support both the Facility Associated Signaling (FAS) and Non-Facility Associated Signaling (NFAS) options.	3.9.3.3 AUX-006830	L	CP MG (O)
7	For incoming Voice calls, the CP SBC shall support access from UC SCs and UC SC SBCs using AS-SIP trunk groups, per the SBC AS-SIP requirements in Section 2.17, SBC, and the AS-SIP 2013 document.	3.9.3.3 AUX-006840	L/T IO-5E	CP SBC (O)
2-4	**3.9.3.4 - Video Call Features (Call Forwarding, Call Transfer, Call Hold, Three-Way Calling, Calling Number Delivery)**			
1	The CP product shall support the following features for video calls, as an extension of the requirements for these features for voice calls in Section 3.9.3.1, Voice Call Features: • Call Forwarding. • Call Transfer. • Call Hold. • Three-Way Calling. • Calling Number Delivery.	3.9.3.4 AUX-006850	L/T IO-7A IO-7B IO-7C IO-7D IO-7E IO-7F	CP (O)
2	On video call requests to CP end users, the CP Client and the CP Server shall not allow the automatic enabling of the user's video camera: • When the video call request is negotiated (i.e., when the video call type is negotiated or when the video codec is negotiated). • When the video call is accepted (i.e., when the video call is answered). After the video call request is negotiated and accepted, the CP Client and the CP Server shall allow the called user to enable his video camera, once the called user takes a positive action to enable that camera (i.e., the user selects an "Enable camera" option in his Client application).	3.9.3.4 AUX-006860	L/T IO-7G	CP Client (O) CP Server (O)
2-5	**3.9.3.5 - Outgoing Video Calls to DSN Numbers (via SBC)**			
1	The CP product shall support the establishment of point-to-point Video over IP calls from CP end users to DSN numbers. • The CP shall route calls to DSN numbers to an AS-SIP "trunk group" on the CP SBC. • The CP can also route a call to a DSN number to another end user served by that CP, if that DSN number is associated with that other end user in the CP's internal routing tables.	3.9.3.5 AUX-006870	T IO-8A	CP Client (O) CP Server (O) CP SBC (O)
2	The CP product shall support outgoing Video call requests from CP end users containing called addresses that are DSN numbers from the DSN numbering plan.	3.9.3.5 AUX-006880	T IO-8B	CP Client (O) CP Server (O) CP SBC (O)
3	When a Video call's called address includes a DSN number from the DSN numbering plan, the CP product shall determine whether the called DSN number is local to the CP or external to the CP. If the called DSN number is local to the CP, then the CP shall complete the Video call request to the destination end user on that CP. If the called DSN number is external to the CP, then the CP shall route the session request outside the CP, using an AS-SIP "trunk group" on the CP SBC (that is, an AS-SIP "trunk group" that is linked with another UC network element such as an SC or an SC SBC).	3.9.3.5 AUX-006890	T IO-8C	CP Client (O) CP Server (O) CP SBC (O)
4	For outgoing Video calls, the CP SBC shall support access to UC SCs and UC SC SBCs using AS-SIP trunk groups, per the SBC AS-SIP requirements in Section 2.17, SBC, and the AS-SIP 2013 document.	3.9.3.5 AUX-006900	T IO-8D	CP SBC (O)

Table 3-5. Collaboration Tool Capability/Functional Requirements (continued)

CR/FR ID	Requirement	UCR Ref (UCR 2013)	LoC/ TP ID	CP R/O/C
2-6	**3.9.3.6 - Incoming Video Calls from DSN Numbers (via SBC)**			
1	The CP product shall support the establishment of point-to-point Video over IP calls to CP end users from DSN numbers. • The CP shall accept calls to DSN numbers from an AS-SIP "trunk group" on the CP SBC. • The CP can also accept a call to a DSN number from another end user served by that CP, if that DSN number is associated with an end user in the CP's internal routing tables.	3.9.3.6 AUX-006910	T IO-8A	CP Client (O) CP Server (O) CP SBC (O)
2	The CP product shall allow incoming Video call requests to the CP end users containing called addresses that are DSN numbers from the DSN numbering plan.	3.9.3.6 AUX-006920	T IO-8B	CP Client (O) CP Server (O) CP SBC (O)
3	When a Video call's called address includes a DSN number from the DSN numbering plan, the CP product shall determine whether the called DSN number is local to the CP or external to the CP. If the called DSN number is local to the CP, then the CP shall complete the Video call request to the destination end user on that CP. If the called DSN number is external to the CP, then the CP may route the session request back outside the CP using the AS-SIP "trunk group" on the CP SBC.	3.9.3.6 AUX-006930	T IO-8C	CP Client (O) CP Server (O) CP MG (O) CP SBC (O)
4	For incoming Video calls, the CP SBC shall support access from UC SCs and UC SC SBCs using AS-SIP trunk groups, per the SBC AS-SIP requirements in Section 2.17, SBC, and the AS-SIP 2013 document.	3.9.3.6 AUX-006940	T IO-8D	CP SBC (O)
2-7	**3.9.3.7 - High Availability (Five 9s) for Collaboration Tool Products**			
1	The CP product shall have a product availability state of 0.99999 (a non-availability state of no more than 5 minutes per year). The CP vendor shall provide an availability model for the product, showing all availability calculations and showing how the overall availability will be met. The product components shall have no single point of failure that could cause an outage of more than 96 VoIP and Video over IP clients.	3.9.3.7 AUX-006950	L/T IO-9	CP (O)
2	The CP product shall meet the following maximum downtime requirements: 1. IP (10/100 Ethernet) network links (CP Server to CP MG connections, CP Server to CP SBC connections, and CP SBC connections to external SCs and SC SBCs): No more than 35 minutes of downtime per year. 2. IP End User connections (CP Client to CP Server connections): No more than 12 minutes of downtime per year.	3.9.3.7 AUX-006960	L	CP (O)
2-8	**3.9.3.8 - Emergency Service (911) for Voice Calls**			
1	The CP product shall support Emergency Services Access services for CP end users. The CP product shall allow the end user to dial an Emergency Services number as part a Voice call request (e.g., 911 in the United States and Canada, and 112 in European countries), in order to place an emergency call and reach an ESB/PSAP.	3.9.3.8 AUX-006970	L/T IO-4I	CP (O)
2	Once the Emergency Services number is dialed, the CP product shall route the call to a specified route for outgoing Emergency calls. The CP product shall support the following Emergency call routes: • CP Client => CP Server => CP MG => PSTN PRI => PSTN EO (which would typically route the call to a PSTN PSAP). • CP Client => CP Server => CP SBC => AS-SIP Interface => UC Session Controller (which could route the call to either a PSTN PSAP or a Military PSAP, depending on the SC's configuration). • CP Client => CP Server => CP MG => DSN PRI => DSN EO => (which could route the call to either a PSTN PSAP or a Military PSAP, depending on the EO's configuration).	3.9.3.8 AUX-006980	T IO-4J	CP (O)
3	Once the Emergency Services call is answered at the ESB, the CP product shall prevent the CP calling party from ending the call (i.e., a disconnect request from that caller shall be rejected). The CP product shall allow the CP MG or the CP SBC to end the call in this case, provided that the CP MG or CP SBC receives a disconnect request from the destination PSAP indicating that the call can be disconnected. This supports the ESB/PSAP "Emergency Call Hold" feature described previously.	3.9.3.8 AUX-006990	T IO-4J	CP (O)

Table 3-5. Collaboration Tool Capability/Functional Requirements (continued)

CR/FR ID	Requirement	UCR Ref (UCR 2013)	LoC/ TP ID	CP R/O/C
2-8	**3.9.3.8 - Emergency Service (911) for Voice Calls**			
4	The CP product shall provide Calling Party Number (CPN) information with the Emergency call request (911 or 112 call) to signal to the destination PSAP where the emergency call is being originated from. The CP product shall include this CPN information in the ISDN PRI signaling when the call leaves the CP product via the CP MG. The CP product shall include this CPN information in the AS-SIP signaling when the call leaves the CP product via the CP SBC.	3.9.3.8 AUX-007000	T IO-4K	CP (O)
5	The CP product shall allow the CP System Administrator to associate a calling user with a calling physical location on the base, and a CPN value that points to that calling physical location. The CP product should use this configured CPN value to identify the calling location on outgoing Emergency call requests, through the CP MG and CP SBC.	3.9.3.8 AUX-007010	T IO-4L	CP (O)
6	The CP product shall allow the CP end user to place a 911 Emergency Services call without having to dial a PSTN access code (e.g., 9+9) or a DSN access code (e.g., 9+4). The CP product is not required to support a 911 Emergency Services call using the PSTN Access Code (e.g., by dialing 9+9+911) or a DSN Access Code (e.g., by dialing 9+4+911).	3.9.3.8 AUX-007020	T IO-4I	CP (O)
7	When the CP product provides the Emergency Service feature using the 911 number, the feature's operation shall also be IAW Telcordia Technologies GR-529-CORE (Functional Specifications Document [FSDs] 15 01-0000, 15-03-0000, and 15-07-0000). Since GR-529-CORE was written for legacy voice systems, the CP product vendor may interpret how to apply the GR's 911 requirements to 911 Voice calls from CP end users. If the vendor's interpretation of GR-529-CORE conflicts with the previous requirements in this section for 911 calls, then those previous requirements should take precedence.	3.9.3.8 AUX-007030	L	CP (O)
2-9	**3.9.3.9 - Basic Session Admission Control**			
1	The CP product shall implement call counts and call thresholds for VoIP sessions, and call counts and call thresholds for Video over IP sessions, in order to perform Session Admission Control (SAC). SAC refers to the CP product's enforcement of voice and video call thresholds for the following: • Outgoing Voice calls from CP end users to UC network and DSN end users, via the CP Server and the CP SBC. • Incoming Voice calls to CP end users from UC network and DSN end users, via the CP SBC and the CP Server. • Outgoing Video calls from CP end users to UC network end users, via the CP Server and the CP SBC. • Incoming Video calls to CP end users from UC network end users, via the CP SBC and the CP Server. The voice and video call thresholds for SAC do not apply to the following types of calls: • Outgoing Voice calls from CP end users to DSN and PSTN end users, via the CP Server and the CP MG. • Incoming Voice calls to CP end users from DSN and PSTN end users, via the CP MG and the CP Server. • Voice calls between CP end users served by the same CP Server. • Video calls between CP end users served by the same CP Server.	3.9.3.9 AUX-007040	T IO-10A	CP (O)
2	The CP product shall support configuration of total voice call thresholds and total video call thresholds.	3.9.3.9 AUX-007050	T IO-10A	CP (O)
3	The CP product shall also support configuration of outbound voice call thresholds, inbound voice call thresholds, outbound video call thresholds, and inbound video call thresholds. This support of different call thresholds for outbound calls (CP Server => CP SBC => UC Network) and inbound calls (UC Network => CP SBC => CP Server) is called directionalization.	3.9.3.9 AUX-007060	T IO-10B	CP (O)

Table 3-5. Collaboration Tool Capability/Functional Requirements (continued)

CR/FR ID	Requirement	UCR Ref (UCR 2013)	LoC/ TP ID	CP R/O/C
2-9	**3.9.3.9 - Basic Session Admission Control**			
4	The CP product shall apply SAC and enforce the configured voice and video call thresholds in the following cases: • Reject outbound voice call requests from the CP product to the UC Network that would exceed the configured voice call threshold (or the configured outbound voice call threshold, when directionalization is supported). • Reject inbound voice call requests from the UC Network to the CP product that would exceed the configured voice call threshold (or the configured inbound voice call threshold, when directionalization is supported). • Reject outbound video call requests from the CP product to the UC Network that would exceed the configured video call threshold (or the configured outbound video call threshold, when directionalization is supported). • Reject inbound video call requests from the UC Network to the CP product that would exceed the configured video call threshold (or the configured inbound video call threshold, when directionalization is supported).	3.9.3.9 AUX-007070	T IO-10B	CP (O)
5	If commercial SIP is used between the CP Server and the CP SBC, then the CP product shall treat new SIP INVITE requests (outbound or inbound) as new CP call requests, for both Voice and Video calls. But the CP product shall not treat SIP re-INVITE requests (outbound or inbound) as new CP call requests, for either Voice or Video calls, because the SIP re-INVITE requests are updates to previously accepted SIP INVITE requests.	3.9.3.9 AUX-007080	L	CP (O)
3	**3.9.4 - IM/Chat/Presence Collaboration Product Requirements (Conditionally required based on support for IM/Chat/Presence)**			
3-1	**3.9.4.1 – Intra-System Capabilities**			
1	The CP shall use TLS to enable secure client-to-server connections between the host server and its clients.	3.9.4.1.1 AUX-007090	L/T IO-11A	CP (R)
2	The CP shall provide the ability for end users to subscribe to another user's presence (i.e., end user availability status) and to be notified when that state changes.	3.9.4.1.2 AUX-007100	T IO-11B	CP (R)
3	Before the subscribing end user is permitted to see a contact's presence information, the contact must authorize the subscription.	3.9.4.1.2 AUX-007110	T IO-11B	CP (R)
4	The CP shall support the ability for end users to cancel a subscription/unsubscribe to an end user's presence	3.9.4.1.2 AUX-007120	T IO-11B	CP (R)
5	The CP shall enable end users to send presence information to the host server, and the host server shall in turn propagate that information to all the user's contacts who have an active subscription to that user's presence information.	3.9.4.1.3 AUX-007130	T IO-11B	CP (R)
6	The CP shall permit end users to update their presence (i.e., Availability Status), and the host server shall in turn broadcast the updated presence information to all the user's contacts who have an active subscription to that user's presence information.	3.9.4.1.3 AUX-007140	T IO-11B	CP (R)
7	With regard to the exchange of presence, the CP shall support the ability to block and unblock communications with selected users.	3.9.4.1.3 AUX-007150	T IO-11C	CP (R)
8	The CP shall store an end user's roster and shall permit end users to retrieve their roster upon login into the host server.	3.9.4.1.4 AUX-007160	T IO-11D	CP (R)
9	The CP shall enable end users to add, modify, or delete items in their roster. For example, adding or deleting a group to a roster.	3.9.4.1.4 AUX-007170	T IO-11D	RP (R)
10	The CP shall enable a one-to-one chat (near real-time, text-based messaging) conversation between two parties.	3.9.4.1.5 AUX-007180	T IO-11E	CP (R)
11	The CP shall communicate chat state notifications (i.e., the ability to communicate when a chat partner is actively engaged in composing/typing a message).	3.9.4.1.5 AUX-007190	T IO-11E	CP (R)
12	With regard to one-to-one chat, the CP shall support the ability to block and unblock communications with selected end users.	3.9.4.1.5 AUX-007200	T IO-11E	CP (R)
13	The CP shall enable groups of end users to participate and maintain ongoing discussions within the context of a real-time, text-based conference.	3.9.4.1.6 AUX-007210	T IO-11E	CP (R)
14	The CP shall permit end users to create a chat room (i.e., a virtual space for a real-time, text-based conference). The end user who creates the room is designated as the owner of the room with moderator privileges.	3.9.4.1.6 AUX-007220	T IO-11F	CP (R)
15	The CP shall permit the owner/moderator to define a name for the room.	3.9.4.1.6 AUX-007230	T IO-11F	CP (R)
16	The CP shall permit an end user to "enter" a room by becoming an "occupant within the room" with the privilege to participate in the ongoing discussions	3.9.4.1.6 AUX-007240	T IO-11F	CP (R)

Table 3-5. Collaboration Tool Capability/Functional Requirements (continued)

CR/FR ID	Requirement	UCR Ref (UCR 2013)	LoC/ TP ID	CP R/O/C
3	**3.9.4 - IM/Chat/Presence Collaboration Tool Requirements**			
3-1	**3.9.4.1 – Intra-System Capabilities**			
17	The CP shall permit an end user to "exit" a room by ceasing to be an "occupant within the room."	3.9.4.1.6 AUX-007250	T IO-11F	CP (R)
18	The CP shall permit the room owner/moderator to ban a user from a room or to remove a participant from a room.	3.9.4.1.6 AUX-007260	T IO-11F	CP (R)
19	The CP shall permit an end user to create a members only room and to grant or revoke membership to other end users.	3.9.4.1.6 AUX-007270	T IO-11F	CP (R)
3-2	**3.9.4.2 – Inter-System Capabilities**			
1	Secure Server-to-Server over TLS [as defined in UC XMPP 2013 Specification] UC XMPP 2.5 XMPP Addressing UC XMPP 2.6.1.1 Hostname Resolution UC XMPP 2.6.2 Stream Negotiation UC XMPP 2.6.3 Stream Features UC XMPP 2.6.4 Stream Restarts UC XMPP 2.6.5 Continuation and Completion of Stream Negotiation UC XMPP 2.6.6 Directionality UC XMPP 2.6.7 Closing a Stream UC XMPP 2.6.8 Stream Attributes UC XMPP 2.6.9 Namespaces UC XMPP 2.7 STARTTLS Negotiation UC XMPP 2.8 Authentication and SASL Negotiation	3.9.4.2 Table 3.9-1	L	CP (O)
2	IM/Presence [as defined in UC XMPP 2013 Specification] UC XMPP 2.12.1 Subscription Requests and Approvals UC XMPP 2.12.2 Cancelling a Subscription UC XMPP 2.12.3 Unsubscribing UC XMPP 2.13 Exchanging Presence Information UC XMPP 2.13.1 Initial Presence UC XMPP 2.13.3 Subsequent Presence Broadcasts UC XMPP 2.13.4 Unavailable Presence UC XMPP 2.13.5 Presence Syntax UC XMPP 2.14.1 One-to-One Chat Sessions UC XMPP 2.14.2 Message Stanza Syntax	3.9.4.2 Table 3.9-1	L	CP (O)
3	Persistent Group Chat [as defined in XEP-0045, Multi-User Chat and UC XMPP 2013 Specification] XEP-0045 3 Requirements XEP-0045 5 Roles, Affiliations, and Privileges (Capabilities which are defined as "Required" in XEP 0045) XEP-0045 6 Entity Use Cases (Capabilities which are defined as "Required" in XEP 0045) XEP-0045 7 Occupant Use Cases (Capabilities which are defined as "Required" in XEP 0045) XEP-0045 8 Moderator Use Cases (Capabilities which are defined as "Required" in XEP 0045) XEP-0045 9 Admin Use Cases (Capabilities which are defined as "Required" in XEP 0045) XEP-0045 10 Owner Use Cases (Capabilities which are defined as "Required" in XEP 0045) UC XMPP, Table 2.16-2 Elevated/Clarified Requirements UC XMPP, 18 DiffServ Code Point (DSCP) Requirements	3.9.4.2 Table 3.9-1	L	CP (O)

Table 3-5. Collaboration Tool Capability/Functional Requirements (continued)

CR/FR ID	Requirement	UCR Ref (UCR 2013)	LoC/ TP ID	CP R/O/C
4	**4 – Information Assurance**			
4-1	**4.2.3 – User Roles**			
1	The product shall be capable of having at least three types of user roles: a system security administrator (e.g., auditor), a system administrator, and an application administrator.	4.2.3 IA-001000	L	CP MG (R) CP SBC (R)
2	The product shall be capable of supporting at least three types of user roles: a system administrator, a privileged application user, and an application user.	4.2.3 IA-002000	L	EI (R)
3	The product shall be capable of setting the default user precedence VVoIP session origination capability as ROUTINE.	4.2.3 IA-003000	L	EI (R)
	The product shall be capable of providing a mechanism for the appropriate administrator (not a user in the User role) to perform the following functions: IA-004010 Monitor the activities of a specific terminal, port, or network address of the system in real time. IA-004020 Define the events that may trigger an alarm, the levels of alarms, the type of notification, and the routing of the alarm. IA-004030 Provide a capability to monitor the system resources and their availabilities	4.2.3 IA-004000	L	CP MG (R) CP SBC (R)
4-2	**4.2.4 – Ancillary Equipment**			
1	Products that use external Authentication, Authorization, and Accounting (AAA) services provided by the Diameter Base Protocol shall do so in accordance with (IAW) Request for Comment (RFC) 3588. IA-009010 Systems that act as Diameter agents shall be capable of being configured as proxy agents. IA-009020 Systems that act as proxy agents shall maintain session state. IA-009030 All Diameter implementations shall ignore answers received that do not match a known Hop-by-Hop Identifier field. IA-009040 All Diameter implementations shall provide transport of its messages IAW the transport profile described in RFC 3539. IA-009050 Products that use the Extensible Authentication Protocol (EAP) within Diameter shall do so IAW RFC 4072**.**	4.2.4 IA-009000	L	CP MG (C) CP SBC (C) EI (C)
2	Products shall support the capability to use the Remote Authentication Dial In User Service (RADIUS) IAW RFC 2865 to provide AAA services. NOTE: For products to which the Conditional statement applies, the condition is implementation of RADIUS. IA-010010 Products that use the EAP within RADIUS shall do so IAW RFC 3579. IA-010020 If the products support RADIUS based accounting, then the system shall do so IAW RFC 2866.	4.2.4 IA-010000	L	CP MG (C) CP SBC (C) EI (C)
3	Products that use external AAA services provided by the Terminal Access Controller Access Control System (TACACS+) shall do so IAW the TACACS+ Protocol Specification 1.78 (or later). NOTE: The intent is to use the most current TACACS+ specification.	4.2.4 IA-011000	L	CP MG (C) CP SBC (C) EI (C)
4	EIs that use external address assignment services provided by the Dynamic Host Configuration Protocol (DHCP) shall do so IAW RFC 2131. NOTE: An external address assignment service is a service that extends beyond the boundary of the system. IA-012010 Products that act as DHCP clients upon receipt of a new IP address shall probe [e.g., with Address Resolution Protocol (ARP)] the network with the newly received address to ensure the address is not already in use. IA-012020 Products that act as DHCP clients upon receipt of a new IP address shall broadcast an ARP reply to announce the client's new IP address and clear outdated ARP cache entries in hosts on the client's subnet.	4.2.4 IA-012000	L	EI (C)
5	Products that use external AAA services provided by port based network access control mechanisms shall do so IAW Institute of Electrical and Electronics Engineers (IEEE) 802.1X-2010 in combination with Protected Extensible Authentication Protocol (PEAP) and Extensible Authentication Protocol (EAP)- Transport Layer Security (TLS) support, at a minimum, plus any other desired secure EAP types [e.g., EAP-Tunneled TLS (TTLS)]. IA-013010 Products that use external EAP services provided by EAP shall do so IAW RFC 3748 and its RFC extensions.	4.2.4 IA-013000	L	EI (C)

Table 3-5. Collaboration Tool Capability/Functional Requirements (continued)

CR/FR ID	Requirement	UCR Ref (UCR 2013)	LoC/ TP ID	CP R/O/C
4-2	**4.2.4 – Ancillary Equipment**			
6	Products that use external syslog services shall support the capability to do so IAW RFC 3164. IA-014010 Products that support syslog over User Datagram Protocol (UDP) IAW RFC 3164 shall use UDP port 514 for the source port of the sender when using UDP for transport. IA-014020 If the product supports syslog, then the product shall support the capability to generate syslog messages that have all the parts of the syslog packet as described in Section 4.1 of RFC 3164. IA-014030 If the originally formed message has a TIMESTAMP in the HEADER part, then it shall support the capability to specify this field's value in the local time of the device within its time zone and support the ability to specify this field's value in Greenwich Mean Time (GMT). IA-014040 If the originally formed message has a HOSTNAME field, then it shall contain the hostname as it knows itself. If it does not have a hostname, then it shall contain its own IP address. IA-014050 If the originally formed message has a TAG value, then it shall be the name of the program or process that generated the message. IA-014060 If products use Transmission Control Protocol (TCP) for the delivery of syslog events, then the system shall support the capability to do so IAW the Read and Write (RAW) profile defined in RFC 3195.	4.2.4 IA-014000	L	CP MG (C) CP SBC (C)
7	The product shall either support an onboard VVoIP Intrusion Detection System (IDS)/IPS capability that can monitor all VVoIP signaling and media traffic in decrypted form, or support the capability to present all signaling and bearer traffic to an external VVoIP IDS/IPS in a secure manner. IA-015010 The VVoIP IDS/IPS threat detection capabilities shall be IAW the VVoIP IDS/IPS functional requirements specified in Section 13, Security Devices. The product shall support the capability to generate and transmit an alarm to the NMS when these threats are identified. IA-015020 [Conditional: SBC] If the product provides the capability to transmit decrypted VVoIP media and signaling to an external IDS/IPS platform, then this interface shall use publicly accessible specifications and standards. NOTE: The intent of this requirement is to ensure that third party IDS/IPS vendors have the information necessary to create an interface that can accept and process the received VVoIP information.	4.2.4 IA-015000	L	CP SBC (R)
	If the product implements NTP, then the default version shall be Network Time Protocol (NTP) version 3 (NTPv3).	4.2.4 IA-016000	L	CP MG (O) CP SBC (O)
4-3	**4.2.5 –VVoIP Authentication**			
1	The product shall be capable of authenticating the SC using TLS (or its equivalent) (Threshold) with PKI certificates issued from a DoD-approved PKI.	4.2.5 IA-019000	L	EI (R)
2	The product shall be capable of allowing users to place ROUTINE precedence calls without authenticating.	4.2.5 IA-021000	L	EI (R)
3	The product shall be capable of allowing users to place emergency calls without authenticating.	4.2.5 IA-022000	L	EI (R)

Table 3-5. Collaboration Tool Capability/Functional Requirements (continued)

CR/FR ID	Requirement	UCR Ref (UCR 2013)	LoC/ TP ID	CP R/O/C
4-3	**4.2.5 –VVoIP Authentication**			
4	If the product supports authentication for precedence calls, then the product shall support a configuration setting which allows only authenticated users to access the product for services above the ROUTINE precedence level. IA-023010 [conditional] If the product uses SIP or AS-SIP, then the system shall, at a minimum, support the use of SIP digest authentication as specified in RFC 3261 when authenticating users. The product may support the ability to authenticate users via PKI certificates when authenticating user credentials to the SC via the EI using proprietary mechanisms. NOTE: The SC is responsible for the authentication decisions. The method for authenticating a user with their PKI certificate is a vendor decision due to the immaturity of the current standards. Vendors may choose to implement user authentication using PKI certificates as described in RFC 3261 or as described in RFC 3893. IA-023020 [Conditional] If the product implements AS-SIP and supports authentication for precedence calls, then the product shall use the procedures and algorithms specified in RFC 3261, Section 22.4, to execute SIP digest authentication for user authentication with a Personal Identification Number (PIN). The User-ID entered by the user shall be used for the value of the "username" field, and the PIN entered by the user shall be used as the value for "secret" in the digest calculation. IA-023030 [Conditional] If the product supports authentication for precedence calls via a PIN, then the device shall support the capability to provide audible and/or visible notification to the user, which, in a human understandable manner, prompts the user to enter his or her assigned User-ID and PIN when a precedence level above ROUTINE is requested. IA-023040 [Required] The user authentication mechanism shall be software enabled or disabled. NOTE: In certain deployments, the user does not have the time to input authentication credentials and the EI or AEI is located in a secure environment where credentials are not necessary due to the mission. By default this capability will be disabled to allow users to place calls without authenticating. IA-023050 [Conditional] If the product is a softphone, then the product shall support the capability to provide user authentication by presenting the user credentials extracted from the Common Access Card (CAC) or other DoD PKI Project Management Office (PMO)-approved PKI token to the SC. NOTE: The mechanism for AEIs and EIs to authenticate the User CAC or approved token credentials is permitted to occur via proprietary means. However, authentication of users via User ID and PIN authentication has been standardized for AEIs in this UCR.	4.2.5 IA-023000	L	EI (R)
5	The product shall adhere to the requirements in RFC 5922, Section 7.2, "Comparing SIP Identities," when comparing the domains extracted from X.509v3 certificates with AS-SIP identities contained in signaling messages.	4.2.5 IA-024000	L	CP MG (R) CP SBC (R)
4-4	**4.2.6 – VVoIP Authorization**			
1	The product shall have the capability of controlling the flow of traffic across an interface to the network based on the source/destination IP address, source/destination port number, Differentiated Services Code Point (DSCP), and protocol identifier ("6 tuple").	4.2.6 IA-026000	L	CP SBC (R)
2	The product shall have the capability of opening and closing "gates/pinholes" (i.e., packet filtering based on the "6 tuple") based on the information contained within the Session Description Protocol (SDP) body of the AS-SIP messages.	4.2.6 IA-027000	L	CP SBC (R)
3	The product shall have the capability to close a "gate/pinhole" based on a configurable media inactivity timer and issue a BYE message to upstream and downstream AS-SIP signaling appliances (lost BYE scenario). NOTE: The inactivity timer is based on the inactivity of the media stream.	4.2.6 IA-028000	L	CP SBC (R)
4	The default media inactivity value for closing a session and issuing BYE messages shall be 15 minutes.	4.2.6 IA-029000	L	CP SBC (R)

Table 3-5. Collaboration Tool Capability/Functional Requirements (continued)

CR/FR ID	Requirement	UCR Ref (UCR 2013)	LoC/ TP ID	CP R/O/C
4-4	**4.2.6 – VVoIP Authorization**			
5	The product shall have the capability of permitting the configuration of filters that will permit or deny IP packets on the basis of the values of the packet's source address, destination address, protocol, source port, and destination port in the packets header. These filters shall have the capability of using any one value, all values, or any combination of values. Filters using source ports and destination ports shall have the capability to be configured to use ranges of values defined by the operators (1) equal to, (2) greater than, (3) less than, (4) greater than or equal to and (5) less than or equal to.	4.2.6 IA-030000	L	CP SBC (R)
6	The product shall be capable of using Network Address Translation (NAT) and Network Address Port Translation (NAPT) on all VVoIP enclave-to-Wide Area Network (WAN) connections.	4.2.6 IA-032000	L	CP SBC (R)
7	The product shall have the capability to deploy using private address space IAW RFC 1918.	4.2.6 IA-033000	L	CP SBC (R)
8	The SBC shall be an AS-SIP intermediary in all WAN signaling sessions.	4.2.6 IA-034000	L	CP SBC (R)
9	To enable the application of NAT and NAPT, the SBC shall be able to inspect and modify the SDP body (i.e., the SDP "c=" and the "m=" lines) of the corresponding AS-SIP message.	4.2.6 IA-035000	L	CP SBC (R)
10	If the system supports H.323 video sessions, then the SBC shall be capable of supporting H.323 NAT and NAPT.	4.2.6 IA-036000	L	CP SBC (C)
11	If DHCP is used, then the product shall be capable of using 802.1X in combination with a secure EAP type (defined within this UCR and the STIGs/SRGs) residing on the authentication server and within the operating system or application software of the EI and AEI to authenticate to the LAN.	4.2.6 IA-037000	L	EI (C)
12	The product FWs deployed at the boundaries of the VVoIP enclave shall have the capability to use stateful packet inspection.	4.2.6 IA-039000	L	CP SBC (R)
4-5	**4.2.7 - Public Key Infrastructure**			
1	The product shall be capable of generating asymmetric keys whose length is at least 2048 for Rivest Shamir Adleman (RSA).	4.2.7 IA-040000	L	CP MG (R) CP SBC (R) EI (C)
2	The product shall be capable of generating symmetric keys whose length is at least 128 bits. NOTE: This generation must be done in accordance with the STIGs and SRGs, which require cryptographic operations to be in accordance with Federal Information Processing Standard (FIPS) 140-2.	4.2.7 IA-041000	L	CP MG (R) CP SBC (R)
3	The product shall be capable of storing key pairs and their related certificates.	4.2.7 IA-042000	L	CP MG (R) CP SBC (R) EI (C)
4	The product shall operate with DoD-approved trust anchors (e.g., public keys and the associated certificates the relying party deems as reliable and trustworthy, typically root certification authorities [CAs]). IA-043010 Any system that performs PKI certificate validation operations must implement the basic steps outlined in Section 6.1.3 of the internet X.509 certificate specification Request for Comment (RFC) 5280. IA-043020 [Conditional: MG, SBC, EI] The system must also provide the capability to check certificate revocation status as part of the certificate validation process as defined in RFC 5280.	4.2.7 IA-043000	L	CP MG (R) CP SBC (R) EI (C)
5	The product shall be capable of supporting end entity server and device certificates and populating all certificate fields IAW methods described in the "DoD PKI Functional Interface Specification."	4.2.7 IA-044000	L	CP MG (R) CP SBC (R) EI (C)

Table 3-5. Collaboration Tool Capability/Functional Requirements (continued)

CR/FR ID	Requirement	UCR Ref (UCR 2013)	LoC/ TP ID	CP R/O/C
4-5	**4.2.7 - Public Key Infrastructure**			
6	The product shall be capable of using the Lightweight Directory Access Protocol (LDAP) version 3 (LDAPv3), LDAP over TLS (LDAPS), Hypertext Transfer Protocol (HTTP), or HTTP Secure (HTTPS) as appropriate when communicating with DoD-approved PKIs.	4.2.7 IA-045000	L	CP MG (R) CP SBC (R) EI (C)
7	If Certificate Revocation Lists (CRLs) are used, then the product shall be capable of using either the date and time specified in the next update field in the CRL or using a configurable parameter to define the period associated with updating the CRLs.	4.2.7 IA-046000	L	CP MG (C) CP SBC (C)
8	If CRLs are used, then the product shall be capable of obtaining the CRL from the CRL Distribution Point (CDP) extension of the certificate in question. The product shall be able to process HTTP pointers in the CDP field whereas the ability to process HTTPS and LDAP pointers is considered Objective and is not a hard requirement. NOTE: This requirement does not prevent the product from supporting the ability to use manually configured, local CDPs which differ from the CDP provided in the certificate.	4.2.7 IA-047000	L	CP MG (C) CP SBC (C)
9	If Online Certificate Status Protocol (OCSP) is used, then the product shall support the capability to use both the Delegated Trust Model (DTM), whereby the OCSP responder's signing certificates are signed by DoD approved PKI CAs, and the OCSP Trusted Responder model, where the OCSP responder uses a self-signed certificate to sign OCSP responses, IAW DoD PKI PMO guidance. NOTE: The OCSP responder's DTM certificate is appended to every OCSP response sent from the DoD PKI OCSP responders. Products should expect these certificates to change regularly (approximately every 30 days or less). NOTE: RFC 2560 describes both the Trust Responder and Delegated Trust (termed "Authorized Responder" within RFC 2560) models. Though DoD PKI-specific implementation details can be found only in DoD PKI PMO publications. NOTE: In DTM, each CA issues a certificate to the OCSP responder specifically to be used for signing OCSP responses [denoted by the inclusion of the id-ad-ocsp Signing object identifier (OID) in the extended key usage extension of the certificate]. The OCSP signing certificate issued by the CA that issued the certificate whose status is being determined is then used to sign the OCSP response. NOTE: In the Explicit Trust Model (self signed), an OCSP client is explicitly configured to look for a specific certificate to have signed the OCSP response. In this model, OCSP clients typically must have the OCSP responder's signing certificate installed in their local trust store.	4.2.7 IA-048000	L	CP SBC (C)
10	If OCSP is used, then the OCSP responder shall be contacted based on the following information: IA-049010 The OCSP responder preconfigured in the application or toolkit; and IA-049020 The OCSP responder location identified in the OCSP field of the Authority Information Access (AIA) extension of the certificate in question. IA-049030 If both of the above are available, then the product shall be configurable to provide preference for one over the other. IA-049040 The product should (not shall) be configurable to provide preferences or a preconfigured OCSP responder based on the Issuer DN.	4.2.7 IA-049000	L	CP SBC (C)
11	If the EI is PKI enabled, then the EI shall support a mechanism for verifying the status of an SC certificate using a Certificate Trust List (CPL), CRLs, or an online status check (OCSP in the case of the DoD PKI). NOTE: It is understood that the system administrator must ensure that the CPL is current to ensure that the status is accurate. NOTE: When implemented the CRL and OCSP implementation must conform to the CRL and OCSP requirements specified previously and later in this section.	4.2.7 IA-050000	L	EI (C)

Table 3-5. Collaboration Tool Capability/Functional Requirements (continued)

CR/FR ID	Requirement	UCR Ref (UCR 2013)	LoC/ TP ID	CP R/O/C
4-5	**4.2.7 - Public Key Infrastructure**			
12	The product shall support all of the applicable requirements in the latest DoD Public Key Enabled (PKE) Application Requirements specification published by the DoD PKI PMO. NOTE: At the time of this UCR's writing, the "DoD Class 3 Public Key Infrastructure Public Key-Enabled Application Requirements" defines the PKE requirements for DoD products.	4.2.7 IA-052000	L	CP MG (R) CP SBC (R) EI (C)
13	Systems that perform any PKI operations (e.g., certificate path processing, certificate validation, digital signature generation, and encryption) must support RSA keys up to 2048 bits with Secure Hash Algorithm (SHA)-1 and SHA-2 digital signatures as dictated by the National Institute of Standards and Technology (NIST) Special Publications (SP) 800-57, SP 800-78, and SP 800-131A and the DoD Certificate Policy. IA-053010 The product shall support the capability to verify certificates, CRLs, OCSP responses, or any other signed data produced by a DoD approved PKI using RSA in conjunction with the SHA-256 algorithm. NOTE: During the migration to SHA-256, certificate chains may contain a mix of certificates signed using either SHA-1 or SHA-256 within the same chain.	4.2.7 IA-053000	L	CP MG (R) CP SBC (R) EI (C)
14	The product shall log when a session is rejected due to a revoked certificate.	4.2.7 IA-054000	L	CP MG (R) CP SBC (R)
15	The product shall be capable of supporting the development of a certificate path and be able to process the path. NOTE: The path development process produces a sequence of certificates that connect a given end-entity certificate to a trust anchor. The process terminates when either the path tracks from a trust anchor to an end entity or a problem occurs that prohibits validation of the path. IA-055010 The path process shall fail when a problem that prohibits the validation of a path occurs.	4.2.7 IA-055000	L	CP MG (R) CP SBC (R) EI (C)
16	The product shall be capable of ensuring that the intended use of the certificate is consistent with the DoD-approved PKI extensions. IA-056010 The product shall be capable of ensuring that the key usage extension in the end entity certificate is set properly. IA-056020 The product shall be capable of ensuring that the digital signature bit is set for authentication uses. IA-056030 The product shall be capable of ensuring that the non-repudiation bit is set for nonrepudiation uses.	4.2.7 IA-056000	L	CP MG (R) CP SBC (R) EI (C)
17	During VVoIP session establishment, if the product uses an online status check to validate a certificate and the product cannot contact the online status check responder (OSCR) (in the case of the DoD PKI, this will be an RFC 2560 OCSP responder) and backup OSCRs, the product will establish the VVoIP session (e.g., shall not terminate the session), but will log the event and send an alarm to the NMS.	4.2.7 IA-057000	L	CP MG (C) CP SBC (C) EI (C)
18	During VVoIP session establishment, if the product uses CRLs to validate a certificate and the product cannot reach the CDP or any backup CDPs, the product will continue the process (e.g. shall not terminate the session), but will log the event and send an alarm to the NMS.	4.2.7 IA-058000	L	CP MG (C) CP SBC (C) EI (C)

Table 3-5. Collaboration Tool Capability/Functional Requirements (continued)

CR/FR ID	Requirement	UCR Ref (UCR 2013)	LoC/ TP ID	CP R/O/C
4-5	**4.2.7 - Public Key Infrastructure**			
19	Periodically, the system shall examine all of the certificates and trust chains associated with ongoing, long-lived, sessions. The system shall terminate any ongoing sessions based on updated revocation/trust information if it is determined that the corresponding certificates have been revoked, are no longer trusted, or are expired. NOTE: The system must not terminate VVoIP sessions simply because of a failure to retrieve the latest CRL or perform an online status check. IA-059010 [Conditional: MG, SBC, EI] If the system supports manual loading of a CRL or CPLs configured by an administrator, then the system shall check all ongoing sessions as soon as updates to the internally stored CRL or trust lists occur. IA-059020 [Conditional: MG, SBC, EI] If the system supports automated retrieval of a CRL from a CDP, then the system shall immediately check the certificates and trust chains associated with all ongoing sessions against the newly retrieved CRL. IA-059030 [Conditional: MG, SBC, EI,] If the system supports automated retrieval of a CRL from a CDP, then the system shall support the ability to configure the interval in which the CRL is retrieved periodically. IA-059040 [Conditional: MG, SBC, EI] If the system supports queries against an online status check responder (an OCSP responder in the case of the DoD PKI), then the system shall periodically query the responder to determine if the certificates corresponding to any ongoing sessions have been revoked. IA-059050 [Conditional: MG, SBC, EI] If the system supports queries against an online status check responder (an OCSP responder in the case of the DoD PKI), by default, for each session, then the device shall query the online status check responder every 24 hours for as long as the session remains active. IA-059060 [Conditional: MG, SBC, EI] If the system supports queries against an online status check responder (an OCSP responder in the case of the DoD PKI), then the system shall support the ability to configure the interval at which the system periodically queries the online status check responder.	4.2.7 IA-059000	L	CP MG (R) CP SBC (R) EI (C)
20	The system shall be capable of sending an alert when installed certificates corresponding to trust chains, OCSP responder certificates, or any other certificates installed on the device that cannot be renewed in an automated manner, are nearing expiration. NOTE: Since EIs and AEIs are not expected to have direct access to the NMS, the SC, or SS is expected to generate this alert to the NMS on behalf of any subtended EIs or AEIs. However, EIs and AEIs should also alert their users via the EI or AEI user interface when certificates are nearing expiration. NOTE: There is no expectation for vendors to develop a proprietary protocol for this purpose. It is sufficient for an SS, or SC to inspect the certificate of a served EI or AEI during registration time and periodically thereafter for the duration of the signaling session. Some products may also store the certificate associated with their subscribing EIs and AEIs so as to enable this check to be performed even when the EIs and AEIs are offline. IA-060010 [Alarm] By default, the system shall be capable of sending this alert 60 days before the expiration of the installed credentials, which cannot be renewed automatically. This alert should be repeated periodically on a weekly or biweekly basis by default.	4.2.7 IA-060000	L	CP MG (R) CP SBC (R) EI (C)
21	The product shall support the capability to verify that the identity claimed in an X.509v3 certificate Subject Common Name, used to establish an authenticated and secure channel, correctly maps to the identity claimed in signaling messages transmitted within the same secure channel. IA-061010 The product shall support the capability to examine the identity claimed by the X.509v3 Subject Common Name field and compare it to the identity claimed within signaling messages regardless of whether the claimed identity contains an FQDN, IPv4 address, or IPv6 address. IA-061020 [Required: MG, SBC, EI] The product shall support the capability to statically map the FQDNs contained in X.509v3 certificate Subject Common Names to IP addresses via a configurable lookup table.	4.2.7 IA-061000	L	CP MG (R) CP SBC (R) EI (C)

Table 3-5. Collaboration Tool Capability/Functional Requirements (continued)

CR/FR ID	Requirement	UCR Ref (UCR 2013)	LoC/ TP ID	CP R/O/C
4-6	**4.2.8 - Integrity**			
1	The product shall be capable of using TLS for providing integrity of AS-SIP messages. NOTE: The condition for the EI is the support of AS-SIP. IA-062010 The product shall be capable of using Hash-Based Message Authentication Code (HMAC)-SHA1-160 with 160 bit keys.	4.2.8 IA-062000	L	CP SBC (R) EI (C)
2	If the product uses H.323, then the product shall be capable of using H.235.1 Baseline Security Profile guidance for mutually authenticated shared keys and HMAC-SHA1-96 with 160 bit keys.	4.2.8 IA-063000	L	EI (C)
3	The product shall be capable of providing data integrity of the Secure Real-Time Transport Protocol (SRTP) bearer (transport) packets. IA-064010 The product shall be capable of using HMACSHA1-32 for the authentication tag with 160 bit key length as the default integrity mechanism for SRTP packets. IA-064020 The product shall be capable of using HMACSHA1-80 for the authentication tag with 160 bit key length as the default integrity mechanism for Secure Real-Time Transport Control Protocol (SRTCP). NOTE: The ability to process received SRTCP messages is optional, but the capability to transmit SRTCP messages is required.	4.2.8 IA-064000	L	CP MG (R) EI (R)
4	If the product uses IP Security (IPSec), then the product shall be capable of using HMAC-SHA (class value 2) as the default Internet Key Exchange (IKE) integrity mechanism as defined in RFC 2409.	4.2.8 IA-065000	L	CP MG (C)
5	The entire SNMPv3 message shall be checked for integrity and shall use the HMAC-SHA1-96 with 160-bit key length by default.	4.2.8 IA-066000	L	CP MG (R) CP SBC (R)
6	If the product uses SSHv2, then the product shall use HMAC-SHA1-96 with 160 bit key length for data integrity.	4.2.8 IA-067000	L	CP MG (C) CP SBC (C)
7	If the product uses TLS, then the product shall be capable of using TLS in combination with HMAC-SHA1-160 with 160 bit keys to provide integrity for the session packets.	4.2.8 IA-068000	L	CP MG (C) CP SBC (C)
4-7	**4.2.9 - Confidentiality**			
1	The product shall be capable of providing confidentiality for media streams using SRTP with either the AES_CM_128 encryption algorithm as the default. IA-069010 The product shall be capable of distributing the Master Key and the Salt Key in the VVoIP signaling messages IAW RFC 4568. IA-069020 The product shall be capable of distributing the Master Key and the Salt Key in concatenated form. IA-069030 The product shall use a Master Key of 128 bits to support 128-bit Advanced Encryption Standard (AES) encryption. NOTE: This implies that the Master Salt Key may be null. IA-069040 The Master Key and a random Master Salt Key shall be supported for SRTP sessions. IA-069050 When the system assigns the port numbers to a session, the system shall assign the SRTP port ranges within a configurable range between 2048 and 65535 with the default between: 16384 to 32764.	4.2.9 IA-069000	L	CP MG (R) EI (R)
2	If H.323, Media Gateway Control Protocol (MGCP), or H.248 (MEGACO) is used, then the product shall be capable of using IPSec to provide confidentiality. IA-070010 [Conditional: MG] If the product uses H.248 (MEGACO), then the product shall be capable of distributing the SRTP Master Key and Salt Key in the SDP "k=" crypto field when using H.248.15. IA-070020 [Conditional: MG, EI] If H.323 is used, then the product shall be capable of distributing the SRTP Master Key and Salt Key in H.235 using the H235Key as described in H.235.0 and H.235.8.	4.2.9 IA-070000	L	CP MG (C) EI (C)

Table 3-5. Collaboration Tool Capability/Functional Requirements (continued)

CR/FR ID	Requirement	UCR Ref (UCR 2013)	LoC/ TP ID	CP R/O/C
4-7	**4.2.9 - Confidentiality**			
3	If IPSec is used, then the product shall be capable of using IKE for IPSec key distribution: IA-071010 [Required: MG, SBC, EI] The product shall be capable of using IKE version 1. IA-071020 [Conditional: MG, SBC, EI] If IPSec is used, then the product shall be capable of using the digital signature authentication mode with X.509 certificates during Phase I of the Internet Security Association and Key Management Protocol (ISAKMP) negotiation for authentication. IA-071030 [Conditional: MG, SBC, EI] If IPSec is used, then the product shall be capable of using the Quick Mode as the default Phase II Security Association mechanism for the IPSec service. IA-071040 [Conditional: MG, SBC, EI] If IPSec is used, then the product shall be capable of using and interpreting certificate requests for Public-Key Cryptography Standard #7 (PKCS#7) wrapped certificates as a request for the whole path of certificates. IA-071050 [Conditional: MG, SBC, EI] If IPSec is used, then the product shall be capable of using Main Mode associated with the Diffie-Hellman approach for key generation for the security association negotiation. IA-071060 [Conditional: MG, SBC, EI] If IPSec is used, then the product shall be capable of using Diffe-Hellman Groups 1, 2, and 14, at a minimum. IA-071070 [Conditional: MG] If the product uses IPSec, then the system shall be capable of using AES_128_CBC as the default encryption algorithm. The system shall be capable of supporting 3DES-CBC (class value 5) for backwards compatibility with previous UCR revisions. IA-071080 [Conditional: MG, SBC, EI] [Former ID: 5.4.6.2.3 1.c.1.c.vi.A] If IPSec is used, then the product shall only support the following erroneous messages associated with a certificate request: (1) Invalid Key. (2) Invalid ID. (3) Invalid certificate encoding. (4) Invalid certificate. (5) Certificate type unsupported. (6) Invalid CA. (7) Invalid hash. (8) Authentication failed. (9) Invalid signature. (10) Certificate unavailable.	4.2.9 IA-071000	L	CP MG (C) CP SBC (C) EI (C)

Table 3-5. Collaboration Tool Capability/Functional Requirements (continued)

CR/FR ID	Requirement	UCR Ref (UCR 2013)	LoC/ TP ID	CP R/O/C
4-7	**4.2.9 - Confidentiality**			
4	The product shall be capable of using TLS (dual path method) to provide confidentiality for the AS-SIP as described in RFC 3261. IA-072010 [Required: SBC, Conditional: EI] The underlying protocol for AS-SIP shall be the TCP. IA-072020 [Required: MG, SBC Conditional: EI] The product shall be capable of using as its default cipher suite TLS_RSA_WITH_AES_128_CBC_SHA. IA-072030 [Required: MG, SBC Conditional: EI] The product shall be capable of using a default of no compression for AS-SIP messages. IA-072040 [Required: MG, SBC Conditional: EI] The product shall be capable of exchanging AS-SIP TLS messages in a single exchange or multiple exchanges. IA-072050 [Required: MG, SBC Conditional: EI] The product shall be capable of distributing the SRTP Master Key and Salt Key in the AS-SIP message using the SDP crypto= field. NOTE: EI condition is whether it supports AS-SIP. IA-072060 [Conditional: EI, SBC] If AS-SIP is used, then the product shall transmit only packets that are secured with TLS and use port 5061. NOTE: The products may use other signaling protocols for interfacing to e.g. MGs, EIs. IA-072070 [Required: EI, SBC] The product shall reject all received AS-SIP packets associated with port 5061 that are not secured with TLS. NOTE: This ensures that the product does not process UDP, Stream Control Transmission Protocol (SCPP), and TCP SIP packets that are not secured using a combination of TLS and TCP. IA-072080 [Required: EI, SBC] The product shall only accept and process AS-SIP packets that arrive on port 5061. NOTE: The product should discard AS-SIP packets that arrive on a different port.	4.2.9 IA-072000	L	CP SBC (R)
5	If the product uses TLS, then the product shall do so in a secure manner as defined by the following subtended requirements. IA-073010 [Conditional: MG, SBC, EI] If the product uses TLS, then the system shall be capable of using TLS_RSA_WITH_AES_128_CBC_SHA as its default cipher suite. IA-073020 [Conditional: MG, SBC, EI] If the product uses TLS, then the system shall be capable of using a default of no compression. IA-073030 [Conditional: MG, SBC, EI] If the product uses TLS, then the system shall be capable of exchanging TLS messages in a single exchange or multiple exchanges. IA-073040 [Conditional: MG, SBC, EI] If TLS session resumption is used, then a timer associated with TLS session resumption shall be configurable and the default shall be 1 hour. NOTE: This requirement is not associated with NM-related sessions. IA-073050 [Conditional: MG, SBC, EI] If TLS session resumption is used, then the maximum time allowed for a TLS session to resume (session resumption) without repeating the TLS authentication/confidentiality/ authorization process (e.g., a full handshake) is 1 hour. IA-073060 [Required: MG, SBC, EI] If the product supports SSL/TLS renegotiation, then the product shall support the capability to disable this feature or the product shall support RFC 5746.	4.2.9 IA-073000	L	CP MG (C) CP SBC (C) EI (C)

Table 3-5. Collaboration Tool Capability/Functional Requirements (continued)

CR/FR ID	Requirement	UCR Ref (UCR 2013)	LoC/ TP ID	CP R/O/C
4-7	**4.2.9 - Confidentiality**			
6	If the product uses Secure Shell (SSH), then the system shall do so in a secure manner as defined by the following subtended requirements. NOTE: An EI's remote manual configurations shall not be enabled and all non-automatic processes shall be performed locally. IA-074010 [Conditional: MG, SBC, EI] If the product uses SSH, then the system shall be capable of supporting the RSA 2,048-bit key algorithm and the Diffie-Hellman 2,048 bit key algorithm. IA-074020 [Conditional: MG, SBC, EI] If the product uses SSH, then a client shall close the session if it receives a request to initiate an SSH session whose version is less than 2.0. NOTE: Closing the session may be either a default behavior or a configurable option. If this is a configurable option, then the conditions of fielding should clearly specify that this option must be configured. IA-074030 [Conditional: MG, SBC, EI] If the product uses SSH, then the SSH sessions shall rekey at a minimum every gigabyte of data received or every 60 minutes, whichever comes sooner. IA-074040 [Conditional: MG, SBC, EI] If the product uses SSH, then the SSH sessions shall rekey at a minimum every gigabyte of data transmitted or every 60 minutes, whichever comes sooner. IA-074050 [Conditional: MG, SBC, EI] If the product uses SSH, then the SSH sessions shall minimally support the AES 128-CBC algorithm as defined in RFC 4253. IA-074070 [Conditional: MG, SBC, EI] If the product uses SSH, then the SSH sessions shall use TCP as the underlying protocol. IA-074080 [Conditional: MG, SBC, EI] If the product uses SSH, then it shall be capable of processing packets with uncompressed payload lengths up to 32,768 bytes or shall be configurable to specify that value; also, this length shall be the default value. This does not preclude the system from automatically sizing the Maximum Transmission Unit (MTU) if it is less than 32,768. IA-074090 [Conditional: MG, SBC, EI] If the product uses SSH, then the SSH packets shall have a maximum packet size of 35,000 bytes or shall be configurable to that value; also, this length shall be the default value. NOTE: The 35,000 bytes includes the packet_length, padding_length, payload, random padding, and MAC. IA-074100 [Conditional: MG, SBC, EI] If the product uses SSH, then the product shall discard SSH packets that exceed the maximum packet size to avoid denial of service (DoS) attacks or buffer overflow attacks. IA-074110 [Conditional: MG, SBC, EI] If the product uses SSH, then the SSH packets shall use random bytes if packet padding is required. IA-074120 [Conditional: MG, SBC, EI] If the product uses SSH, then the system shall treat all SSH-encrypted packets sent in one direction as a single data stream. For example, the initialization vectors shall be passed from the end of one packet to the beginning of the next packet. IA-074130 [Conditional: MG, SBC, EI] If the product uses SSH, then the system shall be capable of setting Diffie-Hellman-Group14-SHA1 as the preferred key exchange mechanism for SSH.	4.2.9 IA-074000	L	CP MG (C) CP SBC (C) EI (C)
7	If the product uses SSH with X.509v3 certificates and provides an SSH server function, then the SSH server shall support the capability to use an X.509v3 certificate provided by a DoD-approved PKI. IA-075010 [Conditional: MG, SBC] If the product uses SSH with X.509v3 certificates and provides an SSH server function, then the SSH Server function shall support, at a minimum, the "x509v3-ssh-rsa" and "x509v3-rsa2048-sha256" key types as defined in RFC 6187 IA-075020 [Conditional: MG, SBC] If the product uses SSH with X.509v3 certificates and provides an SSH server function, then the SSH Server function shall support the capability to, in a configurable manner, specify the highest preferred key type advertised during the SSH_MSG_KEXINIT message exchange. IA-075030 [Conditional: MG, SBC] If the product uses SSH with X.509v3 certificates and provides an SSH server function, then the SSH server function shall support the capability to deny SSH sessions when the session fails to negotiate a configured set of preferred key types.	4.2.9 IA-075000	L	CP MG (C) CP SBC (C)

Table 3-5. Collaboration Tool Capability/Functional Requirements (continued)

CR/FR ID	Requirement	UCR Ref (UCR 2013)	LoC/ TP ID	CP R/O/C
4-7	**4.2.9 - Confidentiality**			
8	If the product uses SSH with X.509v3 certificates and provides an SSH server function, then the SSH client shall support the capability to use an X.509v3 certificate provided by a DoD-approved PKI. IA-076010 [Conditional: MG, SBC] If the product provides an SSH client function and the SSH client has a CAC (or equivalent) reader, then the SSH client may use the X.509v3 certificate on the user's CAC to establish the encrypted session. IA-076020 [Conditional: MG, SBC] If the product uses SSH and if the client has a CAC (or equivalent) reader and also has its own PKI certificate from a DoD-approved PKI, then the client may use either its certificate or the certificate on the user's CAC to establish the encrypted sessions. IA-076030 [Conditional: MG, SBC] If the product uses SSH with X.509v3 certificates, and provides an SSH client function, then the SSH client shall support, at a minimum, the "x509v3-ssh-rsa" and "x509v3-rsa2048-sha256" key types as defined in RFC 6187.	4.2.9 IA-076000	L	CP MG (C) CP SBC (C)
9	The product shall be capable of using SNMPv3 for all SNMP sessions. IA-077010 [Required: MG, SBC] The security level for SNMPv3 in the DoD VVoIP environment shall be authentication with privacy – snmpSecurityLevel=authPriv. The product shall set snmpSecurityLevel=authPriv as the default security level used during initial configuration. IA-077020 [Required: MG, SBC] The SNMPv3 implementation shall be capable of allowing an appropriate administrator to manually configure the snmpEngineID from the operator console. A default unique snmpEngineID may be assigned to avoid unnecessary administrative overhead, but this must be changeable. IA-077030 [Required: MG, SBC] The security model for SNMPv3 shall be the User-Based Security Model – snmpSecurityModel =3. IA-077040 [Conditional: MG, SBC] If the product receives SNMPv3 response messages, then the product shall conduct a timeliness check on the SNMPv3 message. IA-077050 [Required: MG, SBC] An SNMPv3 engine shall perform time synchronization using authenticated messages. IA-077060 [Required: SS, SC, MG, SBC, RSF, R, LS, SD] The message processing model shall be SNMPv3 – snmpMessageProcessingModel=3. IA-077070 [Required: MG, SBC] For backwards compatibility, the product shall support the capability to use Data Encryption Standard- Cipher Block Chaining (DES-CBC) (usmDESPrivProtocol) with a 16 octet (128 bit) input key, as specified in RFC 3414, as an encryption cipher for SNMPv3. IA-077080 [Required: MG, SBC] The product shall support the capability to use the CFB-AES128 encryption cipher usmAesCfb128PrivProtocol for SNMPv3 as defined in RFC 3826 and specify this as the default encryption cipher for SNMPv3. IA-077090 [Conditional: MG, SBC] If the product receives SNMPv3 response messages, then the SNMPv3 engine shall discard SNMP response messages that do not correspond to any current outstanding Request messages. IA-077100 [Conditional: MG, SBC] If the product receives SNMPv3 responses, then the SNMPv3 Command Generator Application shall discard any Response Class Protocol Data Unit (PDU) for which there is no outstanding Confirmed Class PDU. IA-077110 [Required: MG, SBC] When using msgID for correlating Response messages to outstanding Request messages, the SNMPv3 engine shall use different msgIDs in all such Request messages that it sends out during a 150 second Time Window. IA-077120 [Required: MG, SBC] An SNMPv3 Command Generator or Notification Originator Application shall use different request-ids in all Request PDUs that it sends out during a Time Window.	4.2.9 IA-077000	L	CP MG (C) CP SBC (C)

Table 3-5. Collaboration Tool Capability/Functional Requirements (continued)

CR/FR ID	Requirement	UCR Ref (UCR 2013)	LoC/ TP ID	CP R/O/C
4-7	**4.2.9 - Confidentiality**			
9 Cont'd	IA-077130 [Required: MG, SBC] When sending state altering messages to a managed authoritative SNMPv3 engine, a Command Generator Application should delay sending successive messages to that managed SNMPv3 engine until a positive acknowledgement is received from the previous message or until the message expires. IA-077140 [Required: MG, SBC] The product using SNMPv3 shall implement the key-localization mechanism.	4.2.9 IA-077000	L	CP MG (C) CP SBC (C)
10	If the product uses web browsers or web servers, then the product web browsers and web servers shall be capable of supporting TLS 1.0 or higher for confidentiality.	4.2.9 IA-078000	L	CP MG (C) CP SBC (C) EI (C)
11	The product shall be capable of using SSHv2 or TLS 1.0 or higher for remote configuration of appliances. NOTE: The EIs and AEIs remote manual configurations shall not be enabled and all non-automatic processes shall be performed locally.	4.2.9 IA-079000	L	CP MG (C) CP SBC (C)
12	If the product uses different signaling protocols (i.e., H.323 and AS-SIP), then the system shall be capable of translating or transferring the bearer keys between different signaling protocols. NOTE: The rekeying is designed to prevent the "forwarding party" from having the key to the bearer session associated with the originating party and the forwarded-to party. If the forwarding party had the key to the bearer session, then the forwarding party would be able to eavesdrop on the forwarded session. SCs, and SS may act as a B2BUA for an EI or an AEI and so would originate the AS-SIP session on behalf of the EI or AEI.	4.2.9 IA-080000	L	CP MG (C)
13	If the product is the originating party and receives a 181 message indicating that the call is being forwarded, then, upon completion of the session establishment between the originating party and the forwarded-to party, the originating party must initiate a rekeying.	4.2.9 IA-081000	L	CP MG (C) EI (C)
14	If the EI or AEI acts as a bridge or a MCU, then it shall establish a unique key for each EI or AEI connection.	4.2.9 IA-082000	L	EI (C)
15	If the product transmits decrypted VVoIP signaling and/or bearer traffic to an external IDS/IPS, then confidentiality for the decrypted signaling and media traffic shall be ensured using cryptographic protection, where the strength of the cryptographic protocol/algorithms used is greater than or equal to the TLS and SRTP cryptographic profiles defined in this document.	4.2.9 IA-083000	L	CP SBC (C)
4-8	**4.2.10 – Non-Repudiation**			
1	The security log shall be capable of using a circular (or equivalent) recording mechanism (i.e., oldest record overwritten by newest).	4.2.10 IA-084000	L	CP MG (R) CP SBC (R)
2	Only the System Security Administrator and System Administrator roles shall have the ability to retrieve, print, copy, and upload the security log(s)	4.2.10 IA-085000	L	CP MG (R) CP SBC (R)
3	The product/system shall be able to generate a human understandable presentation of any audit data stored in the audit trail.	4.2.10 IA-086000	L	CP MG (R) CP SBC (R)
4	The product shall provide a mechanism to locally store audit log/event data when communication with the management station is unavailable. NOTE: In the case of protocols that use unreliable delivery, such as syslog over UDP, use of mechanisms at lower Open System Interconnect (OSI) layers (e.g. ICMP, OSI Layer 1 and 2 mechanisms) must be used to detect such connectivity issues.	4.2.10 IA-087000	L	CP MG (R) CP SBC (R)

Table 3-5. Collaboration Tool Capability/Functional Requirements (continued)

CR/FR ID	Requirement	UCR Ref (UCR 2013)	LoC/ TP ID	CP R/O/C
5	**Section 5 - IPv6**			
5-1	**5.2.1 - Product**			
1	The product shall support dual IPv4 and IPv6 stacks as described in RFC 4213.	5.2.1 IP6-000010	L/T	CP Server (R) CP SBC (R) EI (R)
2	Dual-stack end points or Call Connection Agents (CCAs) shall be configured to choose IPv4 over IPv6.	5.2.1 IP6-000020	L/T	CP Server (R) CP SBC (R) EI (R)
3	All nodes and interfaces that are "IPv6-capable" must be carefully configured and verified that the IPv6 stack is disabled until it is deliberately enabled as part of a deliberate transition strategy. This includes the stateless autoconfiguration of link-local addresses. Nodes with multiple network interfaces may need to be separately configured per interface.	5.2.1 IP6-000030	L/T	CP Server (R) CP SBC (R) EI (R)
4	The system shall provide the same (or equivalent) functionality in IPv6 as in IPv4 consistent with the requirements in the UCR for its Approved Products List (APL) category. NOTE: This requirement applies only to products that are required to perform IPv6 functionality.	5.2.1 IP6-000050	L/T	CP Server (R) CP SBC (R) EI (R)
5	The product shall support the IPv6 format as described in RFC 2460 and updated by RFC 5095. [Conditional: LS] If the LS also supports a routing function, then the product shall support RFC 2460 and be updated by RFC 5095.	5.2.1 IP6-000060	L	CP Server (R) CP SBC (R) EI (R)
6	The product shall support the transmission of IPv6 packets over Ethernet networks using the frame format defined in RFC 2464. NOTE: This requirement does not mandate that the remaining sections of RFC 2464 have to be implemented.	5.2.1 IP6-000070	L	CP Server (R) CP SBC (R) EI (R)
7	The product shall support Path Maximum Transmission Unit (MTU) Discovery as described in RFC 1981.	5.2.1 IP6-000080		CP SBC (R) EI (soft) (R)
8	The product shall support a minimum MTU of 1280 bytes as described in RFC 2460 and updated by RFC 5095. NOTE: Guidance on MTU requirements and settings can be found in Section 6.11.4.2, Layer 2 – Data Link Layer.	5.2.1.1 IP6-000090	L	CP Server (R) CP SBC (R) EI (R)
9	If Path MTU Discovery is used and a "Packet Too Big" message is received requesting a next-hop MTU that is less than the IPv6 minimum link MTU, then the product shall ignore the request for the smaller MTU and shall include a fragment header in the packet. NOTE: Unlike IPv4, fragmentation in IPv6 is performed only by source nodes, not by routers along a packet's delivery path.	5.2.1.1 IP6-000100	L	CP Server (C) CP SBC (C) EI (C)
10	The product shall not use the Flow Label field as described in RFC 2460.	5.2.1.2 IP6-000110	L	CP Server (R) CP SBC (R) EI (R)
11	The product shall be capable of setting the Flow Label field to zero when originating a packet.	5.2.1.2 IP6-000120	L	CP Server (R) CP SBC (R) EI (R)
12	The product shall be capable of ignoring the Flow Label field when receiving packets.	5.2.1.2 IP6-000140	L	CP Server (R) CP SBC (R) EI (R)

Table 3-5. Collaboration Tool Capability/Functional Requirements (continued)

CR/FR ID	Requirement	UCR Ref (UCR 2013)	LoC/ TP ID	CP R/O/C
5-1	**5.2.1 - Product**			
13	The product shall support the IPv6 Addressing Architecture as described in RFC 4291. NOTE 1: According to "DoD IPv6 Standard Profiles For IPv6-capable Products-Supplemental Guidance" version 6.0, the use of "IPv4-mapped" addresses "on-the-wire" is discouraged due to security risks raised by inherent ambiguities. NOTE 2: As noted in National Institute of Standards and Technology (NIST) Special Publication (SP) 500-267 25, "A Profile for IPv6 in the U.S. Government – Version 1.0": The use of the old Site-Local address type (RFC3879) is deprecated. The Unique Local IPv6 Unicast Addresses (ULA) (RFC 4193) mechanism has been designed to fulfill a similar requirement. While Private Addresses are widely used in IPv4 networks, generalized ULA use and support in IPv6 are not as mature nor is their architectural desirability as well understood. For these reasons, the UC products are not required to support ULA at this time. NOTE 3: An end site is defined as an end-user (subscriber) edge network domain that requires multiple subnets/64. Therefore, vendors will not be required to support anything greater than /64, such as /116 or /126 subnet.	5.2.1.3 IP6-000150	L	CP Server (R) CP SBC (R) EI (R)
14	The product shall support the IPv6 Scoped Address Architecture as described in RFC 4007.	5.2.1.3 IP6-000160	L	CP Server (R) CP SBC (R) EI (R)
15	If a scoped address (RFC 4007) is used, then the product shall use a scope index value of zero when the default zone is intended.	5.2.1.3 IP6-000170	L	CP Server (C) CP SBC (C) EI (C)
16	If Dynamic Host Configuration Protocol (DHCP) is supported within an IPv6 environment, then it shall be implemented in accordance with the DHCP for IPv6 (DHCPv6) as described in RFC 3315.	5.2.1.4 IP6-000180	L	EI (R) CP Server(C)
17	If the product is a DHCPv6 client, then the product shall discard any messages that contain options that are not allowed to appear in the received message type (e.g., an Identity Association option in an Information-Request message).	5.2.1.4 IP6-000200	L	EI (C) CP Server (C)
18	The product shall support DHCPv6 as described in RFC 3315. NOTE: The following subtended requirements are predicated upon an implementation of DHCPv6 for the EI. It is not expected that other UC appliances will use DHCPv6.	5.2.1.4 IP6-000210	L	EI (R)
19	If the product is a DHCPv6 client and the first retransmission timeout has elapsed since the client sent the Solicit message and the client has received an Advertise message(s), but the Advertise message(s) does not have a preference value of 255, then the client shall continue with a client-initiated message exchange by sending a Request message.	5.2.1.4 IP6-000220	L	EI (R) CP Server (C)
20	If the product is a DHCPv6 client and the DHCPv6 solicitation message exchange fails, then it shall restart the reconfiguration process after receiving user input, system restart, attachment to a new link, a system configurable timer, or a user defined external event occurs. NOTE: The intent is to ensure that the DHCP client continues to restart the configuration process periodically until it succeeds.	5.2.1.4 IP6-000230	L	EI (R) CP Server (C)
21	If the product is a DHCPv6 client and it sends an Information-Request message, then it shall include a Client Identifier option to allow it to be authenticated to the DHCPv6 server.	5.2.1.4 IP6-000240	L	EI (R) CP Server (C)
22	If the product is a DHCPv6 client, then it shall perform duplicate address detection upon receipt of an address from the DHCPv6 server before transmitting packets using that address for itself.	5.2.1.4 IP6-000250	L	EI (R) CP Server (C)
23	If the product is a DHCPv6 client, then it shall log all reconfigure events. NOTE: Some systems may not be able to log all this information (e.g., the system may not have access to this information).	5.2.1.4 IP6-000260	L	EI (R) CP Server (C)

Table 3-5. Collaboration Tool Capability/Functional Requirements (continued)

CR/FR ID	Requirement	UCR Ref (UCR 2013)	LoC/ TP ID	CP R/O/C
5-1	**5.2.1 - Product**			
24	If the product supports DHCPv6 and uses authentication, then it shall discard unauthenticated DHCPv6 messages from UC products and log the event. NOTE: Some systems may not be able to log all this information (e.g., the system may not have access to this information).	5.2.1.4 IP6-000270	L	EI (C) CP Server (C)
25	The product shall support Neighbor Discovery for IPv6 as described in RFC 4861.	5.2.1.5 IP6-000280	L	EI (R) CP Server (R) CP SBC (R)
26	The product shall not set the override flag bit in the Neighbor Advertisement message for solicited advertisements for any cast addresses or solicited proxy advertisements.	5.2.1.5 IP6-000300	L	EI (R) CP Server (R) CP SBC (R)
27	When a valid "Neighbor Advertisement" message is received by the product and the product neighbor cache does not contain the target's entry, the advertisement shall be silently discarded.	5.2.1.5 IP6-000310	L	EI (R) CP Server (R) CP SBC (R)
28	When a valid "Neighbor Advertisement" message is received by the product and the product neighbor cache entry is in the INCOMPLETE state when the advertisement is received and the link layer has addresses and no target link-layer option is included, the product shall silently discard the received advertisement.	5.2.1.5 IP6-000320	L	EI (R) CP Server (R) CP SBC (R)
29	When address resolution fails on a neighboring address, the entry shall be deleted from the product's neighbor cache.	5.2.1.5 IP6-000330	L	EI (R) CP Server (R) CP SBC (R
30	The product shall support the ability to configure the product to ignore Redirect messages.	5.2.1.5.1 IP6-000340	L	EI (R) CP Server (R) CP SBC (R
31	The product shall only accept Redirect messages from the same router as is currently being used for that destination. NOTE: The intent of this requirement is that if a node is sending its packets destined for location A to router X, that it can only accept a Redirect message from router X for packets destined for location A to be sent to router Z.	5.2.1.5.1 IP6-000350	L	EI (R) CP Server (R) CP SBC (R
32	If "Redirect" messages are allowed, then the product shall update its destination cache in accordance with the validated Redirect message.	5.2.1.5.1 IP6-000360	L	EI (C) CP Server (C)
33	If the valid "Redirect" message is allowed and no entry exists in the destination cache, then the product shall create an entry.	5.2.1.5.1 IP6-000370	L	EI (C) CP Server (C)
34	If redirects are supported, then the device shall support the ability to disable this functionality. NOTE: The default setting is "disabled" so that the redirect functions must explicitly be "enabled."	5.2.1.5.1 IP6-000380	L	EI (C) CP Server (C)
35	The product shall prefer routers that are reachable over routers whose reachability is suspect or unknown.	5.2.1.5.2 IP6-000400	L	EI (R) CP Server (R) CP SBC (R
36	If the product supports stateless IP address autoconfiguration including those provided for the commercial market, then the product shall support IPv6 Stateless Address Autoconfiguration (SLAAC) for interfaces supporting UC functions in accordance with RFC 4862. NOTE 1: RFC 4862 has replaced the now-obsolete RFC 2462. The scope of RFC 2462, Section 5.5, is Creation of Global and Site-Local Addresses. The scope of RFC 4862, Section 5.5, is Creation of Global Addresses. NOTE 2: "DoD IPv6 Standard Profiles for IPv6-capable Products-Supplemental Guidance" defines Host as a PC or other end-user computer or workstation running a general-purpose operating system. NOTE 3: The UC EI platform (on which the softphone is located) may be certified to the DoD IPv6 Profile and required to support autonomous configuration, either SLAAC or DHCPv6 client.	5.2.1.6 IP6-000420	L	EI (C) CP Server (C) CP SBC (C)

Table 3-5. Collaboration Tool Capability/Functional Requirements (continued)

CR/FR ID	Requirement	UCR Ref (UCR 2013)	LoC/ TP ID	CP R/O/C
5-1	**5.2.1 - Product**			
37	If the product supports IPv6 SLAAC, then the product shall have a configurable parameter that allows the function to be enabled and disabled. Specifically, the product shall have a configurable parameter that allows the "managed address configuration" flag and the "other stateful configuration" flag to always be set and not perform stateless autoconfiguration.	5.2.1.6 IP6-000430	L	EI (C) CP Server (C) CP SBC (C)
38	If the product supports IPv6 SLAAC, then the product shall have the configurable parameter set not to perform stateless autoconfiguration. NOTE: The objective of this requirement is to prevent a product from using stateless auto configuration. Stateless address autoconfiguration is focused solely on softphones since they reside on PCs.	5.2.1.6 IP6-000440	L	EI (C) EI(soft) (R) CP Server (C) CP SBC (C)
39	While nodes are not required to autoconfigure their addresses using SLAAC, all IPv6 Nodes shall support link-local address configuration and Duplicate Address Detection (DAD) as specified in RFC 4862. In accordance with RFC 4862, DAD shall be implemented and shall be on by default. Exceptions to the use of DAD are noted in the following text.	5.2.1.6 IP6-000450	L	EI (R) CP Server (R) CP SBC (R)
40	A node MUST allow for autoconfiguration-related variable to be configured by system management for each multicast-capable interface to include DupAddrDetectTransmits where a value of zero indicates that DAD is not performed on tentative addresses as specified in RFC 4862. NOTE: Network Infrastructure Security Technical Implementation Guide (STIG) states the following: The use of Duplicate Address Detection opens up the possibility of denial of service attacks. Any node can respond to Neighbor Solicitations for a tentative address, causing the other node to reject the address as a duplicate. This attack is similar to other attacks involving the spoofing of Neighbor Discovery messages. Further, RFC 4862 states the following: By default, all addresses should be tested for uniqueness prior to their assignment to an interface for safety. The test should individually be performed on all addresses obtained manually, via stateless address autoconfiguration, or via DHCPv6. To accommodate sites that believe the overhead of performing Duplicate Address Detection outweighs its benefits, the use of Duplicate Address Detection can be disabled through the administrative setting of a per-interface configuration flag. The products may include an administrative setting to disable DAD.	5.2.1.6 IP6-000460	L	EI (R) CP Server (R) CP SBC (R)
41	The product shall support manual assignment of IPv6 addresses.	5.2.1.6 IP6-000470	L	EI (R) CP Server (R) CP SBC (R)
42	The product shall support Stateful autoconfiguration (i.e., managedFlag= TRUE) as described in RFC 4862. NOTE: This requirement is associated with the earlier Requirement 10.2 for the EI to support DHCPv6.	5.2.1.6 IP6-000480	L	EI (soft) (R)
43	If the product supports a subtended appliance behind it, then the product shall ensure that the IP address assignment process of the subtended appliance is transparent to the UC components of the product and does not cause the product to attempt to change its IP address. NOTE: An example is a PC that is connected to the LAN through the hub or switch interface on a phone. The address assignment process of the PC should be transparent to the EI and should not cause the phone to attempt to change its IP address.	5.2.1.6 IP6-000500	L	EI (C)
44	If the product supports SLAAC and security constraints prohibit the use of hardware identifiers as part of interface addresses generated using SLAAC, then Internet Protocol Security (IPSec)-capable products shall support privacy extensions for stateless address autoconfiguration as defined in RFC 4941.	5.2.1.6 IP6-000510	L	EI (soft) (C)
45	The product shall support the Internet Control Message Protocol (ICMP) for IPv6 as described in RFC 4443.	5.2.1.7 IP6-000520	L	EI (R) CP Server (R) CP SBC (R)

Table 3-5. Collaboration Tool Capability/Functional Requirements (continued)

CR/FR ID	Requirement	UCR Ref (UCR 2013)	LoC/ TP ID	CP R/O/C
5-1	**5.2.1 - Product**			
46	The product shall support the capability to enable or disable the ability of the product to generate a Destination Unreachable message in response to a packet that cannot be delivered to its destination for reasons other than congestion. NOTE: In lieu of the RFC 4443 paragraph 3.1 requirement to prohibit routers from forwarding a code 3 (address unreachable) message on point-to-point link back onto the arrival link, vendors may alternatively use a prefix length of 127 on Inter-Router Links to address ping-pong issues on non-Ethernet interfaces (the ping-pong issue is not present on Ethernet interfaces).	5.2.1.7 IP6-000540	L	CP Server (R) CP SBC (R)
47	The product shall support the enabling or disabling of the ability to send an Echo Reply message in response to an Echo Request message sent to an IPv6 multicast or anycast address. NOTE: The number of responses may be traffic conditioned to limit the effect of a denial of service attack.	5.2.1.7 IP6-000550	L	EI (R) CP Server (R) CP SBC (R)
48	The product shall validate ICMPv6 messages, using the information contained in the payload, before acting on them. NOTE: The actual validation checks are specific to the upper layers and are out of the scope of this UCR. Protecting the upper layer with IPSec mitigates these attacks.	5.2.1.7 IP6-000560	L	EI (R) CP Server (R) CP SBC (R)
49	If the product supports routing functions, then the product shall support the Multicast Listener Discovery (MLD) process as described in RFC 2710 and extended in RFC 3810. NOTE: The current VVoIP design does not use multicast, but routers supporting VVoIP also support data applications that may use multicast. A softphone will have nonrouting functions that require MLDv2. a. If the product supports MLD process as described in RFC 2710 and extended in RFC 3810, then the product shall support RFC 2711.	5.2.1.7 IP6-000670	L	EI (soft) (R)
50	The product shall support MLD as described in RFC 2710. NOTE: This requirement was added to ensure that Neighbor Discovery multicast requirements are met. Routers are not included in this requirement since they have to meet RFC 2710 in the preceding requirement.	5.2.1.8 IP6-000680	L	EI (R) CP Server (R) CP SBC (R)
51	If the product uses IPSec, then the product shall be compatible with the Security Architecture for the IPSec described in RFC 4301. NOTE 1: RFC 4301 mandates support for several features for which support is available in Internet Key Exchange (IKE) version 2 (IKEv2) but not in IKEv1, e.g., negotiation of a Security Association (SA) representing ranges of local and remote ports or negotiation of multiple SAs with the same selectors. However, at this time the UCR does not require the use of IKEv2. Therefore, implementation at this time of RFC 4301 will include only those features, which are compatible with the use of IKEv1. NOTE 2: The interfaces required to use IPSec are defined in Section 4, Information Assurance. If RFC 4301 is supported, then the product shall support binding of a SA with a particular context. If RFC 4301 is supported, then the product shall be capable of disabling the BYPASS IPSec processing choice. NOTE: The intent of this requirement is to ensure that no packets are transmitted unless they are protected by IPSec.	5.2.1.9 IP6-000690	L	EI (soft) (R) EI (C) CP Server (C) CP SBC (C)
52	If RFC 4301 is supported, then the product shall not support the mixing of IPv4 and IPv6 in a SA.	5.2.1.9 IP6-000700	L	EI (soft) (R) EI (C) CP Server (C) CP SBC (C)
53	If RFC 4301 is supported, then the product's security association database (SAD) cache shall have a method to uniquely identify a SAD entry. NOTE: The concern is that a single SAD entry will be associated with multiple security associations. RFC 4301, Section 4.4.2, Security Association Database (SAD), describes a scenario where this could occur.	5.2.1.9 IP6-000710	L	EI (soft) (R) EI (C) CP Server (C) CP SBC (C)

Table 3-5. Collaboration Tool Capability/Functional Requirements (continued)

CR/FR ID	Requirement	UCR Ref (UCR 2013)	LoC/ TP ID	CP R/O/C
5-1	**5.2.1 - Product**			
54	If RFC 4301 is supported, then the product shall implement IPSec to operate with both integrity and confidentiality.	5.2.1.9 IP6-000720	L	EI (soft) (R) EI (C) CP Server (C) CP SBC (C)
55	If RFC 4301 is supported, then the product shall be capable of enabling and disabling the ability of the product to send an ICMP message informing the sender that an outbound packet was discarded.	5.2.1.9 IP6-000730	L	EI (soft) (R) EI (C) CP Server (C) CP SBC (C)
56	If an ICMP outbound packet message is allowed, then the product shall be capable of rate limiting the transmission of ICMP responses.	5.2.1.9 IP6-000740	L	EI (soft) (R) EI (C) CP Server (C) CP SBC (C)
57	If RFC 4301 is supported, then the system's Security Policy Database (SPD) shall have a nominal, final entry that discards anything unmatched.	5.2.1.9 IP6-000750	L	EI (soft) (R) EI (C) CP Server (C) CP SBC (C)
58	If RFC 4301 is supported, and the product receives a packet that does not match any SPD cache entries, and the product determines it should be discarded, then the product shall log the event and include the date/time, Security Parameter Index (SPI) if available, IPSec protocol if available, source and destination of the packet, and any other selector values of the packet. NOTE: Some products may not be able to log all this information (e.g., the product may not have access to this information).	5.2.1.9 IP6-000760	L	EI (soft) (R) EI (C) CP Server (C) CP SBC (C)
59	If RFC 4301 is supported, then the product should include a management control to allow an administrator to enable or disable the ability of the product to send an IKE notification of an INVALID_SELECPORS. NOTE: Some products may not be able to log all this information (e.g., the product may not have access to this information).	5.2.1.9 IP6-000770	L	EI (soft) (R) EI (C) CP Server (C) CP SBC (C)
60	If RFC 4301 is supported, then the product shall support the ESP Protocol in accordance with RFC 4303.	5.2.1.9 IP6-000780	L	EI (soft) (R) EI (C) CP Server (C) CP SBC (C)
61	If RFC 4303 is supported, then the product shall be capable of enabling anti-replay.	5.2.1.9 IP6-000790	L	EI (soft) (R) EI (C) CP Server (C) CP SBC (C)
62	If RFC 4303 is supported, then the product shall check, as its first check, after a packet has been matched to its SA whether the packet contains a sequence number that does not duplicate the sequence number of any other packet received during the life of the security association.	5.2.1.9 IP6-000800	L	EI (soft) (R) EI (C) CP Server (C) CP SBC (C)
63	If RFC 4301 is supported, then the product shall support IKEv1 as defined in RFC 2409. NOTE: The IKEv1 requirements are found in Section 4, Information Assurance.	5.2.1.9 IP6-000810	L	EI (soft) (R) EI (C) CP Server (C) CP SBC (C)
64	To prevent a Denial of Services (DoS) attack on the initiator of an IKE_SA, the initiator shall accept multiple responses to its first message, treat each as potentially legitimate, respond to it, and then discard all the invalid half-open connections when it receives a valid cryptographically protected response to any one of its requests. Once a cryptographically valid response is received, all subsequent responses shall be ignored whether or not they are cryptographically valid.	5.2.1.9 IP6-000820	L	EI (C) CP Server (C) CP SBC (C)
65	If RFC 4301 is supported, then the product shall support extensions to the Internet IP Security Domain of Interpretation for the Internet Security Association and Key Management Protocol (ISAKMP) as defined in RFC 2407.	5.2.1.9 IP6-000830	L	EI (soft) (R) EI (C) CP Server (C) CP SBC (C)
66	If RFC 4301 is supported, then the product shall support the ISAKMP as defined in RFC 2408.	5.2.1.9 IP6-000840	L	EI (soft) (R) EI (C) CP Server (C) CP SBC (C)

Table 3-5. Collaboration Tool Capability/Functional Requirements (continued)

CR/FR ID	Requirement	UCR Ref (UCR 2013)	LoC/ TP ID	CP R/O/C
5-1	**5.2.1 - Product**			
67	If the product supports the IPSec Authentication Header Mode, then the product shall support the IP Authentication Header (AH) as defined in RFC 4302.	5.2.1.9 IP6-000850	L	EI (soft) (R) EI (C) CP Server (C) CP SBC (C)
68	If RFC 4301 is supported, then the product shall support manual keying of IPSec.	5.2.1.9 IP6-000860	L	EI (soft) (R) EI (C) CP Server (C) CP SBC (C)
69	If RFC 4301 is supported, then the product shall support the ESP and AH cryptographic algorithm implementation requirements as defined RFC 4835.	5.2.1.9 IP6-000870	L	EI (soft) (R) EI (C) CP Server (C) CP SBC (C)
70	If RFC 4301 is supported, then the product shall support the IKEv1 security algorithms as defined in RFC 4109.	5.2.1.9 IP6-000880	L	EI (soft) (R) EI (C) CP Server (C) CP SBC (C)
71	If the product uses Uniform Resource Identifiers (URIs) in combination with IPv6, then the product shall use the URI syntax described in RFC 3986.	5.2.1.10 IP6-000990	L	EI (soft) (R) EI (C) CP Server (C) CP SBC (C)
72	If the product uses the Domain Name Service (DNS) resolver for IPv6 based queries, then the product shall conform to RFC 3596 for DNS queries.	5.2.1.10 IP6-001000	L	EI (C) CP Server (C)
73	For traffic engineering purposes, the bandwidth required per voice subscriber is calculated to be 110.0 kbps (each direction) for each IPv6 call. This is based on G.711 (20 ms codec) with IP overhead (100 kbps) resulting in a 250-byte bearer packet plus 10 kbps for signaling, Ethernet Interframe Gap, and the Secure Real-Time Transport Control Protocol (SRTCP) overhead. Based on overhead bits included in the bandwidth calculations, vendor implementations may use different calculations and hence arrive at slightly different numbers.	5.2.1.11 IP6-001010	L	CP Server (R) CP SBC (R)
74	The product shall forward packets using the same IP version as the version in the received packet. NOTE: If the packet was received as an IPv6 packet, then the appliance will forward it as an IPv6 packet. If the packet was received as an IPv4 packet, then the appliance will forward the packet as an IPv4 packet. This requirement is primarily associated with the signaling packets to ensure that translation does not occur.	5.2.1.12 IP6-001040	L	CP Server (R) CP SBC (R)
75	When the product is establishing media streams from dual-stacked appliances for AS-SIP signaled sessions, the product shall use the Alternative Network Address Type (ANAT) semantics for the Session Description Protocol (SDP) in accordance with RFC 4091. Also, the following conditional requirements would apply. NOTE 1: Guidance on clarification on the use of ANAT for related media is located in the AS-SIP 2013, Section 5.2.5, Clarification on the Use of ANAT for Related Media Streams. NOTE 2: Guidance on SIP syntax and encoding rules for IPv6 Augmented Backus-Naur Form (ABNF) per RFC 5954 is located in AS-SIP 2013, Section 4.1.3, Basic Requirements for AS-SIP Signaling Appliances and AS-SIP EI. IP6-001050.a [Required: EI, NA/SS] The product shall prefer any IPv4 address to any IPv6 address when using ANAT semantics. NOTE: This requirement will result in all AS-SIP sessions being established using IPv4. IP6-001050.b [Required: EI, NA/SS] The product shall place the option tag "SDPANAT" in a Required header field when using ANAT semantics in accordance with RFC 4092. IP6-001050.c [Required: EI] The products shall include the IPv4 and IPv6 addresses within the SDP of the SIP INVITE message when the INVITE contains the SDP.	5.2.1.12 IP6-001050	L	EI (R) CP Server (R)

Table 3-5. Collaboration Tool Capability/Functional Requirements (continued)

CR/FR ID	Requirement	UCR Ref (UCR 2013)	LoC/ TP ID	CP R/O/C
5-1	**5.2.1 - Product**			
76	If the product is using AS-SIP, and the <addrtype> is IPv6, and the <connection-address> is a unicast address, then the product shall support generation and processing of unicast IPv6 addresses having the following formats: x:x:x:x:x:x:x:x (where x is the hexadecimal values of the eight 16-bit pieces of the address). Example: 1080:0:0:0:8:800:200C:417A. x:x:x:x:x:x:d.d.d.d (where x is the hexadecimal values of the six high-order 16-bit pieces of the address, and d is the decimal values of the four low-order 8-bit pieces of the address (standard IPv4 representation). For example, 1080:0:0:0:8:800:116.23.135.22.	5.2.1.13 IP6-001060	L	EI (C) CP Server (C) CP SBC (C)
77	If the product is using AS-SIP, then the product shall support the generation and processing of IPv6 unicast addresses using compressed zeros consistent with one of the following formats: x:x:x:x:x:x:x:x format: 1080:0:0:0:8:800:200C:417A. x:x:x:x:x:x:d.d.d.d format: 1080:0:0:0:8:800:116.23.135.22. compressed zeros: 1080::8:800:200C:417A.	5.2.1.12 IP6-001070	L	EI (C) CP Server (C) CP SBC (C)
78	If the product is using AS-SIP, and the <addrtype> is IPv6, and the <connection-address> is a multicast group address (i.e., the two most significant hexadecimal digits are FF), then the product shall support the generation and processing of multicast IPv6 addresses having the same formats as the unicast IPv6 addresses.	5.2.1.12 IP6-001080	L	EI (C) CP Server (C) CP SBC (C)
79	If the product is using AS-SIP, and the <addrtype> is IPv6, then the product shall support the use of RFC 4566 for IPv6 in SDP as described in AS-SIP 2013, Section 4, SIP Requirements for AS-SIP Signaling Appliances and AS-SIP EIs.	5.2.1.12 IP6-001090	L	EI (C) CP Server (C) CP SBC (C)
80	If the product is using AS-SIP, and the <addrtype> is IPv6, and the <connection-address> is an IPv6 multicast group address, then the multicast connection address shall not have a Time To Live (TTL) value appended to the address as IPv6 multicast does not use TTL scoping.	5.2.1.12 IP6-001100	L	EI (C) CP Server (C) CP SBC (C)
81	If the product is using AS-SIP, then the product shall support the processing of IPv6 multicast group addresses having the <number of address> field and may support generating the <number of address> field. This field has the identical format and operation as the IPv4 multicast group addresses.	5.2.1.12 IP6-001110	L	EI (C) CP Server (C) CP SBC (C)
82	The product shall be able to provide topology hiding [e.g., Network Address Translation (NAT)] for IPv6 packets as described in Section 4, Information Assurance. NOTE: Deployments requiring the network topology hiding that IPv4 NAT provided as a side-effect should consider RFC 4864 – Local Network Protection (LNP) for IPv6.	5.2.1.12 IP6-001120	L	CP SBC (R)
83	The product shall support default address selection for IPv6 as defined in RFC 3484 (except for Section 2.1). NOTE: It is assumed that an IPv6 appliance will have as a minimum an IPv6 link local and an IPv4 address, and will have at least two addresses.	5.2.1.12 IP6-001130	L	EI (soft) (R)
84	If the product supports Remote Authentication Dial-in User Service (RADIUS) authentication, then the product shall support RADIUS as defined in RFC 3162. [Conditional: LS] If the LS supports a routing function and supports RADIUS authentication, then the product shall support RADIUS as defined in RFC 3162. NOTE 1: RFC 3162 defines only the additional attributes of RADIUS that are unique to IPv6 implementations. For the base RADIUS requirements, other RFCs are required, such as RFC 2865. NOTE 2: Because RFC 3162 cites the Network Access Server (NAS) functions would be on the Access Point (router), this function should be a feature of the router.	5.2.1.12 IP6-001140	L	CP SBC (R)
85	The products shall support Differentiated Services as described in RFC 2474 for a voice and video stream in accordance with Section 2, Session Control Products, and Section 6, Network Infrastructure End-to-End Performance, plain text DSCP plan.	5.2.1.14 IP6-001150	L	EI (R) CP Server (R) CP SBC (R)
86	If the product acts as an IPv6 tunnel broker, then the product shall support the function as defined in RFC 3053.	5.2.1.14 IP6-001160	L	CP Server (C)

Table 3-5. Collaboration Tool Capability/Functional Requirements (continued)

CR/FR ID	Requirement	UCR Ref (UCR 2013)	LoC/ TP ID	CP R/O/C
5-2	**5.2.2 - Mapping of RFCs to UC Profile Categories**			
1	EIs shall meet IPv6 RFCs in Table 5.2-3	5.2.2	L	EI (R)
2	CP shall meet IPv6 RFCs in Table 5.2-4	5.2.2	L	CP (R)
3	CP SBC shall meet the RFCs in Table 5.2-7	5.2.2	L	CP SBC (R)

LEGEND:

AS-SIP	Assured Services Session Initiation Protocol	O	Optional
C	Conditional	PRI	Primary Rate Interface
COM	commercial	PSAP	Public Service Access Point
CP	Collaboration Product	PSTN	Public Switched Telephone Network
DSCP	Differentiated Services Code Points	R	Required
DSN	Defense Switched Network	Ref	Reference
EI	End Instrument	RFC	Request For Comment
EO	End Office	SASL	Simple Authentication and Security Layer
ESB	emergency Services Bridge	SBC	Session Border Controller
ETSI	European Telecommunications Standards Institute	SC	Session Controller
GR	General Requirement	SNMP	Simple Network Management Protocol
IAW	In accordance with	SRTP	Secure Real Time Protocol
ID	Identification	STARTTLS	Extension to plain text protocols
IM	Instant Messaging	STIG	Security Technical Implementation Guide
IO	Interoperability	T	Test (verified via test procedure)
IP	Internet Protocol	TLS	Transport Layer Security
ISDN	Integrated Services Digital Network	TP	Test Procedure
L	Letter (verified via LoC)	UC	Unified Capabilities
LoC	Letter of Compliance	UCR	Unified Capabilities Requirements
MG	Media Gateway	VoIP	Voice over Internet Protocol
NA/SS	Network Appliance /Simple Server	XEP	XMPP Extension Protocols
NRT	Near Real time	XMPP	Extensible Messaging and Presence Protocol
QoS	Quality of Service		

Joint Interoperability Certification Errata Revision History

Errata Version	Date	Approved By	Comments
1.0	9 September 2013	Joseph Schulte	This is the original Joint Interoperability Certification.
1.1	26 September 2014		The following changes were made to clarify the SUT is certified with either the Acme Packet Net-Net 4500 or 3820 with any release S-CX6.3.0.MR-5 GA (Build 573) or later that is on the UC APL. • Memo, Table 4, note 2 and Enclosure 3, Table 3-3, note 1 was added with the following text: The SUT was tested with the Acme Packet Net-Net 4500 SD. However, the 3820 utilizes the same software and similar hardware and JITC analysis determined it to be functionally identical for interoperability certification purposes and the 3820 is also covered under this certification for use with the SUT. In addition, the SUT is certified with any 4500 or 3820 with this release or later that is on the UC APL. • Enclosure 2, paragraph 2, third subparagraph was updated to include the following text: The SUT was tested with the Acme Packet Net-Net 4500 SD with release S-CX6.3.0.MR-5 GA (Build 573). However, the 3820 utilizes the same software and similar hardware and JITC analysis determined it to be functionally identical for interoperability certification purposes and the 3820 is also covered under this certification for use with the SUT. In addition, the SUT is certified with any 4500 or 3820 with this release or later that is on the UC Approved Products List (APL).

LEGEND:

APL	Approved Products List	SUT	System Under Test
JITC	Joint Interoperability Test Command	UC	Unified Capabilities