



DEFENSE INFORMATION SYSTEMS AGENCY

P. O. BOX 549
FORT MEADE, MARYLAND 20755-0549

IN REPLY
REFER TO: Joint Interoperability Test Command (JITE)

17 Jan 13

MEMORANDUM FOR DISTRIBUTION

SUBJECT: Joint Interoperability Certification of the Acme Packet Net-Net 3820 Session Border Controller (SBC) and Net-Net 4500 SBC, Release S-CX6.3.0 MR-2 Patch 2 (Build 403)

References: (a) DoD Directive 4630.05, "Interoperability and Supportability of Information Technology (IT) and National Security Systems (NSS)," 5 May 2004
(b) Department of Defense Instruction 8100.04, "DoD Unified Capabilities (UC)," 9 December 2010
(c) through (f), see Enclosure 1

1. References (a) and (b) establish Defense Information Systems Agency (DISA) Joint Interoperability Test Command (JITC), as the responsible organization for interoperability test certification.
2. The Acme Packet Net-Net 3820 SBC and Net-Net 4500 SBC with Release S-CX6.3.0 MR-2 Patch 2 (Build 403) are hereinafter referred to as the System Under Test (SUT). The SUT meets all the critical interoperability requirements as a High-Availability Edge Boundary Controller (EBC) with No Loss of Active Sessions (NLAS) in a dual-chassis configuration. The SUT also meets the High Availability EBC requirements without NLAS, and Medium Availability EBC requirements in a dual chassis configuration. The Low Availability EBC requirements are met by the SUT in a single chassis configuration. The SUT is certified for joint use within the Defense Information Systems Network (DISN) in both classified and sensitive-but-unclassified (SBU) networks. 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 Plan of Action and Milestones (POA&M), which will address all new critical Test Discrepancy Reports (TDRs) within 120 days of identification. Testing was conducted using EBC requirements derived from the Unified Capabilities Requirements (UCR), Reference (c), and EBC test procedures, Reference (d). No other configurations, features, or functions, except those cited within this memorandum, are certified by JITC. This certification expires upon changes that could affect interoperability, but no later than three years from this memorandum.
3. This finding is based on interoperability testing conducted by JITC, review of the vendor's Letters of Compliance (LoC), DISA adjudication of open TDRs, Department of Defense (DoD) Chief Information Officer (CIO) limited waiver (May 2013) of Internet Protocol version 6 (IPv6) requirements, and DISA Information Assurance (IA) Certification Authority (CA) approval of the IA configuration. Interoperability testing was conducted by JITC, Fort Huachuca, Arizona, from 5 through 16 December 2011 and from 29 October through 9 November 2012. Review of

the vendor’s LoC was completed on 12 December 2011. DISA adjudication of outstanding TDRs was completed on 26 November 2012. The DoD CIO issued a waiver of IPv6 requirements until May 2013. If the vendor does not fully comply with IPv6 requirements by the end of May 2013, then the SUT will be subject to removal from the Unified Capabilities (UC) Approved Products List (APL). The DISA CA provided a positive Recommendation on 30 November 2012 based on the security testing completed by DISA-led IA test teams and published in separate reports, References (e) and (f). The acquiring agency or site will be responsible for the DoD Information Assurance Certification and Accreditation Process (DIACAP) accreditation. Enclosure 2 documents the test results and describes the tested network and system configurations including specified patch releases.

4. The interface, Capability Requirements (CR) and Functional Requirements (FR), and component status of the SUT is listed in Tables 1 and 2. The threshold Capability/Functional requirements for EBCs are established by Section 5.3.2.14 of Reference (c) and were used to evaluate the interoperability of the SUT. Enclosure 3 provides a detailed list of the interface, capability, and functional requirements.

Table 1. SUT Interface Interoperability Status

Interface	Critical ¹	UCR Paragraph	Threshold CR/FR Requirements ²	Status	Remarks ³
LAN/WAN Interfaces					
10Base-X	No	5.3.2.4 / 5.3.3.10.1.2	1-3, 5	Certified	IEEE 802.3i and 802.3j
100Base-X	No	5.3.2.4 / 5.3.3.10.1.2	1-3, 5	Certified	IEEE 802.3u
1000Base-X	No	5.3.2.4 / 5.3.3.10.1.2	1-3, 5	Certified	IEEE 802.3z
NM Interfaces					
10Base-X	No	5.3.2.4.4	4, 5	Certified	IEEE 802.3i and 802.3j
100Base-X	No	5.3.2.4.4	4, 5	Certified	IEEE 802.3u
NOTES:					
1. The UCR does not define the provision of any specific interface. The SUT must minimally provide one of the WAN interfaces and one of the NM interfaces.					
2. The SUT’s high-level capability and functional requirement ID numbers depicted in the 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.					
3. The SUT must meet IEEE 802.3 standards for interface provided.					
LEGEND:					
10Base-X	Generic designation for 10 Mbps Ethernet	FR	Functional Requirement		
100Base-X	Generic designation for 100 Mbps Ethernet	ID	Identification		
1000Base-X	Generic designation for 1000 Mbps Ethernet	IEEE	Institute of Electrical and Electronics Engineers		
802.3i	IEEE Ethernet standard for 10 Mbps over twisted pair	LAN	Local Area Network		
802.3j	IEEE Ethernet standard for 10 Mbps over fiber	Mbps	Megabits per second		
802.3u	IEEE Ethernet Standard for 100 Mbps over twisted pair and fiber	NM	Network Management		
802.3z	IEEE Ethernet standard for 1000 Mbps over fiber	SUT	System Under Test		
CR	Capability Requirement	UCR	Unified Capabilities Requirements		
		WAN	Wide Area Network		

Table 2. SUT Capability Requirements and Functional Requirements Status

CR/FR ID	Capability/Function	Applicability ¹	UCR Paragraph	Status
1	Edge Boundary Controller Requirements			
	AS-SIP Back-to-Back User Agent	Required	5.3.2.15.1	Met
	Call Processing Load	Required	5.3.2.15.2	Met
	Network Management	Required	5.3.2.15.3 5.3.2.17	Met
	DSCP Policing	Required	5.3.2.15.4	Partially Met ²
	Codec Bandwidth Policing	Required	5.3.2.15.5	Met
	Availability	Required	5.3.2.15.6	Met ³
	IEEE 802.1Q Support	Required	5.3.2.15.7	Met
	Packet Transit Time	Required	5.3.2.15.8	Met ⁴
	ITU-T H.323 Support	Conditional	5.3.2.15.9	Not Tested
Tactical EBC Requirements	Conditional	5.3.2.15.11	Met	
2	AS-SIP Requirements			
	Requirements for AS-SIP Signaling Appliances	Required	5.3.4.7	Met
3	IPv6 Requirements			
	Product Requirements	Required	5.3.5.4	Not Met ⁵
4	NM Requirements			
	VVoIP NMS Interface Requirements	Required	5.3.2.4.4	Met
	General Management Requirements	Required	5.3.2.17.2	Met
	Requirement for FCAPS Management	Required	5.3.2.17.3	Met
	NM requirements of Appliance Functions	Required	5.3.2.18	Met ⁶
5	IA Requirements			
	IA Requirements	Required	5.4	Met ⁷

NOTES:

- The notation of 'required' refers to the high-level requirement category. These high-level CR/FR requirements refer to a detailed list of requirements provided in Enclosure 3.
- The SUT does not properly support DSCP Policing. DISA adjudicated this as minor and has changed this to optional in the next version of the UCR (UCR 2013).
- The SUT met this requirement for the High Availability with No Loss of Active Sessions in a dual chassis configuration. This was verified through the vendor's LoC and testing.
- This requirement was not directly tested at the JITC because of testing limitations. However, JITC analysis determined that the SUT did not have any latency issues during the operation of the EBC attributable to packet transit time and therefore determined that the SUT met the overall requirement.
- The SUT does not fully support IPv6 in accordance with the UCR 2008, Change 3 requirements. The Department of Defense (DoD) Chief Information Officer (CIO) issued a waiver of IPv6 requirements until May 2013. If IPv6 is not fully supported by the end of May 2013, then the SUT will be subject to removal from the UC APL.
- The CM and PM data is not available via SNMPv3; however FM data is. DISA adjudicated this minor and has changed SNMPv3 to optional for CM and PM in the next version of the UCR (UCR 2013).
- Security is tested by DISA-led Information Assurance test teams and the results published in separate reports, References (e) and (f).

Table 2. SUT Capability Requirements and Functional Requirements Status (continued)

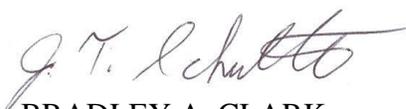
LEGEND:		
802.1Q	Standards for Local and Metropolitan Area Networks: Virtual Bridged Local Area Networks	ID Identification
APL	Approved Products List	IEEE Institute of Electrical and Electronics Engineers
AS-SIP	Assured Services Session Initiation Protocol	IPv6 Internet Protocol version 6
CM	Configuration Management	ITU-T International Telecommunication Union - Telecommunication Standardization Sector
CR	Capability Requirement	JITC Joint Interoperability Test Command
DISA	Defense Information Systems Agency	LoC Letters of Compliance
DSCP	Differentiated Services Code Point	NM Network Management
EBC	Edge Boundary Controller	OSD Office of the Secretary of Defense
FCAPS	Fault, Configuration, Accounting, Performance, and Security	PM Performance Management
FM	Fault Management	SNMPv3 Simple Network Management Protocol version 3
FR	Functional Requirement	SUT System Under Test
H.323	Standard for multi-media communications on packet-based networks	UC Unified Capabilities
IA	Information Assurance	UCR Unified Capabilities Requirements
		VVoIP Voice and Video over Internet Protocol

5. No detailed test report was developed in accordance with the Program Manager’s request. JITC distributes interoperability information via the JITC Electronic Report Distribution (ERD) system, which uses Unclassified-But-Sensitive Internet Protocol Router Network (NIPRNet) e-mail. More comprehensive interoperability status information is available via the JITC System Tracking Program (STP). STP is accessible by .mil/gov users on the NIPRNet 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 <http://jit.fhu.disa.mil> (NIPRNet). Information related to DSN testing is on the Telecom Switched Services Interoperability (TSSI) website at <http://jitc.fhu.disa.mil/tssi>. 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 through government civilian or uniformed military personnel from the Unified Capabilities Certification Office (UCCO), e-mail: disa.meade.ns.list.unified-capabilities-certification-office@mail.mil. All associated data is available on the DISA UCCO website located at <http://www.disa.mil/ucco/>.

6. The JITC point of contact is Mr. Edward Mellon, DSN 879-5159, commercial (520) 538-5159, FAX DSN 879-4347, or e-mail to edward.a.mellon.civ@mail.mil. JITC’s mailing address is P.O. Box 12798, Fort Huachuca, AZ 85670-2798. The UCCO tracking number for the Net-Net 3820 SBC is 1125902. The UCCO tracking number for the Net-Net 4500 SBC is 1127302.

FOR THE COMMANDER:

3 Enclosures a/s


for BRADLEY A. CLARK
Acting Chief
Battlespace Communications Portfolio

JITC Memo, JTE, Joint Interoperability Certification of the Acme Packet Net-Net 3820 Session Border Controller (SBC) and Net-Net 4500 SBC, Release S-CX6.3.0 MR-2 Patch 2 (Build 403)

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 2008, Change 3," 22 January 2010
- (d) Joint Interoperability Test Command, "Unified Capabilities Test Plan (UCTP)," October 2009
- (e) Joint Interoperability Test Command, "Information Assurance (IA) Assessment of ACME Packet, Inc. 3820 Release (Rel.) S-CX6.3.0m2p2 (Tracking Number 1125902)," Draft
- (f) Joint Interoperability Test Command, "Information Assurance (IA) Assessment of ACME Packet, Inc. Net-Net 4500 Rel. S-CX6.3.0m2p2 (Tracking Number 1127302)," Draft

CERTIFICATION TESTING SUMMARY

1. SYSTEM TITLE. The Acme Packet Net-Net 3820 Session Border Controller (SBC) and Net-Net 4500 SBC, Release S-CX6.3.0 MR-2 Patch 2 (Build 403); hereinafter referred to as the System Under Test (SUT).

2. SPONSOR. Defense Information Systems Agency (DISA), Mr. Lou Schmuckler, Post Office Box 549, Fort Meade, Maryland 20755-0549, e-mail: louis.a.schmuckler.civ@mail.mil.

3. SYSTEM POC. Acme Packet, Mr. James Kevin, 100 Crosby Drive, Bedford, Massachusetts 01730, e-mail: kjames@acmepacket.com

4. TESTER. Joint Interoperability Test Command (JITC), Fort Huachuca, Arizona.

5. SYSTEM DESCRIPTION. The SUT is an Edge Boundary Controller (EBC), which performs voice firewall and back-to-back user agent functions. The EBC consists of the voice or video firewall/border controller. The Call Connection Agent (CCA) in the Softswitch (SS) and Local Session controller (LSC) needs to interact with Assured Services Session Initiation Protocol (AS-SIP) functions in the EBC which:

- Mediates AS-SIP signaling between an LSC and an Multifunction Softswitch (MFSS) or Wide Area Network (WAN) SS, and between two MFSSs or SSs.
- Supports Session Border Controller functions, such as Network Address Translation (NAT) and Network Address and Port Translation (NAPT).
- Supports Internet Protocol (IP) firewall functions.

Acme Packet EBC for AS-SIP applications are SBC platforms designed to provide voice-aware firewall and back-to-back user agent functionality in accordance with the Unified Capabilities Requirements (UCR). Acme Packet EBCs support the deployment and delivery of a broad range of interactive real time communications services and applications ranging from basic Voice over Internet Protocol (VoIP) to unified communications in a fully secure manner. The EBCs secure the AS-SIP and International Telecommunication Union - Telecommunication Standardization Sector (ITU-T) H.323 trunking border to internal and external networks. The AS-SIP, ITU-T H.323, and Internet Protocol version 4 (IPv4) interworking capabilities of the Acme Packet EBCs ensure interoperability with and between legacy IP Private Branch Exchange (PBX) equipment and next-generation unified communications platforms. The EBCs control session admission, IP PBX or Unified Capabilities (UC) server loads and overloads, IP network transport and Session Initiation Protocol (SIP)/ITU-T H.323 session routing. Per the vendor's documentation the SUT's maximum threshold for simultaneous IP to IP calls with Transport Layer Security (TLS) are depicted in Table 2-1 as follows:

Table 2-1. SUT Maximum Simultaneous Sessions with TLS

System	Memory	Maximum Simultaneous Sessions with TLS
Net-Net 3820	1GB	28,000
	2GB	45,000
Net-Net 4500	4GB	60,000

LEGEND:
 GB Gigabyte
 SUT System Under Test
 TLS Transport Layer Security

6. OPERATIONAL ARCHITECTURE. Figure 2-1 depicts a notional operational architecture that the SUT may be used in.

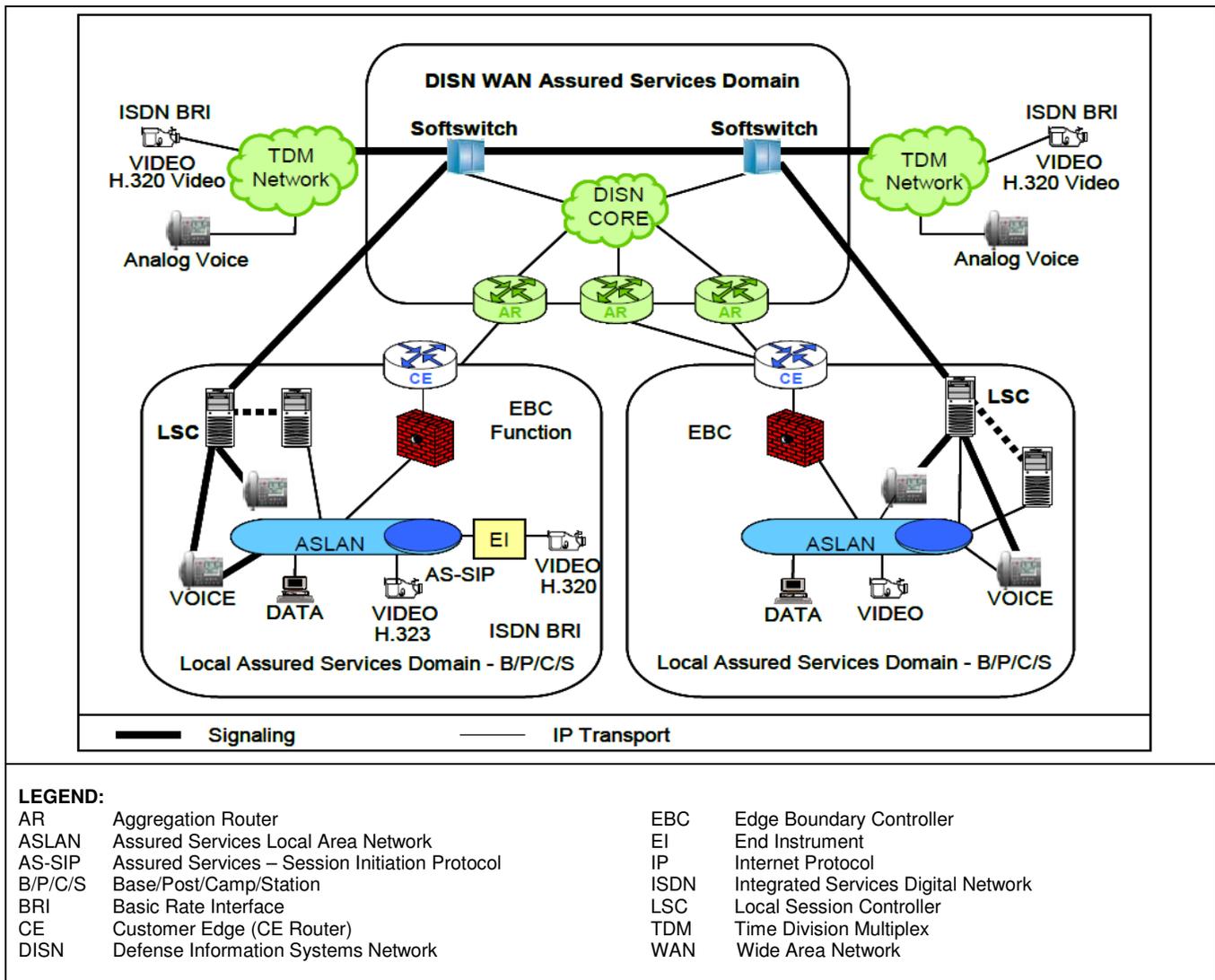


Figure 2-1. Edge Boundary Controller Architecture

7. INTEROPERABILITY REQUIREMENTS. The interface, Capability Requirements (CR), Functional Requirements (FR), Information Assurance (IA), and other requirements for EBCs are established by Reference (c).

7.1 Interfaces. The SUT uses external interfaces to connect to the Global Information Grid (GIG) network. Table 2-2 shows the physical interfaces supported by the SUT. The table documents the physical interfaces and the associated standards.

Table 2-2. Edge Boundary Controller Interface Requirements

Interface	Critical ¹	UCR Reference ²	Criteria ³								
LAN/WAN Interfaces											
10Base-X	No	5.3.2.4 / 5.3.3.10.1.2	Meet IEEE 802.3 standards for 802.3i and 802.3j and meet threshold CR/FR 1-3, 5 requirements.								
100Base-X	No	5.3.2.4 / 5.3.3.10.1.2	Meet IEEE 802.3 standards for 802.3u and meet threshold CR/FR 1-3, 5 requirements.								
1000Base-X	No	5.3.2.4 / 5.3.3.10.1.2	Meet IEEE 802.3 standards for 802.3z and meet threshold CR/FR 1-3, 5 requirements.								
NM Interfaces											
10Base-X	No	5.3.2.4.4	Meet IEEE 802.3 standards for 802.3i and 802.3j and meet threshold CR/FR 4 and 5 requirements.								
100Base-X	No	5.3.2.4.4	Meet IEEE 802.3 standards for 802.3u and meet threshold CR/FR 4 and 5 requirements.								
<p>NOTES:</p> <p>1. The UCR does not define the provision of any specific interface. The SUT must minimally provide one of the WAN interfaces and one of the NM interfaces.</p> <p>2. The SUT's high-level capability and functional requirement ID numbers depicted in the CRs/FRs column can be cross-referenced in Table 2-3. These high-level CR/FR requirements refer to a detailed list of requirements provided in Enclosure 3.</p> <p>3. The SUT must meet IEEE 802.3 standards for interface provided.</p> <p>LEGEND:</p> <table style="width: 100%; border: none;"> <tr> <td style="width: 50%;">CR Capability Requirement</td> <td style="width: 50%;">NM Network Management</td> </tr> <tr> <td>FR Functional Requirement</td> <td>SUT System Under Test</td> </tr> <tr> <td>ID Identification</td> <td>UCR Unified Capabilities Requirements</td> </tr> <tr> <td>IEEE Institute of Electrical and Electronics Engineers</td> <td>WAN Wide Area Network</td> </tr> </table>				CR Capability Requirement	NM Network Management	FR Functional Requirement	SUT System Under Test	ID Identification	UCR Unified Capabilities Requirements	IEEE Institute of Electrical and Electronics Engineers	WAN Wide Area Network
CR Capability Requirement	NM Network Management										
FR Functional Requirement	SUT System Under Test										
ID Identification	UCR Unified Capabilities Requirements										
IEEE Institute of Electrical and Electronics Engineers	WAN Wide Area Network										

7.2 Capability Requirements (CR) and Functional Requirements (FR). EBCs have required and conditional features and capabilities that are established by the UCR. The SUT does not need to provide non-critical (conditional) requirements. If they are provided, they must function according to the specified requirements. The SUTs features and capabilities and its aggregated requirements in accordance with (IAW) the EBC requirements are listed in Table 2-3. Detailed CR/FR requirements are provided in Enclosure 3.

Table 2-3 Edge Boundary Controller Requirements and Functional Requirements

CR/FR ID	Capability/ Function	Applicability (See note.)	UCR Paragraph																																								
1	Edge Boundary Controller Requirements																																										
	AS-SIP Back-to-Back User Agent	Required	5.3.2.15.1																																								
	Call Processing Load	Required	5.3.2.15.2																																								
	Network Management	Required	5.3.2.15.3 / 5.3.2.17																																								
	DSCP Policing	Required	5.3.2.15.4																																								
	Codec Bandwidth Policing	Required	5.3.2.15.5																																								
	Availability	Required	5.3.2.15.6																																								
	IEEE 802.1Q Support	Required	5.3.2.15.7																																								
	Packet Transit Time	Required	5.3.2.15.8																																								
	ITU-T H.323 Support	Conditional	5.3.2.15.9																																								
Tactical EBC Requirements	Conditional	5.3.2.15.11																																									
2	AS-SIP Requirements																																										
	Requirements for AS-SIP Signaling Appliances	Required	5.3.4.7																																								
3	IPv6 Requirements																																										
	Product Requirements	Required	5.3.5.4																																								
4	NM Requirements																																										
	VVoIP NMS Interface Requirements	Required	5.3.2.4.4																																								
	General Management Requirements	Required	5.3.2.17.2																																								
	Requirement for FCAPS Management	Required	5.3.2.17.3																																								
	NM requirements of Appliance Functions	Required	5.3.2.18																																								
5	IA Requirements																																										
	IA Requirements	Required	5.4																																								
<p>NOTE: The notation of 'required' refers to the high-level requirement category. These high-level CR/FR requirements refer to a detailed list of requirements provided in Enclosure 3.</p> <p>LEGEND:</p> <table border="0"> <tr> <td>802.1Q</td> <td>IEEE VLAN tagging standard</td> <td>IEEE</td> <td>Institute of Electrical and Electronics Engineers</td> </tr> <tr> <td>AS-SIP</td> <td>Assured Services Session Initiation Protocol</td> <td>IPv6</td> <td>Internet Protocol version 6</td> </tr> <tr> <td>CR</td> <td>Capabilities Requirement</td> <td>ITU-T</td> <td>International Telecommunication Union - Telecommunication Standardization Sector</td> </tr> <tr> <td>DSCP</td> <td>Differentiated Services Code Point</td> <td>NM</td> <td>Network Management</td> </tr> <tr> <td>EBC</td> <td>Edge Boundary Controller</td> <td>NMS</td> <td>NM System</td> </tr> <tr> <td>FCAPS</td> <td>Fault, Configuration, Accounting, Performance, and Security</td> <td>SIP</td> <td>Session Initiation Protocol</td> </tr> <tr> <td>FR</td> <td>Functional Requirement</td> <td>SUT</td> <td>System Under Test</td> </tr> <tr> <td>H.323</td> <td>ITU-T recommendation that defines audio-visual session protocols</td> <td>UCR</td> <td>Unified Capabilities Requirements</td> </tr> <tr> <td>IA</td> <td>Information Assurance</td> <td>VVoIP</td> <td>Voice and Video over Internet Protocol</td> </tr> <tr> <td>ID</td> <td>Identification</td> <td></td> <td></td> </tr> </table>				802.1Q	IEEE VLAN tagging standard	IEEE	Institute of Electrical and Electronics Engineers	AS-SIP	Assured Services Session Initiation Protocol	IPv6	Internet Protocol version 6	CR	Capabilities Requirement	ITU-T	International Telecommunication Union - Telecommunication Standardization Sector	DSCP	Differentiated Services Code Point	NM	Network Management	EBC	Edge Boundary Controller	NMS	NM System	FCAPS	Fault, Configuration, Accounting, Performance, and Security	SIP	Session Initiation Protocol	FR	Functional Requirement	SUT	System Under Test	H.323	ITU-T recommendation that defines audio-visual session protocols	UCR	Unified Capabilities Requirements	IA	Information Assurance	VVoIP	Voice and Video over Internet Protocol	ID	Identification		
802.1Q	IEEE VLAN tagging standard	IEEE	Institute of Electrical and Electronics Engineers																																								
AS-SIP	Assured Services Session Initiation Protocol	IPv6	Internet Protocol version 6																																								
CR	Capabilities Requirement	ITU-T	International Telecommunication Union - Telecommunication Standardization Sector																																								
DSCP	Differentiated Services Code Point	NM	Network Management																																								
EBC	Edge Boundary Controller	NMS	NM System																																								
FCAPS	Fault, Configuration, Accounting, Performance, and Security	SIP	Session Initiation Protocol																																								
FR	Functional Requirement	SUT	System Under Test																																								
H.323	ITU-T recommendation that defines audio-visual session protocols	UCR	Unified Capabilities Requirements																																								
IA	Information Assurance	VVoIP	Voice and Video over Internet Protocol																																								
ID	Identification																																										

7.3 Information Assurance. Table 2-4 details the IA requirements applicable to the EBC products.

Table 2-4. Edge Boundary Controller Information Assurance Requirements

Requirement	Applicability (See note.)	UCR Reference	Criteria
General Requirements	Required	5.4.6.2	Detailed requirements and associated criteria for an Edge Boundary Controller are listed in Reference (e).
Authentication	Required	5.4.6.2.1	
Integrity	Required	5.4.6.2.2	
Confidentiality	Required	5.4.6.2.3	
Non-Repudiation	Required	5.4.6.2.4	
Availability	Required	5.4.6.2.5	

NOTE: Annotation of 'required' refers to high level requirement category. Applicability of each sub-requirement is provided in Enclosure 3.

LEGEND:
UCR Unified Capabilities Requirements

7.4 Other. None.

8. TEST NETWORK DESCRIPTION. The SUT was tested at JITC, Fort Huachuca, Arizona in a manner and configuration similar to that of a notional operational environment. Testing the system's required functions and features was conducted using the test configurations depicted in Figures 2-2 and 2-3. Figure 2-2 depicts the minimum test architecture for testing EBCs. Figure 2-3 depicts the SUT's test configuration.

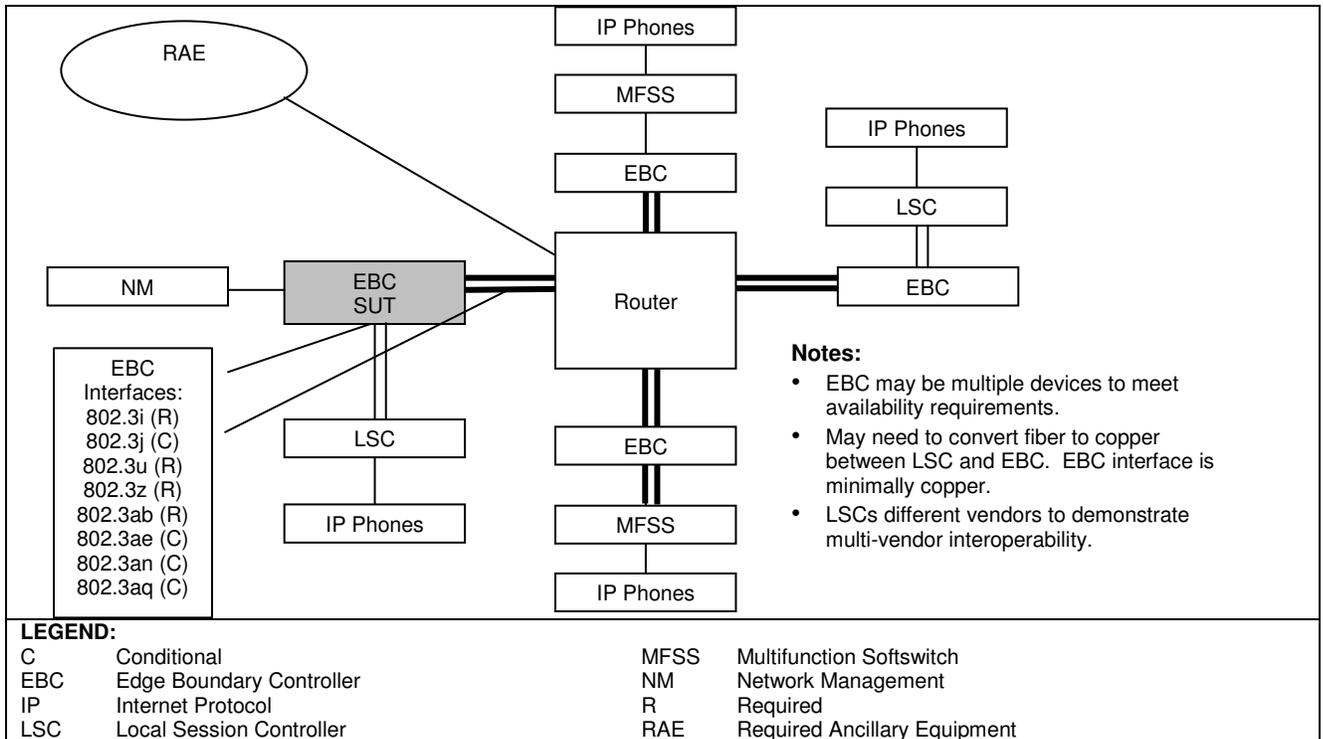


Figure 2-2. EBC Minimum Test Architecture

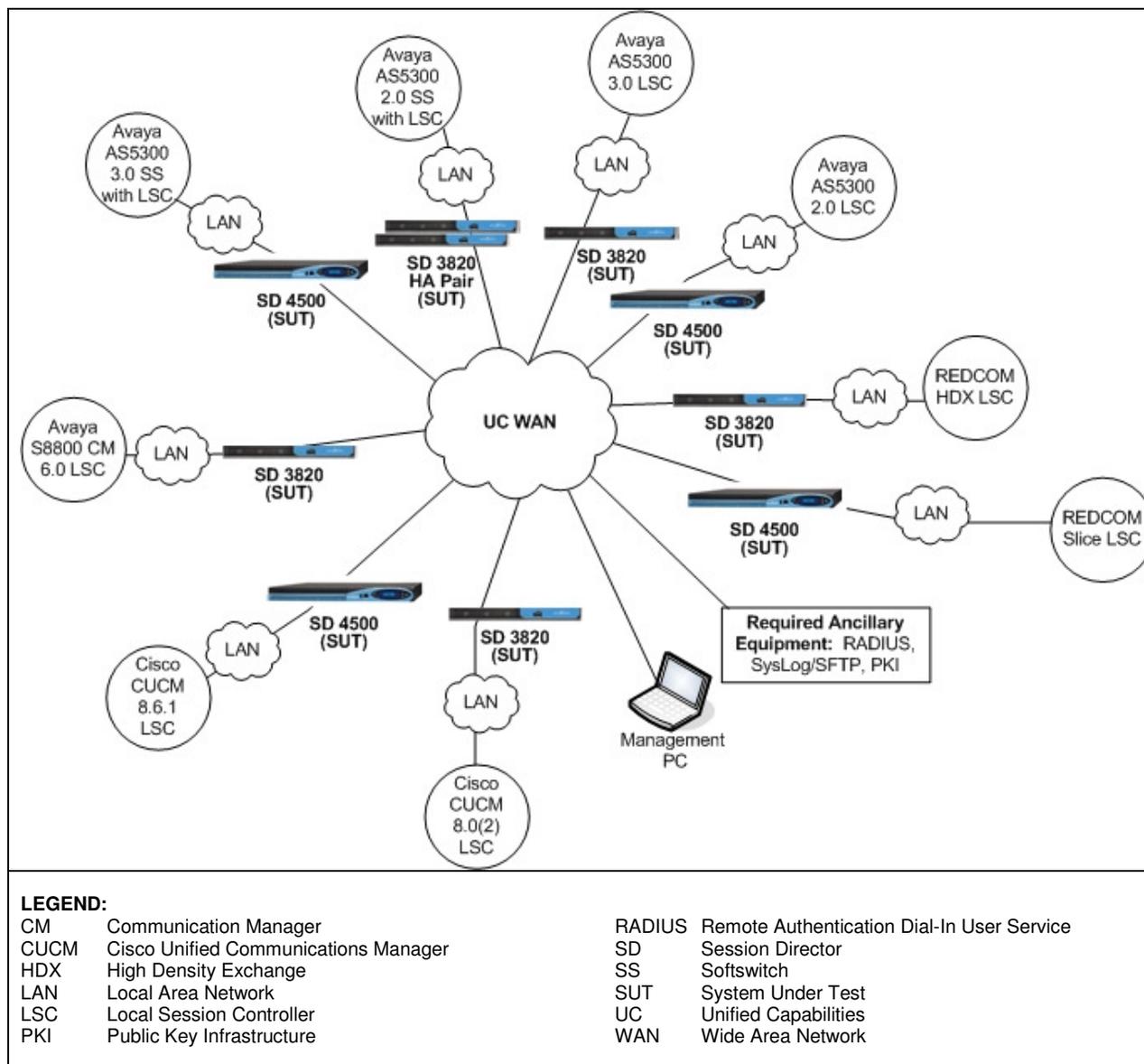


Figure 2-3. SUT Test Configuration

9. SYSTEM CONFIGURATIONS. Table 2-5 provides the system configurations and hardware and software components tested with the SUT. The SUT was tested in an operationally realistic environment to determine its interoperability capability with associated network devices and network traffic.

Table 2-5. Tested System Configurations

System Name		Release	
Avaya AS5300 LSC/SS		3.0	
Avaya AS5300 LSC		2.0	
Avaya S8800 LSC		Communication Manager 6.0	
Cisco CUCM LSC		8.6.1	
Cisco CUCM LSC		8.0(2)	
REDCOM HDX LSC		4.0 Revision 3 with Specified Patch Group 8 (4.0AR3P8)	
REDCOM Slice LSC		4.0 Revision 3 with Specified Patch Group 8 (4.0AR3P8)	
ACME Packet Net-Net SD 3820		6.2	
ACME Packet Net-Net SD 4500		6.2	
Other Required Equipment (Site-provided)			
Required Ancillary Equipment		Public Key Infrastructure (PKI)	
		Remote Access Dial-In User Service (RADIUS)	
		SysLog Server	
Management PC		Windows 7 Professional with Service Pack 1	
Hardware		Cards	Software/Firmware
ACME Packet Net-Net SBC 3820		NG17AN7SAB	VxWorks v6.4
			SCX6.3.0 MR-2 Patch 2 (Build 403)
ACME Packet Net-Net SBC 4500		NG17AM6SAA	SCX6.3.0 MR-2 Patch 2 (Build 403)
LEGEND:			
CUCM	Cisco Unified Communications Manager	PC	Personal Computer
HDX	High Density Exchange	SBC	Session Border Controller
LSC	Local Session Controller	SS	Softswitch

10. TESTING LIMITATIONS. The JITC test team noted the following testing limitations including the impact they may have on interpretation of the results and conclusions. Any untested requirements are also included in the testing limitations.

a. Packet Transit Time. JITC was unable to test this requirement because it would require special test equipment that could communicate with an EBC using appropriate protocols and security processes. JITC did not note any issues during the operation of the EBC attributable to packet transit time and therefore determined that the SUT met the overall requirement.

b. Network Management (NM). JITC did not test the SUT’s ability to meet UCR NM requirements. The vendor did submit a Letter of Compliance (LoC) that was reviewed by JITC. JITC’s evaluation of the SUT’s NM capabilities is provided in paragraph 11.

11. INTEROPERABILITY EVALUATION RESULTS. The SUT meets the critical interoperability requirements for an EBC in accordance with the UCR and is certified for joint use with other UC products listed on the Approved Products List (APL). Additional discussion regarding specific testing results is located in subsequent paragraphs.

11.1 Interfaces. The interface status of the SUT is provided in Table 2-6.

Table 2-6. SUT Interface Requirements Status

Interface	Critical ¹	UCR Paragraph	Threshold CR/FR Requirements ²	Status	Remarks ³																																				
LAN/WAN Interfaces																																									
10Base-X	No	5.3.2.4 / 5.3.3.10.1.2	1-3, 5	Certified	IEEE 802.3i and 802.3j																																				
100Base-X	No	5.3.2.4 / 5.3.3.10.1.2	1-3, 5	Certified	IEEE 802.3u																																				
1000Base-X	No	5.3.2.4 / 5.3.3.10.1.2	1-3, 5	Certified	IEEE 802.3z																																				
NM Interfaces																																									
10Base-X	No	5.3.2.4.4	4, 5	Certified	IEEE 802.3i and 802.3j																																				
100Base-X	No	5.3.2.4.4	4, 5	Certified	IEEE 802.3u																																				
<p>NOTES:</p> <p>1. The UCR does not define the provision of any specific interface. The SUT must minimally provide one of the WAN interfaces and one of the NM interfaces.</p> <p>2. The SUT's high-level capability and functional requirement ID numbers depicted in the 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.</p> <p>3. The SUT must meet IEEE 802.3 standards for interface provided.</p> <p>LEGEND:</p> <table style="width: 100%; border: none;"> <tr> <td style="width: 20%;">10Base-X</td> <td style="width: 30%;">Generic designation for 10 Mbps Ethernet</td> <td style="width: 20%;">FR</td> <td style="width: 30%;">Functional Requirement</td> </tr> <tr> <td>100Base-X</td> <td>Generic designation for 100 Mbps Ethernet</td> <td>ID</td> <td>Identification</td> </tr> <tr> <td>1000Base-X</td> <td>Generic designation for 1000 Mbps Ethernet</td> <td>IEEE</td> <td>Institute of Electrical and Electronics Engineers</td> </tr> <tr> <td>802.3i</td> <td>IEEE Ethernet standard for 10 Mbps over twisted pair</td> <td>LAN</td> <td>Local Area Network</td> </tr> <tr> <td>802.3j</td> <td>IEEE Ethernet standard for 10 Mbps over fiber</td> <td>Mbps</td> <td>Megabits per second</td> </tr> <tr> <td>802.3u</td> <td>IEEE Ethernet Standard for 100 Mbps over twisted pair and fiber</td> <td>NM</td> <td>Network Management</td> </tr> <tr> <td>802.3z</td> <td>IEEE Ethernet standard for 1000 Mbps over fiber</td> <td>SUT</td> <td>System Under Test</td> </tr> <tr> <td>CR</td> <td>Capability Requirement</td> <td>UCR</td> <td>Unified Capabilities Requirements</td> </tr> <tr> <td></td> <td></td> <td>WAN</td> <td>Wide Area Network</td> </tr> </table>						10Base-X	Generic designation for 10 Mbps Ethernet	FR	Functional Requirement	100Base-X	Generic designation for 100 Mbps Ethernet	ID	Identification	1000Base-X	Generic designation for 1000 Mbps Ethernet	IEEE	Institute of Electrical and Electronics Engineers	802.3i	IEEE Ethernet standard for 10 Mbps over twisted pair	LAN	Local Area Network	802.3j	IEEE Ethernet standard for 10 Mbps over fiber	Mbps	Megabits per second	802.3u	IEEE Ethernet Standard for 100 Mbps over twisted pair and fiber	NM	Network Management	802.3z	IEEE Ethernet standard for 1000 Mbps over fiber	SUT	System Under Test	CR	Capability Requirement	UCR	Unified Capabilities Requirements			WAN	Wide Area Network
10Base-X	Generic designation for 10 Mbps Ethernet	FR	Functional Requirement																																						
100Base-X	Generic designation for 100 Mbps Ethernet	ID	Identification																																						
1000Base-X	Generic designation for 1000 Mbps Ethernet	IEEE	Institute of Electrical and Electronics Engineers																																						
802.3i	IEEE Ethernet standard for 10 Mbps over twisted pair	LAN	Local Area Network																																						
802.3j	IEEE Ethernet standard for 10 Mbps over fiber	Mbps	Megabits per second																																						
802.3u	IEEE Ethernet Standard for 100 Mbps over twisted pair and fiber	NM	Network Management																																						
802.3z	IEEE Ethernet standard for 1000 Mbps over fiber	SUT	System Under Test																																						
CR	Capability Requirement	UCR	Unified Capabilities Requirements																																						
		WAN	Wide Area Network																																						

11.2 Capability Requirements (CR) and Functional Requirements (FR). The SUT CR and FR status is depicted in Table 2-6. Detailed CR/FR requirements are provided in Enclosure 3, Table 3-1.

Table 2-6. SUT Capability Requirements and Functional Requirements Status

CR/FR ID	Capability/Function	Applicability ¹	UCR Paragraph	Status
1	Edge Boundary Controller Requirements			
	AS-SIP Back-to-Back User Agent	Required	5.3.2.15.1	Met
	Call Processing Load	Required	5.3.2.15.2	Met
	Network Management	Required	5.3.2.15.3 5.3.2.17	Met
	DSCP Policing	Required	5.3.2.15.4	Partially Met ²
	Codec Bandwidth Policing	Required	5.3.2.15.5	Met
	Availability	Required	5.3.2.15.6	Met ³
	IEEE 802.1Q Support	Required	5.3.2.15.7	Met
	Packet Transit Time	Required	5.3.2.15.8	Met ⁴
	ITU-T H.323 Support	Conditional	5.3.2.15.9	Not Tested
Tactical EBC Requirements	Conditional	5.3.2.15.11	Met	

Table 2-6. SUT Capability Requirements and Functional Requirements Status (continued)

CR/FR ID	Capability/Function	Applicability ¹	UCR Paragraph	Status
2	AS-SIP Requirements			
	Requirements for AS-SIP Signaling Appliances	Required	5.3.4.7	Met
3	IPv6 Requirements			
	Product Requirements	Required	5.3.5.4	Not Met ⁵
4	NM Requirements			
	VVoIP NMS Interface Requirements	Required	5.3.2.4.4	Met
	General Management Requirements	Required	5.3.2.17.2	Met
	Requirement for FCAPS Management	Required	5.3.2.17.3	Met
	NM requirements of Appliance Functions	Required	5.3.2.18	Met ⁶
5	IA Requirements			
	IA Requirements	Required	5.4	Met ⁷

NOTES:

1. The notation of 'required' refers to the high-level requirement category. These high-level CR/FR requirements refer to a detailed list of requirements provided in Enclosure 3.
2. The SUT does not properly support DSCP Policing. DISA adjudicated this as minor and has changed this to optional in the next version of the UCR (UCR 2013).
3. The SUT met this requirement for the High Availability with No Loss of Active Sessions in a dual chassis configuration. This was verified through the vendor's LoC and testing.
4. This requirement was not directly tested at the JITC because of testing limitations. However, JITC analysis determined that the SUT did not have any latency issues during the operation of the EBC attributable to packet transit time and therefore determined that the SUT met the overall requirement.
5. The SUT does not fully support IPv6 in accordance with the UCR 2008, Change 3 requirements. The Department of Defense (DoD) Chief Information Officer (CIO) issued a waiver of IPv6 requirements until May 2013. If IPv6 is not fully supported by the end of May 2013, then the SUT will be subject to removal from the UC APL.
6. The CM and PM data is not available via SNMPv3; however FM data is. DISA adjudicated this minor and has changed SNMPv3 to optional for CM and PM in the next version of the UCR (UCR 2013).
7. Security is tested by DISA-led Information Assurance test teams and the results published in separate reports, References (e) and (f).

LEGEND:

802.1Q	Standards for Local and Metropolitan Area Networks: Virtual Bridged Local Area Networks	ID	Identification
APL	Approved Products List	IEEE	Institute of Electrical and Electronics Engineers
AS-SIP	Assured Services Session Initiation Protocol	IPv6	Internet Protocol version 6
CM	Configuration Management	ITU-T	International Telecommunication Union - Telecommunication Standardization Sector
CR	Capability Requirement	JITC	Joint Interoperability Test Command
DISA	Defense Information Systems Agency	LoC	Letters of Compliance
DSCP	Differentiated Services Code Point	NM	Network Management
EBC	Edge Boundary Controller	OSD	Office of the Secretary of Defense
FCAPS	Fault, Configuration, Accounting, Performance, and Security	PM	Performance Management
FM	Fault Management	SNMPv3	Simple Network Management Protocol version 3
FR	Functional Requirement	SUT	System Under Test
H.323	Standard for multi-media communications on packet-based networks	UC	Unified Capabilities
IA	Information Assurance	UCR	Unified Capabilities Requirements
		VVoIP	Voice and Video over Internet Protocol

a. Edge Boundary Controller Requirements

(1) AS-SIP Back-to-Back User Agent (B2BUA). The UCR 2008 Change 3, section 5.3.2.15.1, states the product shall act as an AS-SIP B2BUA for interpreting the

AS-SIP messages to meet its functions. The SUT met all requirements as an AS-SIP B2BUA. Requirements for fronting multiple MFSSs and SSs were met via an LoC.

(2) Call Processing Load. The UCR 2008 Change 3, section 5.3.2.15.2, states the product shall be capable of handling the aggregated WAN call processing load associated with its subtended LSCs and MFSSs. The SUT met all requirements for call processing load.

(3) Network Management. The UCR 2008 Change 3, section 5.3.2.15.3, states the product shall support Fault, Configuration, Accounting, Performance, and Security (FCAPS) NM functions as defined in Section 5.3.2.17, Management of Network Appliances, of UCR 2008. Network management requirements were met via a vendor-submitted LoC. The SUT met all critical network management requirements.

(4) Differentiated Services Code Point Policing. The UCR 2008 Change 3, section 5.3.2.15.4, states the EBC shall be capable of ensuring that media streams associated with a particular session use the appropriate Differentiated Services Code Point (DSCP) based on the information in the AS-SIP Resource Priority Header (RPH). This was tested at JITC; however, the vendor does support DSCP Policing but the EBC does not recognize the Resource-Priority Header. DISA adjudicated this as minor and has changed this to optional in the next version of the UCR (UCR 2013).

(5) Codec Bandwidth Policing. The UCR 2008 Change 3, section 5.3.2.15.5, states the EBC shall be capable of ensuring that the media streams associated with a particular session use the appropriate codec (bandwidth) based on the SDP information in the AS-SIP message. The SUT met all requirements for Codec Bandwidth Policing.

(6) Availability. There are four types of EBCs: High Availability with No Loss of Active Sessions (NLAS), High Availability without NLAS, Medium Availability without NLAS, and Low Availability. IAW Section 5.3.2.15.6 of UCR 2008 Change 3, the EBC shall meet availability requirements as specified for the availability type. These were met via a vendor-submitted LoC and through testing. The SUT met the Availability requirements for the High Availability with NLAS with a dual chassis configuration, and Low Availability with a single chassis configuration. Furthermore, if an SUT meets High Availability with NLAS it also meets High Availability without NLAS and Medium Availability without NLAS.

(7) IEEE 802.1Q Support. The UCR 2008 Change 3, section 5.3.2.15.7, states the product shall be capable of supporting the IEEE 802.1Q 2-byte Tag Control Information (TCI) Field 12-bit Virtual Local Area Network (VLAN) Identifier (VID). The SUT met all requirements for IEEE 802.1Q VLAN Support.

(8) Packet Transit Time. The UCR 2008 Change 3, section 5.3.2.15.8 of UCR 2008 Change 3, the product shall be capable of receiving, processing, and transmitting an UC packet within 2 ms to include executing all internal functions. JITC was unable to directly test this feature because no test equipment is available to test

this requirement. However, JITC analysis determined that the SUT did not have any latency issues during the operation of the EBC attributable to packet transit time and therefore determined that the SUT met the overall requirement.

(9) ITU-T H.323 Support. The UCR 2008 Change 3, section 5.3.2.15.9 states that if the EBC supports ITU-T H.323 video, then the product shall be capable of processing and forwarding ITU-T H.323 messages in accordance with Section 5.4, Information Assurance Requirements, of this document. This is a conditional requirement and was not tested at JITC.

(10) Tactical EBC Requirements. The UCR 2008 Change 3, section 5.3.2.15.11 states that the EBC shall support more than one LSC. The SUT met this requirement through testing.

b. Assured Services Session Initiation Protocol Requirements. Requirements for AS-SIP Signaling Appliances. The UCR 2008 Change 3, section 5.3.4.7, states the EBC must meet all requirements for AS-SIP Signaling Appliances. The SUT met all requirements for AS-SIP signaling appliances.

c. Internet Protocol version 6 (IPv6) Requirements. The UCR 2008 Change 3, section 5.3.5.4, states the EBC must meet specified IPv6 requirements. The SUT does not fully support IPv6 in accordance with the UCR 2008, Change 3 requirements. The Department of Defense (DoD) Chief Information Officer (CIO) issued a waiver of IPv6 requirements until May 2013. The waiver was based on a low risk to the operational architecture due to no scheduled IPv6 deployments prior to May 2013, vendor commitment to resolve the IPv6 discrepancies by May 2013, and the vendor's commitment to upgrade the SUT version 6.3 at no cost to the government with an IPv6 software patch when available. If Acme Packets does not meet their obligation to implement IPv6 by May 2013, then the SUT will be subject to removal from the UC APL.

d. Network Management Requirements. The UCR 2008, Change 3, sections 5.3.2.4, 5.3.2.17, and 5.3.2.18 state the EBC must meet the following Network Management Requirements. Network Management requirements were met via a vendor-submitted LoC.

(1) VVoIP NMS Interface Requirements. The UCR 2008, Change 3, section 5.3.2.4.4, states the physical interface between the DISA Voice and Video over IP (VVoIP) Element Management system (EMS) and the network components is a 10/100-Mbps Ethernet interface. The interface will work in either of the two following modes using auto-negotiation: IEEE, Ethernet Standard 802.3, 1993; or IEEE, Fast Ethernet Standard 802.3u, 1995. The SUT LoC stated compliance to both 10/100-Mbps interfaces.

(2) General Management Requirements. The UCR 2008, Change 3, section 5.3.2.17.2, states the EBC must meet the general management requirements. The SUT's NM LoC stated compliance to Section 5.3.2.17.2.

(3) Requirement for FCAPS Management. The UCR 2008, Change 3, section 5.3.2.17.3, states the EBC must meet the requirements for the five general functional areas of FCAPS. The SUT's NM LoC stated compliance to Section 5.3.2.17.3.

(4) NM requirements of Appliance Functions. The UCR 2008, Change 3, section 5.3.2.18, states the EBC must meet the NM requirements of Appliance Functions listed for an EBC. The SUT's NM LoC stated compliance with the following minor exception. The Configuration Management (CM) and Performance Management (PM) data is not available via Simple Network Management Protocol version 3 (SNMPv3); however Fault Management data is. DISA adjudicated this minor and has changed SNMPv3 to optional for CM and PM in the next version of the UCR (UCR 2013).

11.3 Information Assurance. The Information Assurance requirements are tested by DISA-led Information Assurance test teams and the results published in a separate report, Reference (e).

11.4 Other. None.

12. TEST AND ANALYSIS REPORT. No detailed test report was developed in accordance with the Program Manager's request. JITC distributes interoperability information via the JITC Electronic Report Distribution (ERD) system, which uses Unclassified-But-Sensitive Internet Protocol Router Network (NIPRNet) e-mail. More comprehensive interoperability status information is available via the JITC System Tracking Program (STP). STP is accessible by .mil/gov users on the NIPRNet 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 <http://jit.fhu.disa.mil> (NIPRNet). Information related to DSN testing is on the Telecom Switched Services Interoperability (TSSI) website at <http://jitc.fhu.disa.mil/tssi>. 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 through government civilian or uniformed military personnel from the Unified Capabilities Certification Office (UCCO), e-mail: disa.meade.ns.list.unified-capabilities-certification-office@mail.mil. All associated data is available on the DISA UCCO website located at <http://www.disa.mil/ucco/>.

SYSTEM FUNCTIONAL AND CAPABILITY REQUIREMENTS

The Edge Boundary Controllers (EBCs) have required and conditional features and capabilities that are established by Section 5.3.2.15 of the Unified Capabilities Requirements (UCR). The System Under Test (SUT) need not provide conditional requirements. If they are provided, they must function according to the specified requirements. The detailed Functional Requirements and Capability Requirements for EBCs are listed in Table 3-1. Detailed Information Assurance (IA) requirements are included in References (e) and (f) and are not listed below.

Table 3-1. EBC Capability/Functional Requirements Table

ID	Requirement	UCR Ref (UCR 2008 Change 3)	R/C
1	The product shall act as AS-SIP B2BUA for interpreting the AS-SIP messages to meet its functions.	5.3.2.15.1	R
2	The product shall be capable of bidirectionally anchoring (NAT and NAPT) the media associated with a voice or video session that originates or terminates within its enclave.	5.3.2.15.1 (1)	R
3	The product shall assign a locally unique combination of “c” and “m” lines when anchoring the media stream.	5.3.2.15.1 (1.a)	R
4	If an INVITE request is forwarded to a product fronting an MFSS for which the INVITE request is not destined (i.e., the MFSS will forward the INVITE request downstream to another MFSS or LSC), the product shall be capable of anchoring the media upon receipt of the INVITE request, but shall restore the original “c” and “m” lines upon receipt of the forwarded INVITE request from the MFSS.	5.3.2.15.1 (1.b)	R
5	If a session is forwarded or transferred so the session is external to the enclave (i.e., the session no longer terminates or originates within the enclave), then the product shall restore the original received “c” and “m” lines to the forwarding/transfer message, as appropriate, to ensure that the media is no longer anchored to that product.	5.3.2.15.1 (1.c)	R
6	The EBC shall be capable of processing Route headers in accordance with RFC 3261, Sections 20.34, 8.1.2, 16.4, and 16.12.	5.3.2.15.1 (2)	R
7	The product shall preserve/pass the CCA-ID field in the Contact header.	5.3.2.15.1 (3)	R
8	The product shall always decrement the Max-Forward header.	5.3.2.15.1 (4)	R
9	The product shall modify the Contact header to reflect its IP address to ensure it is in the return routing path.	5.3.2.15.1 (5)	R
10	The product fronting an LSC shall be capable of maintaining a persistent TLS session between the EBC fronting the primary MFSS and the EBC fronting the secondary MFSS.	5.3.2.15.1 (6)	R
11	The EBC shall be capable of distinguishing between the primary (associated with the primary MFSS) and a secondary (associated with the secondary MFSS) TLS path for the purposes of forwarding AS-SIP messages.	5.3.2.15.1 (6.a)	R
12	With the exception of OPTIONS requests, the EBC shall forward all AS-SIP messages received from the LSC across the secondary TLS path if the primary TLS path fails, or a notification arrives at the product indicating that the primary MFSS has failed. If the primary TLS path is available, then the EBC MUST continue to send OPTIONS requests received from the LSC to the EBC serving the primary MFSS. Once the primary TLS path is restored or the primary MFSS recovers, the product shall forward all AS-SIP messages corresponding to new call requests across the primary TLS paths. The AS-SIP messages associated with existing calls that were established in conjunction with the secondary MFSS MUST continue to be sent to the EBC for the secondary MFSS to facilitate a non-disruptive failback to the primary MFSS.	5.3.2.15.1 (6.b)	R
13	The EBC shall fail over to the secondary TLS path when the product receives an AS-SIP message indicating a (408) Request Timeout, (503) Service Unavailable, or (504) Server Timeout response.	5.3.2.15.1 (6.b.1)	R
14	The EBC shall fail over to the secondary TLS path when it detects a configurable number of AS-SIP OPTIONS request failures. The default number of failures shall be two. NOTE: A failure is indicated by a lack of a response or a failure notice.	5.3.2.15.1 (6.b.2)	R

Table 3-1. EBC Capability/Functional Requirements Table (continued)

ID	Requirement	UCR Ref (UCR 2008 Change 3)	R/C
15	The EBC shall return to forwarding all new calls on the primary TLS path (to the primary MFSS) upon receipt of a 200 (OK) response from the primary MFSS to an OPTIONS request issued by its LSC.	5.3.2.15.1 (6.b.3)	R
16	The EBC fronting a secondary MFSS shall respond with a (481) Call/Transaction Does Not Exist when it receives a RE-INVITE, UPDATE, or BYE AS-SIP message for which it has no match (because the session was established via the primary MFSS).	5.3.2.15.1 (6.b.4)	R
17	The EBC initiates a session toward its subtended LSC/MFSS (arriving from the WAN) when receiving an incoming INVITE AS-SIP message from the WAN.	5.3.2.15.1 (6.c)	R
18	The product shall be capable of handling the aggregated WAN call processing load associated with its subtended LSCs and MFSSs.	5.3.2.15.2	R
19	The product shall support FCAPS Network Management functions as defined in Section 5.3.2.17, Management of Network Appliances, of UCR 2008 Change 3.	5.3.2.15.3	R
20	The EBC shall be capable of ensuring that media streams associated with a particular session use the appropriate DSCP based on the information in the AS-SIP RPH.	5.3.2.15.4	R
21	The EBC shall be capable of ensuring that the media streams associated with a particular session use the appropriate codec (bandwidth) based on the SDP information in the AS-SIP message.	5.3.2.15.5	R
22	<p>[Required: High Availability EBC with NLAS] The product shall have an availability of 99.999 percent (non-availability of no more than 5 minutes per year). The product shall meet the requirements specified in Section 5.3.2.5.2, Product Quality Factors.</p> <p>[Conditional: High Availability EBC without NLAS] The product shall have an availability of 99.999 percent (non-availability of no more than 5 minutes per year). The product shall meet the requirements specified in UCR 2008, Section 5.3.2.5.2.1, Product Availability, except for Item 9, No Loss of Active Sessions.</p> <p>[Required: Medium Availability EBC without NLAS] The product shall have an availability of 99.99 percent. The product shall meet the requirements specified in Section 5.3.2.5.2.1, Product Availability, except for Item 9, No Loss of Active Sessions.</p> <p>[Conditional: Low Availability EBC] The product shall have an availability of 99.9 percent. The product does not need to meet the requirements specified in Section 5.3.2.5.2, Product Quality Factors, of this document.</p>	5.3.2.15.6	R
23	The product shall be capable of supporting the IEEE 802.1Q 2-byte TCI Field 12-bit Virtual VID.	5.3.2.15.7	R
24	The product shall be capable of receiving, processing, and transmitting an UC packet within 2 ms to include executing all internal functions.	5.3.2.15.8	R
25	If the EBC supports ITU-T H.323 video, then the product shall be capable of processing and forwarding ITU-T H.323 messages in accordance with Section 5.4, Information Assurance Requirements, of this document.	5.3.2.15.9	C
26	This requirement applies to both Deployable (Tactical) and Fixed (Strategic) EBCs. A physical EBC may house two or more logical EBCs supporting two or more LSCs. Each logical EBC is a software based partition of the single physical EBC asset. Each logical EBC will have its own IP address. Virtual machine middleware may be employed for the partitioning of the physical EBC into two or more logical EBCs.	5.3.2.15.11	C
27	<p>When an EBC is implemented as a B2BUA, then:</p> <ul style="list-style-type: none"> • Whenever the EBC receives a SIP request, before it forwards the request downstream, the EBC MUST replace the hostname part of the SIP URI of the Contact header with its own routable IP address (i.e., B2BUAs perform this replacement on all SIP requests). • Whenever the EBC receives a SIP response, before it forwards the response upstream, the EBC MUST replace the hostname part of the SIP URI of the Contact header with its own routable IP address (i.e., B2BUAs perform this replacement on all SIP responses). 	5.3.4.7.1.3d	R
28	If an EBC receives an INVITE from its AS-SIP signaling appliance and has been unable to establish a TLS connection with either the EBC or the AS-SIP signaling appliance that is the next hop for the INVITE and is unable to do so upon receipt of the INVITE, then the EBC MUST reply to the INVITE with a 403 (Forbidden) response code with a Warning header with warn-code 399 (Miscellaneous warning) and warn-text "TLS connection failure".	5.3.4.7.1.11	R

Table 3-1. EBC Capability/Functional Requirements Table (continued)

ID	Requirement	UCR Ref (UCR 2008 Change 3)	R/C
29	The hostname of the SIP URI in the Contact header of a SIP request or response forwarded by an EBC implemented as a B2BUA MUST be a routable IP address.	5.3.4.7.6.15.4	R
30	The hostname of the SIP URI in the Contact header of a SIP request or response generated by an AS-SIP EI or by an LSC serving an IP EI implemented as a proxy or forwarded by a LSC, Softswitch, or EBC implemented as a proxy MAY either be a routable IP address or a UC network name.	5.3.4.7.6.15.5	R
31	The product shall support dual IPv4 and IPv6 stacks as described in RFC 4213.	5.3.5.4 (1)	R
32	Dual stack end points or Call Control Agents shall be configured to choose IPv4 over IPv6.	5.3.5.4 (1.1)	R
33	All nodes that are "IPv6-capable" shall be carefully configured and verified that the IPv6 stack is disabled until it is deliberately enabled as part of a risk management strategy.	5.3.5.4 (1.2)	R
34	The product shall support the manual tunnel requirements as described in RFC 4213.	5.3.5.4 (1.3)	C
35	The system shall provide the same (or equivalent) functionality in IPv6 as in IPv4 consistent with the requirements in the UCR for its APL category.	5.3.5.4 (1.4)	R
36	The product shall support the IPv6 format as described in RFC 2460 and updated by RFC 5095.	5.3.5.4 (2)	R
37	The product shall support the transmission of IPv6 packets over Ethernet networks using the frame format defined in RFC 2464.	5.3.5.4 (3)	R
38	The product shall support Path MTU Discovery (RFC 1981).	5.3.5.4.1 (4)	R
39	The product shall support a minimum MTU of 1280 bytes (RFC 2460 and updated by RFC 5095).	5.3.5.4.1 (5)	R
40	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, the product shall ignore the request for the smaller MTU and shall include a fragment header in the packet.	5.3.5.4.1 (6)	C
41	The product shall not use the Flow Label field as described in RFC 2460.	5.3.5.4.2 (7)	R
42	The product shall be capable of setting the Flow Label field to zero when originating a packet.	5.3.5.4.2 (7.1)	R
43	The product shall not modify the Flow Label field when forwarding packets.	5.3.5.4.2 (7.2)	R
44	The product shall be capable of ignoring the Flow Label field when receiving packets.	5.3.5.4.2 (7.3)	R
45	The product shall support the IPv6 Addressing Architecture as described in RFC 4291.	5.3.5.4.3 (8)	R
46	The product shall support the IPv6 Scoped Address Architecture as described in RFC 4007.	5.3.5.4.3 (9)	R
47	If a scoped address (RFC 4007) is used, the product shall use a scope index value of zero when the default zone is intended.	5.3.5.4.3 (9.1)	R
48	The product shall support Neighbor Discovery for IPv6 as described in RFC 2461 and RFC 4861 (UCR 2010).	5.3.5.4.5 (11)	R
49	The product shall not set the override flag bit in the Neighbor Advertisement message for solicited advertisements for anycast addresses or solicited proxy advertisements.	5.3.5.4.5 (11.1)	R
50	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.	5.3.5.4.5 (11.3)	R
51	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.	5.3.5.4.5 (11.4)	R
52	When address resolution fails on a neighboring address, the entry shall be deleted from the product's neighbor cache.	5.3.5.4.5 (11.5)	R
53	The product shall support the ability to configure the product to ignore Redirect messages.	5.3.5.4.5.1 (11.6)	R
54	The product shall only accept Redirect messages from the same router as is currently being used for that destination.	5.3.5.4.5.1 (11.7)	R
55	If "Redirect" messages are allowed, the product shall update its destination cache in accordance with the validated Redirect message.	5.3.5.4.5.1 (11.7.1)	C
56	If the valid "Redirect" message is allowed and no entry exists in the destination cache, the product shall create an entry.	5.3.5.4.5.1 (11.7.2)	C

Table 3-1. EBC Capability/Functional Requirements Table (continued)

ID	Requirement	UCR Ref (UCR 2008 Change 3)	R/C
57	The product shall prefer routers that are reachable over routers whose reachability is suspect or unknown.	5.3.5.4.5.12 (11.8.1)	R
58	If the product supports stateless IP address autoconfiguration, including those provided for the commercial market, the product shall support IPv6 SLAAC for interfaces supporting UC functions in accordance with RFC 2462 and RFC 4862 (UCR 2010).	5.3.5.4.6 (12)	C
59	If the product supports IPv6 SLAAC, the product shall have a configurable parameter that allows the function to be enabled and disabled.	5.3.5.4.6 (12.1)	C
60	If the product supports IPv6 SLAAC, 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.	5.3.5.4.6 (12.1.1)	C
61	If the product supports stateless IP address autoconfiguration including those provided for the commercial market, the DAD shall be disabled in accordance with RFC 2462 and RFC 4862.	5.3.5.4.6 (12.2)	R
62	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.	5.3.5.4.6 (12.2.1)	R
63	The product shall support manual assignment of IPv6 addresses.	5.3.5.4.6 (12.3)	R
64	The product shall support the ICMPv6 as described in RFC 4443.	5.3.5.4.7 (14)	R
65	The product shall have a configurable rate limiting parameter for rate limiting the forwarding of ICMP messages.	5.3.5.4.7 (14.1)	R
66	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.	5.3.5.4.7 (14.2)	R
67	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.	5.3.5.4.7 (14.3)	R
68	The product shall validate ICMPv6 messages, using the information contained in the payload, before acting on them.	5.3.5.4.7 (14.4)	R
69	The product shall support MLD as described in RFC 2710.	5.3.5.4.8 (21)	R
70	If the product uses IPSec, the product shall support the Security Architecture for the IP RFC 2401 and RFC 4301 (UCR 2010).	5.3.5.4.9 (22)	C
71	If RFC 4301 is supported, the product shall support binding of a Security Association (SA) with a particular context.	5.3.5.4.9 (22.1)	C
72	If RFC 4301 is supported, the product shall be capable of disabling the BYPASS IPSec processing choice.	5.3.5.4.9 (22.2)	C
73	If RFC 4301 is supported, the product shall not support the mixing of IPv4 and IPv6 in a security association.	5.3.5.4.9 (22.3)	C
74	If RFC 4301 is supported, the product's 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, describes a scenario where this could occur.	5.3.5.4.9 (22.4)	C
75	If RFC 4301 is supported, the product shall be capable of correlating the DSCP for a VVoIP stream to the security association in accordance with Section 5.3.2, Assured Services Requirements and Section 5.3.3, Network Infrastructure E2E Performance Requirements, plain text DSCP plan.	5.3.5.4.9 (22.5)	C
76	If RFC 4301 is supported, the product shall implement IPSec to operate with both integrity and confidentiality.	5.3.5.4.9 (22.6)	C
77	If RFC 4301 is supported, 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.	5.3.5.4.9 (22.7)	C
78	If an ICMP outbound packet message is allowed, the product shall be capable of rate limiting the transmission of ICMP responses.	5.3.5.4.9 (22.7.1)	C
79	If RFC 4301 is supported, the product shall be capable of enabling or disabling the propagation of the Explicit Congestion Notification (ECN) bits.	5.3.5.4.9 (22.8)	C
80	If RFC 4301 is supported, the system's SPD shall have a nominal, final entry that discards anything unmatched.	5.3.5.4.9 (22.9)	C

Table 3-1. EBC Capability/Functional Requirements Table (continued)

ID	Requirement	UCR Ref (UCR 2008 Change 3)	R/C
81	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, 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.	5.3.5.4.9 (22.10)	C
82	If RFC 4301 is supported, the product should include a management control to allow an administrator to enable or disable the ability of the product to send an IKE notification of an INVALID_SELECTORS.	5.3.5.4.9 (22.11)	C
83	If RFC 4301 is supported, the product shall support the ESP Protocol in accordance with RFC 4303.	5.3.5.4.9 (22.12)	C
84	If RFC 4303 is supported, the product shall be capable of enabling anti-replay.	5.3.5.4.9 (22.12.1)	C
85	If RFC 4303 is supported, 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.	5.3.5.4.9 (22.12.2)	C
86	Reserved.	5.3.5.4.9 (22.13)	
87	If RFC 4301 is supported, the product shall support IKE version 1 (IKEv1) (Threshold) as defined in RFC 2409, and IKE version 2 (IKEv2) (UCR 2010) as defined in RFC 4306 (UCR 2010).	5.3.5.4.9 (22.14)	C
88	Reserved.	5.3.5.4.9 (22.14.1)	
89	Reserved.	5.3.5.4.9 (22.14.2)	
90	To prevent a 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.	5.3.5.4.9 (22.14.3)	C
91	If RFC 4301 is supported, the product shall support extensions to the Internet IP Security Domain of Interpretation for the ISAKMP as defined in RFC 2407.	5.3.5.4.9 (22.15)	C
92	If RFC 4301 is supported, the product shall support the ISAKMP as defined in RFC 2408.	5.3.5.4.9 (22.16)	C
93	If the product supports the IPSec Authentication Header Mode, the product shall support the IP AH as defined in RFC 4302.	5.3.5.4.9 (22.17)	C
94	If RFC 4301 is supported, the product shall support manual keying of IPSec.	5.3.5.4.9 (22.18)	C
95	If RFC 4301 is supported, the product shall support the ESP and AH cryptographic algorithm implementation requirements as defined in RFC 4305 and RFC 4835 (UCR 2010).	5.3.5.4.9 (22.19)	C
96	If RFC 4301 is supported, the product shall support the IKEv1 security algorithms as defined in RFC 4109.	5.3.5.4.9 (22.21)	C
97	If the product uses URIs, the product shall use the URI syntax described in RFC 3986.	5.3.5.4.10 (32)	C
98	If the product uses the DNS resolver, the product shall conform to RFC 3596 for DNS queries.	5.3.5.4.10 (33)	C
99	For traffic engineering purposes, the bandwidth required per voice subscriber is calculated to be 110.0 kbps (each direction) for each IPv6 call.	5.3.5.4.11 (34)	R
100	The product shall forward packets using the same IP Version as the Version in the received packet.	5.3.5.4.12 (37)	R
101	When the product is establishing media streams from dualstacked appliances for AS-SIP signaled sessions, the product shall use the ANAT semantics for the SDP in accordance with RFC 4091. Also, the following conditional requirements would apply.	5.3.5.4.12 (38)	R
102	The product shall prefer any IPv4 address to any IPv6 address when using ANAT semantics.	5.3.5.4.12 (38.1)	R
103	The product shall place the option tag "SDP-ANAT" in a Required header field when using ANAT semantics in accordance with RFC 4092.	5.3.5.4.12 (38.2)	R
104	If the product is using AS-SIP and the <addrtype> is IPv6 and the <connection-address> is a unicast address, the product shall support generation and processing of unicast IPv6 addresses as specified in UCR 2008 Change 3	5.3.5.4.13 (39)	C
105	If the product is using AS-SIP, the product shall support the generation and processing of IPv6 unicast addresses using compressed zeros as specified.	5.3.5.4.13 (40)	C

Table 3-1. EBC Capability/Functional Requirements Table (continued)

ID	Requirement	UCR Ref (UCR 2008 Change 3)	R/C
106	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), the product shall support the generation and processing of multicast IPv6 addresses having the same formats as the unicast IPv6 addresses.	5.3.5.4.13 (41)	C
107	If the product is using AS-SIP and the <addrtype> is IPv6, the product shall support the use of RFC 3266 and RFC 4566 [UCR 2010] for IPv6 in SDP as described in Section 5.3.4, AS-SIP Requirements.	5.3.5.4.13 (42)	C
108	If the product is using AS-SIP and the <addrtype> is IPv6 and the <connection-address> is an IPv6 multicast group address, 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.	5.3.5.4.13 (43)	C
109	If the product is using AS-SIP, 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.	5.3.5.4.13 (44)	C
110	The products shall support Differentiated Services as described in RFC 2474 for a voice and video stream in accordance with Section 5.3.2, Assured Services Requirements, and Section 5.3.3, Network Infrastructure E2E Performance Requirements, plain text DSCP plan.	5.3.5.4.14 (52)	R
111	If the product acts as an IPv6 tunnel broker, the product shall support the function as defined in RFC 3053.	5.3.5.4.14 (53)	C
112	Mapping of RFCs to UC Profile Categories - Table 5.3.5-6.	5.3.5.5	R
113	The physical interface between the DISA VVoIP EMS and the network components (i.e., LSC, MFSS, EBC, CE Router) is a 10/100-Mbps Ethernet interface. The interface will work in either of the two following modes using auto-negotiation: IEEE, Ethernet Standard 802.3, 1993; or IEEE, Fast Ethernet Standard 802.3u, 1995.	5.3.2.4.4	R
114	SNMPv3 format	5.3.2.17.2	R
115	As specified in Section 5.3.2.4.4, VoIP NMS Interface Requirements, the EBC and CE Router components shall support one pair of physical Ethernet management interfaces at the component level. One of these Ethernet management interfaces shall be used for component-level communication with a Local EMS. The other Ethernet management interface shall be used for component-level communication with the remote VVoIP EMS. The EBC and CE Router components shall also support at two redundant physical Ethernet interfaces at the component level to carry the signaling and media streams for VVoIP traffic.	5.3.2.17.2	R
116	A network appliance shall have Operations interfaces that provide a standard means by which management systems can directly or indirectly communicate with and, thus, manage the various network appliances in the DISN.	5.3.2.17.2	R
117	There shall be a local craftsperson interface (CID) for OA&M for all VVoIP network components. The CID is a supplier-provided input/output device that is locally connected to a network component. The CID may be connected to the Local EMS, which is in turn connected to the VVoIP component using the Local EMS Ethernet management interface. The CID may be connected directly to the VVoIP network component also, using the Ethernet management interface on the component that would otherwise be used by the Local EMS (there is no Local EMS in this case). The CID may be connected directly to the VVoIP network component using a separate serial interface.	5.3.2.17.2	R
118	The network appliances shall provide NM data to the external VVoIP EMS.	5.3.2.17.2	R
119	A network appliance shall communicate with an external Voice and Video management system by a well-defined, standards-based management interface using an industry-accepted management protocol.	5.3.2.17.2	R
120	Communications between VVoIP EMS and the VVoIP network appliances shall be via IP.	5.3.2.17.2	R
121	Where an EMS is the interface with a VVoIP component, the TCP/IP-based communications between the VVoIP EMS and the Local EMS shall be via <ul style="list-style-type: none"> • [Required 2010: NM] Extensible Markup Language (XML) • [Objective 2012: NM] Multi-Technology Operations System(s) Interface (MTOSI) 	5.3.2.17.2	R
122	A network appliance shall issue state change notifications for changes in the states of replaceable components, including changes in operational state or service status, and detection of new components.	5.3.2.17.2	R

Table 3-1. EBC Capability/Functional Requirements Table (continued)

ID	Requirement	UCR Ref (UCR 2008 Change 3)	R/C
123	A network appliance shall be provisioned by the VVoIP EMS with the address, software, and OSI Layer 4 port information associated with its Core Network interfaces.	5.3.2.17.2	R
124	A network appliance shall be capable of maintaining and responding to VVoIP EMS requests for resource inventory, configuration, and status information concerning Core Network interface resources (e.g., IP or MAC addresses) that have been installed and placed into service.	5.3.2.17.2	R
125	A network appliance shall be capable of setting the Administrative state and maintaining the Operational state of each Core Network interface, and maintaining the time of the last state change.	5.3.2.17.2	R
126	A network appliance shall generate an alarm condition upon the occurrence of any of the following failure conditions, as defined in ITU-T Recommendation M.3100: <ul style="list-style-type: none"> • Power loss • Environmental condition not conducive to normal operation • Loss of data integrity 	5.3.2.17.2	R
127	A network appliance shall be capable of maintaining and responding to requests for physical resource capacity information for installed components. This information includes the following: <ul style="list-style-type: none"> • Component type and model • Shelf location • Rack location • Bay location 	5.3.2.17.2	R
128	Fault Management supports the detection, isolation, and correction of abnormal operating conditions in a telecommunications network and its environment. Fault Management provides the functions to manage service problems, to support customer interactions associated with service troubles, and to support business policies related to service problems. Faults will be reported IAW IETF RFC 1215.	5.3.2.17.3.1	R
129	The network components shall send alarm messages in SNMPv3 format.	5.3.2.17.3.1.5	R
130	Configuration Management (CM) exercises control over, identifies, collects data from, and provides data to NEs and the connections between NEs. Configuration Management is responsible for the planning and installation of NEs and their interconnection into a network. Configuration Management includes the establishment of customer services that use the network, all services and product planning, and business policy level functions related to service establishment. All CM information shall be presented IAW RFCs 1213 and 3418.	5.3.2.17.3.2	C
131	Accounting Management enables the network service usage to be measured and the costs for such use to be determined. It provides facilities to collect accounting records and to set billing parameters for the usage of services and for access to the network. It also includes functionality to exercise control over the proper flow of funds within the enterprise and between the enterprise and its owners and creditors. Detailed requirements for Accounting Management, including requirements related to call quality, are found in Section 5.3.2.19, Accounting Management.	5.3.2.17.3.3	C
132	Performance Management (PM) evaluates and reports the effectiveness with which the network and its NEs support assigned services. Performance Management provides mechanisms to measure service quality and provides the business policy functions for quality control.	5.3.2.17.3.4	C
133	All management interactions shall meet the Information Assurance requirements in Section 5.4, Information Assurance Requirements.	5.3.2.17.3.5	R
134	Faults will be reported IAW RFCs 1215 and 3418.	5.3.2.18.1	R
135	Standard CM information shall be presented IAW RFCs 1213 and 3418.	5.3.2.18.1	R
136	Standard PM information shall be presented IAW RFCs 1213 and 3418.	5.3.2.18.1	R
137	Nonstandard (vendor-specific) CM and PM information shall be presented as private vendor MIBs, as defined by the applicable RFCs.	5.3.2.18.1	C
138	SNMPv3 format.	5.3.2.18.1	R
139	The CE Router QoS queues must be readable and settable by the VVoIP EMS.	5.3.2.18.1	R

Table 3-1. EBC Capability/Functional Requirements Table (continued)

LEGEND:		
802.1Q	Standards for Local and Metropolitan Area Networks: Virtual Bridged Local Area Networks	ITU-T International Telecommunication Union - Telecommunication Standardization Sector
AH	Authentication Header	LSC Local Session Controller
ANAT	Alternative Network Address Type	MAC Media Access Control
APL	Approved Products List	Mbps Megabits per second
AS-SIP	Assured Services Session Initiation Protocol	MFSS Multifunction Softswitch
B2BUA	Back-to-Back User Agent	MLD Multicast Listener Discover
C	Conditional	ms millisecond
CCA-ID	Call Connection Agent Identification	MTU Maximum Transmission Unit
CE	Customer Edge	NAPT Network Address Port Translation
CID	Craft Input Device	NAT Network Address Translation
CM	Configuration Management	NE Network Element
DAD	Duplicate Address Detection	NLAS No Loss of Active Sessions
DISA	Defense Information Systems Agency	NM Network Management
DISN	Defense Information Systems Network	NMS Network Management System
DNS	Domain Name Service	OA&M Operations, Administration, and Maintenance
DoS	Denial of Service	OSI Open Systems Interconnect
DSCP	Differentiated Services Code Point	PM Performance Management
E2E	End to End	QoS Quality of Service
EBC	Edge Boundary Controller	R Required
EI	End Instrument	RFC Request for Comments
EMS	Element Management System	RPH Resource-Priority Header
ESP	Encapsulating Security Payload	SA Security Association
FCAPS	Fault, Configuration, Accounting, Performance, and Security	SAD Security Association Database
H.323	Standard for multi-media communications on packet-based networks	SDP Session Description Protocol
IAW	in accordance with	SIP Session Initiation Protocol
ICMP	Internet Control Message Protocol	SLAAC Stateless Address Autoconfiguration
ICMPv6	Internet Control Message Protocol for IPv6	SPD Security Policy Database
ID	Identification	SNMPv3 Simple Network Management Protocol version 3
IEEE	Institute of Electrical and Electronics Engineers	TCI Tag Control Information
IETF	Internet Engineering Task Force	TCP/IP Transmission Control Protocol/Internet Protocol
IKE	Internet Key Exchange	TLS Transport Layer Security
IP	Internet Protocol	UC Unified Capabilities
IPSEC	Internet Protocol Security	UCR Unified Capabilities Requirements
IPv4	Internet Protocol version 4	URI Uniform Resource Identifier
IPv6	Internet Protocol version 6	VID VLAN Identification
ISAKMP	Internet Security Association and Key Management Protocol	VLAN Virtual Local Area Network
		VVoIP Voice and Video over Internet Protocol
		WAN Wide Area Network