



DEFENSE INFORMATION SYSTEMS AGENCY

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

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

12 May 11

MEMORANDUM FOR DISTRIBUTION

SUBJECT: Special Interoperability Test Certification of the Cisco 3800, 3900, 2900, and 2800 Series Integrated Services Router (ISR) Edge Boundary Controller (EBC) with Internetworking Operating System (IOS) 15.1 Engineering Special (ES) 15.1(20110111:230218) [15-1-3-17-T]

References: (a) DoD Directive 4630.05, "Interoperability and Supportability of Information Technology (IT) and National Security Systems (NSS)," 5 May 2004
(b) CJCSI 6212.01E, "Interoperability and Supportability of Information Technology and National Security Systems," 15 December 2008
(c) through (e), see Enclosure 1

1. References (a) and (b) establish the Defense Information Systems Agency (DISA) Joint Interoperability Test Command (JITC), as the responsible organization for interoperability test certification.

2. The Cisco 3845 and 3945 ISRs EBC with IOS 15.1 Engineering Special Version 15.1(20110111:230218) [15-1-3-17-T] are hereinafter referred to as the System Under Test (SUT). The SUT meets all of its critical interoperability requirements for joint use within the Defense Information System Network (DISN) as a High Availability EBC without "No Loss of Active Sessions" (NLAS) because during failover of a redundant component, all active sessions are lost. When an EBC meets the High Availability EBC requirements without NLAS, it is also certified as a Medium Availability without NLAS, and a Low Availability EBC. To meet the High Availability and Medium Availability EBC requirements, the SUT must be configured in a dual chassis configuration. The Low Availability EBC requirements are met with a single chassis configuration. The SUT is certified for joint use within the DISN in both classified and sensitive-but-unclassified (SBU) networks. The Defense Information Systems Agency (DISA) adjudicated Test Discrepancy Reports (TDRs) open at the completion of testing to have a minor operational impact. The minor operational impact of noted discrepancies was based on the SUT's conditions of fielding during the initial transition from legacy to Internet Protocol (IP) based communications. The certification status of the SUT will be monitored and verified during operational deployment in the Department of Defense (DoD) Unified Capabilities (UC) Pilot. 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 that addresses all new critical 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). The Cisco 3945E, 3925, 3925E, 3825, 2951, 2921, 2911, 2901 2851, 2821, 2811, and 2801 ISR with IOS 15.1 Engineering Special Version 15.1(20110111:230218) [15-1-3-17-T] EBCs employ the same

JITC Memo, JTE, Special Interoperability Test Certification of the Cisco 3800, 3900, 2900, and 2800 Series Integrated Services Router (ISR) Edge Boundary Controller (EBC) with Internetworking Operating System (IOS) 15.1 Engineering Special (ES) 15.1(20110111:230218) [15-1-3-17-T]

software as the SUT and uses similar hardware. The JITC analysis determined these systems to be functionally identical to the SUT for interoperability certification purposes and it is also certified for joint use. No other configurations, features, or functions, except those cited within this memorandum, are certified by JITC. This certification expires upon changes that affect interoperability, but no later than three years from the date of this memorandum.

3. This finding is based on interoperability testing conducted by JITC, review of the vendor's Letters of Compliance (LoC), and DISA Information Assurance (IA) Certification Authority (CA) approval of the IA configuration. Interoperability testing was conducted by JITC, Fort Huachuca, Arizona, from 11 through 22 October 2010. Final verification and validation testing was conducted by JITC, Fort Huachuca, Arizona, from 17 through 28 January 2011. Review of the vendor's LoC was completed on 13 April 2011. The DISA CIO has reviewed the IA Assessment Report for the SUT, Reference (e), and has granted an Authorization to Operate for the SUT for the DoD UC utilizing Spiral 1 Deployment. 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.

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 (See note 1.)	UCR Paragraph	Threshold CR/FR Requirements (See note 2.)	Status	Remarks (See note 3.)
WAN Interfaces					
1000Base-X	No	5.3.2.4 / 5.3.3.10.1.2	1-3	Certified	IEEE 802.3z
NM Interfaces					
10Base-X	No	5.3.2.4.4	4	Certified	IEEE 802.3i and IEEE 802.3j
100Base-X	No	5.3.2.4.4	4	Certified	IEEE 802.3u

JITC Memo, JTE, Special Interoperability Test Certification of the Cisco 3800, 3900, 2900, and 2800 Series Integrated Services Router (ISR) Edge Boundary Controller (EBC) with Internetworking Operating System (IOS) 15.1 Engineering Special (ES) 15.1(20110111:230218) [15-1-3-17-T]

Table 1. SUT Interface Interoperability Status (continued)

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 identification (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	CR	Capability Requirement		
100Base-X	Generic designation for 100 Mbps Ethernet	FR	Functional Requirement		
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	Mbps	Megabits per second		
802.3j	IEEE Ethernet standard for 10 Mbps over fiber	NM	Network Management		
802.3u	IEEE Ethernet Standard for 100 Mbps over twisted pair and fiber	SUT	System Under Test		
		UCR	Unified Capabilities Requirements		
802.3z	IEEE Ethernet standard for 1000 Mbps over fiber	WAN	Wide Area Network		

Table 2. SUT Capability Requirements and Functional Requirements Status

CR/FR ID	Capability/ Function	Applicability (See note 1.)	UCR Paragraph	Status	Remarks (See note 2.)
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	This was verified through the vendor's LoC.
	Network Management	Required	5.3.2.15.3 5.3.2.17	Met	This was verified through the vendor's LoC.
	DSCP Policing	Required	5.3.2.15.4	Not Met	See note 3.
	Codec Bandwidth Policing	Required	5.3.2.15.5	Not Met	See note 3.
	Availability	Required	5.3.2.15.6	Met	The SUT met this requirement for the high availability without NLAS option. This was verified through the vendor's LoC.
	IEEE 802.1Q Support	Required	5.3.2.15.7	Met	
	Packet Transit Time	Required	5.3.2.15.8	Met	This was verified through the vendor's LoC.
	ITU-T H.323 Support	Conditional	5.3.2.15.9	Not Tested	The SUT offers ITU-T H.323 support, however it was not tested and is not certified.
2	AS-SIP Requirements				
	Requirements for AS-SIP Signaling Appliances	Required	5.3.4.7	Met	
	SIP Session Keep-Alive Timer	Required	5.3.4.8	Met	
	Session Description Protocol	Required	5.3.4.9	Met	
	Precedence and Preemption	Required	5.3.4.10	Met	
	Calling Services	Required	5.3.4.13	Met	
3	IPv6 Requirements				
	Product Requirements	Required	5.3.5.4	Partially Met	This was verified through the vendor's LoC with the exceptions listed in note 4.

JITC Memo, JTE, Special Interoperability Test Certification of the Cisco 3800, 3900, 2900, and 2800 Series Integrated Services Router (ISR) Edge Boundary Controller (EBC) with Internetworking Operating System (IOS) 15.1 Engineering Special (ES) 15.1(20110111:230218) [15-1-3-17-T]

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

CR/FR ID	Capability/ Function	Applicability (See note 1.)	UCR Paragraph	Status	Remarks (See note 2.)																																																								
4	NM Requirements																																																												
	VVoIP NMS Interface Requirements	Required	5.3.2.4.4	Met	This was verified through the vendor's LoC.																																																								
	General Management Requirements	Required	5.3.2.17.2	Met	This was verified through the vendor's LoC.																																																								
	Requirement for FCAPS Management	Required	5.3.2.17.3	Met	This was verified through the vendor's LoC.																																																								
	NM requirements of Appliance Functions	Required	5.3.2.18	Met	This was verified through the vendor's LoC.																																																								
<p>NOTES:</p> <ol style="list-style-type: none"> 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. Paragraph 11 of Enclosure 2 provides detailed information pertaining to open TDRs and associated operational impacts 3. The DISA adjudicated this discrepancy as having a low operational impact because vendors have until July 2011 to comply with this requirement. 4. The LoC stated non-compliance with traffic engineering requirements listed in UCR 2008 Change 1 Section 5.3.5.4.11 paragraph 34. Per DISA clarification dated 21 April 2011, this requirement correlates to UCR 2008 Change 1 Section 5.3.2.15.5 (Codec Bandwidth Policing) which is a new requirement since UCR 2008, therefore the vendor has until July 2011 to comply with this requirement. DISA stated their intent to update this disparity in the next UCR errata change. <p>LEGEND:</p> <table> <tr> <td>802.1Q</td> <td>IEEE VLAN tagging standard</td> <td>ITU-T</td> <td>International Telecommunication Union - Telecommunication Standardization Sector</td> </tr> <tr> <td>AS-SIP</td> <td>Assured Services Session Initiation Protocol</td> <td>JITC</td> <td>Joint Interoperability Test Command</td> </tr> <tr> <td>CR</td> <td>Capabilities Requirement</td> <td>LoC</td> <td>Letters of Compliance</td> </tr> <tr> <td>DISA</td> <td>Defense Information Systems Agency</td> <td>NLAS</td> <td>No Loss of Active Sessions</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>PoAM</td> <td>Plan of Actions and Milestones</td> </tr> <tr> <td>FR</td> <td>Functional Requirement</td> <td>RFC</td> <td>Request for Comment</td> </tr> <tr> <td>H.323</td> <td>ITU-T recommendation that defines audio-visual session protocols</td> <td>SIP</td> <td>Session Initiation Protocol</td> </tr> <tr> <td>ID</td> <td>Identification</td> <td>SS</td> <td>Softswitch</td> </tr> <tr> <td>IEEE</td> <td>Institute of Electrical and Electronics Engineers</td> <td>SUT</td> <td>System Under Test</td> </tr> <tr> <td>IPsec</td> <td>Internet Protocol Security</td> <td>UCR</td> <td>Unified Capabilities Requirements</td> </tr> <tr> <td>IPv6</td> <td>Internet Protocol version 6</td> <td>VVoIP</td> <td>Voice and Video over Internet Protocol</td> </tr> <tr> <td></td> <td></td> <td>WAN</td> <td>Wide Area Network</td> </tr> </table>						802.1Q	IEEE VLAN tagging standard	ITU-T	International Telecommunication Union - Telecommunication Standardization Sector	AS-SIP	Assured Services Session Initiation Protocol	JITC	Joint Interoperability Test Command	CR	Capabilities Requirement	LoC	Letters of Compliance	DISA	Defense Information Systems Agency	NLAS	No Loss of Active Sessions	DSCP	Differentiated Services Code Point	NM	Network Management	EBC	Edge Boundary Controller	NMS	NM System	FCAPS	Fault, Configuration, Accounting, Performance, and Security	PoAM	Plan of Actions and Milestones	FR	Functional Requirement	RFC	Request for Comment	H.323	ITU-T recommendation that defines audio-visual session protocols	SIP	Session Initiation Protocol	ID	Identification	SS	Softswitch	IEEE	Institute of Electrical and Electronics Engineers	SUT	System Under Test	IPsec	Internet Protocol Security	UCR	Unified Capabilities Requirements	IPv6	Internet Protocol version 6	VVoIP	Voice and Video over Internet Protocol			WAN	Wide Area Network
802.1Q	IEEE VLAN tagging standard	ITU-T	International Telecommunication Union - Telecommunication Standardization Sector																																																										
AS-SIP	Assured Services Session Initiation Protocol	JITC	Joint Interoperability Test Command																																																										
CR	Capabilities Requirement	LoC	Letters of Compliance																																																										
DISA	Defense Information Systems Agency	NLAS	No Loss of Active Sessions																																																										
DSCP	Differentiated Services Code Point	NM	Network Management																																																										
EBC	Edge Boundary Controller	NMS	NM System																																																										
FCAPS	Fault, Configuration, Accounting, Performance, and Security	PoAM	Plan of Actions and Milestones																																																										
FR	Functional Requirement	RFC	Request for Comment																																																										
H.323	ITU-T recommendation that defines audio-visual session protocols	SIP	Session Initiation Protocol																																																										
ID	Identification	SS	Softswitch																																																										
IEEE	Institute of Electrical and Electronics Engineers	SUT	System Under Test																																																										
IPsec	Internet Protocol Security	UCR	Unified Capabilities Requirements																																																										
IPv6	Internet Protocol version 6	VVoIP	Voice and Video over Internet Protocol																																																										
		WAN	Wide Area Network																																																										

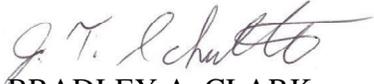
5. No detailed test report was developed in accordance with the Program Manager's request. JITC distributes interoperability information via the JITC Electronic Report Distribution (ERD) system, which uses Unclassified-But-Sensitive Internet Protocol Router Network (NIPRNet) e-mail. More comprehensive interoperability status information is available via the JITC System Tracking Program (STP). The 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>. All associated data is available on the Defense Information Systems Agency Unified Capability Coordination Office (UCCO) website located at <http://www.disa.mil/ucco/>.

JITC Memo, JTE, Special Interoperability Test Certification of the Cisco 3800, 3900, 2900, and 2800 Series Integrated Services Router (ISR) Edge Boundary Controller (EBC) with Internetworking Operating System (IOS) 15.1 Engineering Special (ES) 15.1(20110111:230218) [15-1-3-17-T]

6. The JITC point of contact is Edward Mellon, JITC, commercial (520) 538-5159 or DSN 312-879-5164; e-mail address is edward.mellon@disa.mil. The JITC's mailing address is P.O. Box 12798, Fort Huachuca, AZ 85670-2798. The UCCO tracking number is 0922204.

FOR THE COMMANDER:

3 Enclosures a/s


for BRADLEY A. CLARK
Chief
Battlespace Communications Portfolio

JITC Memo, JTE, Special Interoperability Test Certification of the Cisco 3800, 3900, 2900, and 2800 Series Integrated Services Router (ISR) Edge Boundary Controller (EBC) with Internetworking Operating System (IOS) 15.1 Engineering Special (ES) 15.1(20110111:230218) [15-1-3-17-T]

Distribution (electronic mail):

Joint Staff J-6

Joint Interoperability Test Command, Liaison, TE3/JT1

Office of Chief of Naval Operations, CNO N6F2

Headquarters U.S. Air Force, Office of Warfighting Integration & CIO, AF/XCIN (A6N)

Department of the Army, Office of the Secretary of the Army, DA-OSA CIO/G-6 ASA (ALT), SAIS-IOQ

U.S. Marine Corps MARCORSYSCOM, SIAT, MJI Division I

DOT&E, Net-Centric Systems and Naval Warfare

U.S. Coast Guard, CG-64

Defense Intelligence Agency

National Security Agency, DT

Defense Information Systems Agency, TEMC

Office of Assistant Secretary of Defense (NII)/DOD CIO

U.S. Joint Forces Command, Net-Centric Integration, Communication, and Capabilities Division, J68

Defense Information Systems Agency, GS23

ADDITIONAL REFERENCES

- (c) Office of the Assistant Secretary of Defense, "Department of Defense Unified Capabilities Requirements 2008, Change 1," 22 January 2010
- (d) Joint Interoperability Test Command, "Unified Capabilities Test Plan (UCTP)," October 2010
- (e) Joint Interoperability Test Command, "JITC Memo, JTE, Information Assurance (IA) Assessment of Cisco 3845 Release (Rel.) Internetwork Operating System (IOS) 15.1(2)YB4 (Tracking Number 0922204)

CERTIFICATION TESTING SUMMARY

- 1. SYSTEM TITLE.** The Cisco 3845 Integrated Services Router (ISR) with Internetworking Operating System (IOS) 15.1 Engineering Special (ES) 15.1(20110111:230218) [15-1-3-17-T] Edge Boundary Controller (EBC)
- 2. SPONSOR.** Defense Information Systems Agency, ATTN: Mr. Jordan Silk, Address: ELIE-ISE-TI, Building 53302, Fort Huachuca, Arizona, 85613-5300, e-mail: jordan.silk@us.army.mil.
- 3. SYSTEM POC.** Cisco Systems, INC., Phone: (408)526-4000 or (800)553-NET, e-mail: ucapl@cisco.com, URL <http://www.cisco.com/go/ucapl>
- 4. TESTER.** Joint Interoperability Test Command (JITC), Fort Huachuca, Arizona.
- 5. SYSTEM DESCRIPTION.** The EBC performs voice firewall and back-to-back user agent functions. The EBC consists of the voice or video firewall/border Controller. The call control agent (CCA) in the Wide Area Network (WAN) SoftSwitch (SS) and Local Session controller (LSC) needs to interact with Assured Services Session Initiation Protocol (AS-SIP) functions in the EBC which:
 - Mediates Assured Services Session Initiation Protocol (AS-SIP) signaling between an LSC and an MFSS or WAN SS, and between two MFSSs or SSs.
 - Supports Session Border Controller functions, such as Network Address Translation and Network Address and Port Translation.
 - Supports Internet Protocol (IP) firewall functions.

The Cisco Unified Border Element (CUBE) on a Cisco 3845 ISR or Cisco 3945 ISR with IOS 15.1 Engineering Special Version 15.1(20110111:230218) [15-1-3-17-T] Edge Border Controller (EBC), hereinafter referred to as the System Under Test (SUT), provides the EBC capabilities.

The SUT is an intelligent unified communications network border element. The SUT includes EBC functions that help enable end-to-end IP-based transport of voice, video, and data between independent unified communications networks. EBCs are critical components for scaling unified communications networks from being "IP islands" within a single customer network to becoming an end-to-end IP community. The CUBE is an integrated Cisco Internetworking Operating System (IOS) Software application that runs on the Cisco 3800 Series and Cisco 3900 Series ISRs.

The Cisco 3945E, 3925E, 3925, 2951, 2921, 2911, 2901, 3825, 2851, 2821, 2811, and the Cisco 2801 were not tested; however, they utilize the same software and similar hardware as the 3945 and 3845. JITC analysis determined them to be functionally identical for interoperability certification purposes and they are also certified for joint use. While these products are certified for joint use the following caveat exists for all systems. Due to the engineering nature of the Cisco EBC's all certified equipment that will be configured to traverse the SUT must be configured with an Assured Services Admission Control (ASAC) budget to prevent from exceeding the SUT's maximum threshold for IP to IP calls. These thresholds are as follows:

- Cisco 3945E has a maximum of 2500 simultaneous IP to IP calls.
- Cisco 3925E has a maximum of 2100 simultaneous IP to IP calls.
- Cisco 3945 has a maximum of 950 simultaneous IP to IP calls.
- Cisco 3925 has a maximum of 800 simultaneous IP to IP calls.
- Cisco 2951 has a maximum of 500 simultaneous IP to IP calls.
- Cisco 2921 has a maximum of 400 simultaneous IP to IP calls.
- Cisco 2911 has a maximum of 200 simultaneous IP to IP calls.
- Cisco 2901 has a maximum of 100 simultaneous IP to IP calls.
- Cisco 3845 has a maximum of 500 simultaneous IP to IP calls.
- Cisco 3825 has a maximum of 400 simultaneous IP to IP calls.
- Cisco 2851 has a maximum of 225 simultaneous IP to IP calls.
- Cisco 2821 has a maximum of 200 simultaneous IP to IP calls.
- Cisco 2811 has a maximum of 110 simultaneous IP to IP calls.
- Cisco 2801 has a maximum of 55 simultaneous IP to IP calls.

These values assume the use of a G.711 codec, with voice activation detection turned off, call-hold times of 180 seconds, flow-through mode, Cisco IOS 15.1 Engineering Special Version 15.1(20110111:230218) [15-1-3-17-T], Ethernet egress, and central processor unit use not to exceed 75 percent.

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

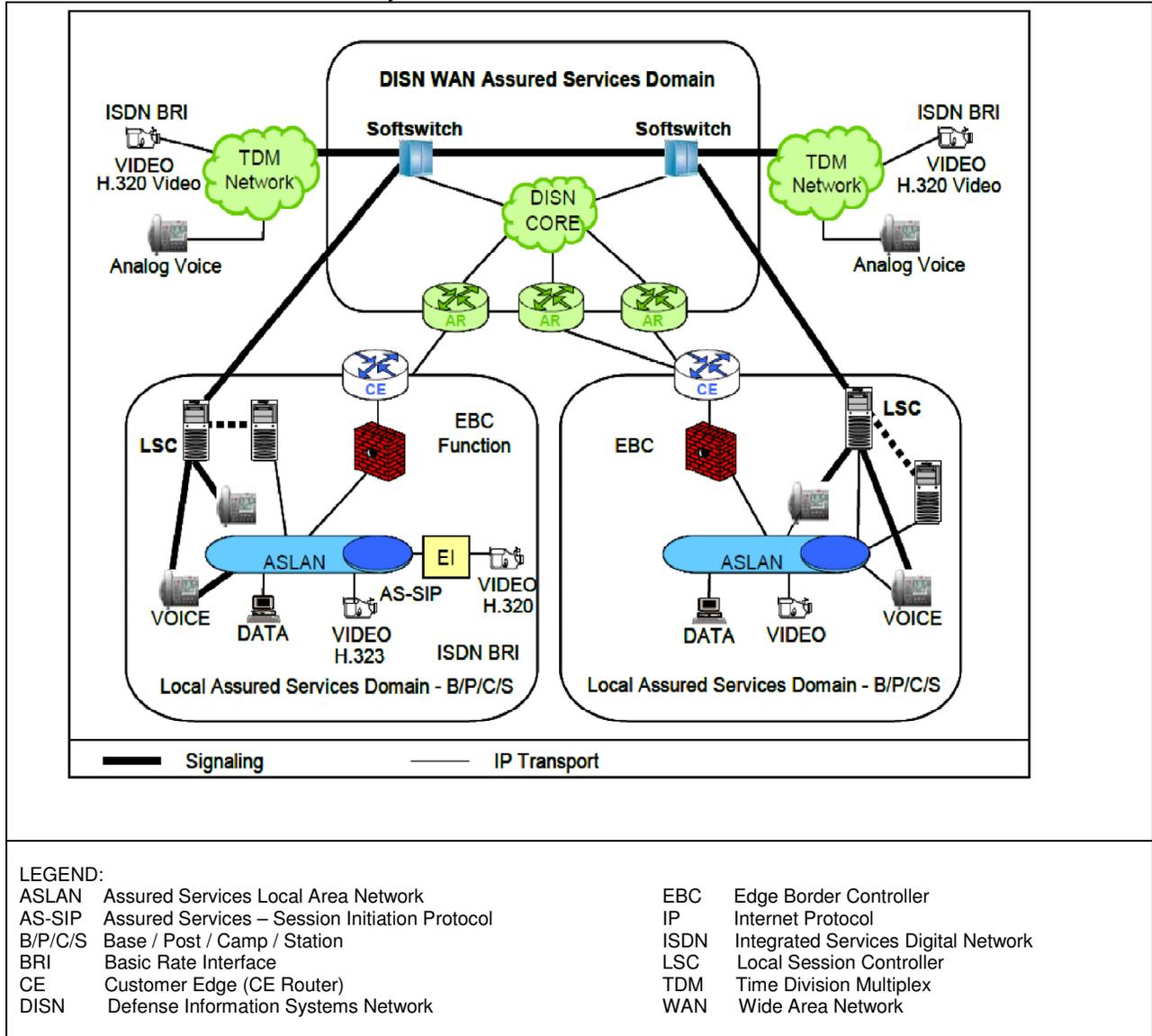


Figure 2-1. Edge Boundary Controller Architecture

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 Cisco 3845 ISR with IOS 15.1 Engineering Special Version 15.1(20110111:230218) [15-1-3-17-T] Edge Border Controller (EBC) uses the external interface to connect to the Global Information Grid network. Table 2-1 shows the physical interface supported by the SUT. The table documents the physical interfaces and the associated standards.

Table 2-1. EBC Interface Requirements

Interface	Critical (See note 1.)	UCR Ref (See note 2.)	Criteria (See note 3.)								
WAN Interfaces											
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 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 requirements.								
100Base-X	No	5.3.2.4.4	Meet IEEE 802.3 standards for 802.3u and meet threshold CR/FR 4 requirements.								
<p>NOTES:</p> <ol style="list-style-type: none"> 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. The SUT's high-level capability and functional requirement ID numbers depicted in the CRs/FRs column can be cross-referenced in Table 2-2. These high-level CR/FR requirements refer to a detailed list of requirements provided in Enclosure 3. The SUT must meet IEEE 802.3 standards for interface provided. <p>LEGEND:</p> <table style="width: 100%; border: none;"> <tr> <td style="width: 50%;">CR Capability Requirement</td> <td style="width: 50%;">SUT System Under Test</td> </tr> <tr> <td>FR Functional Requirement</td> <td>UCR Unified capabilities Requirements</td> </tr> <tr> <td>ID Identification</td> <td>WAN Wide Area Network</td> </tr> <tr> <td>NM Network Management</td> <td></td> </tr> </table>				CR Capability Requirement	SUT System Under Test	FR Functional Requirement	UCR Unified capabilities Requirements	ID Identification	WAN Wide Area Network	NM Network Management	
CR Capability Requirement	SUT System Under Test										
FR Functional Requirement	UCR Unified capabilities Requirements										
ID Identification	WAN Wide Area Network										
NM Network Management											

7.2 CR and 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 IAW the EBC requirements are listed in Table 2-2. Detailed CR/FR requirements are provided in Table 3-1 of Enclosure 3.

Table 2-2. EBC Requirements and FRs

CR/FR ID	Capability/ Function	Applicability (See note.)	UCR Paragraph	Criteria																																				
1	EBC Requirements																																							
	AS-SIP Back-to-Back User Agent	Required	5.3.2.15.1	Detailed requirements and associated criteria for EBCs are listed in Table 3-1 of Appendix 3.																																				
	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	Required	5.3.2.15.9																																						
2	AS-SIP Requirements																																							
	Requirements for AS-SIP Signaling Appliances	Required	5.3.4.7	Detailed requirements and associated criteria for EBCs are listed in Table 3-1 of Appendix 3.																																				
	SIP Session Keep-Alive Timer	Required	5.3.4.8																																					
	Session Description Protocol	Required	5.3.4.9																																					
	Precedence and Preemption	Required	5.3.4.10																																					
Calling Services	Required	5.3.4.13																																						
3	IPv6 Requirements																																							
	Product Requirements	Required	5.3.5.4	See Table 3-1																																				
4	NM Requirements																																							
	VVoIP NMS Interface Requirements	Required	5.3.2.4.4	Detailed requirements and associated criteria for EBCs are listed in Table 3-1 of Appendix 3.																																				
	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																																						
<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>FCAPS</td> <td>Fault, Configuration, Accounting, Performance, and Security</td> <td>NMS</td> <td>NM System</td> </tr> <tr> <td>FR</td> <td>Functional Requirement</td> <td>SIP</td> <td>Session Initiation Protocol</td> </tr> <tr> <td>H.323</td> <td>ITU-T recommendation that defines audio-visual session protocols</td> <td>SUT</td> <td>System Under Test</td> </tr> <tr> <td>ID</td> <td>Identification</td> <td>UCR</td> <td>Unified Capabilities Requirements</td> </tr> <tr> <td></td> <td></td> <td>VVoIP</td> <td>Voice and Video over Internet Protocol</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	FCAPS	Fault, Configuration, Accounting, Performance, and Security	NMS	NM System	FR	Functional Requirement	SIP	Session Initiation Protocol	H.323	ITU-T recommendation that defines audio-visual session protocols	SUT	System Under Test	ID	Identification	UCR	Unified Capabilities Requirements			VVoIP	Voice and Video over Internet Protocol
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																																					
FCAPS	Fault, Configuration, Accounting, Performance, and Security	NMS	NM System																																					
FR	Functional Requirement	SIP	Session Initiation Protocol																																					
H.323	ITU-T recommendation that defines audio-visual session protocols	SUT	System Under Test																																					
ID	Identification	UCR	Unified Capabilities Requirements																																					
		VVoIP	Voice and Video over Internet Protocol																																					

7.3 Information Assurance (IA). Table 2-3 details the IA requirements applicable to the EBC products.

Table 2-3. EBC IA Requirements

Requirement	Applicability (See note)	UCR Reference	Criteria								
General Requirements	Required	5.4.6.2	Detailed requirements and associated criteria for EBC are listed in the IATP, 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									
<p>NOTE: Annotation of 'required' refers to high level requirement category. Applicability of each sub-requirement is provided in enclosure 3.</p> <p>LEGEND:</p> <table> <tr> <td>EBC</td> <td>Edge Boundary Controller</td> <td>IATP</td> <td>IA Test Plan</td> </tr> <tr> <td>IA</td> <td>Information Assurance</td> <td>UCR</td> <td>Unified capabilities Requirements</td> </tr> </table>				EBC	Edge Boundary Controller	IATP	IA Test Plan	IA	Information Assurance	UCR	Unified capabilities Requirements
EBC	Edge Boundary Controller	IATP	IA Test Plan								
IA	Information Assurance	UCR	Unified capabilities Requirements								

7.4 Other. None.

8. TEST NETWORK DESCRIPTION. The SUT was tested at JITC 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 Figure 2-2.

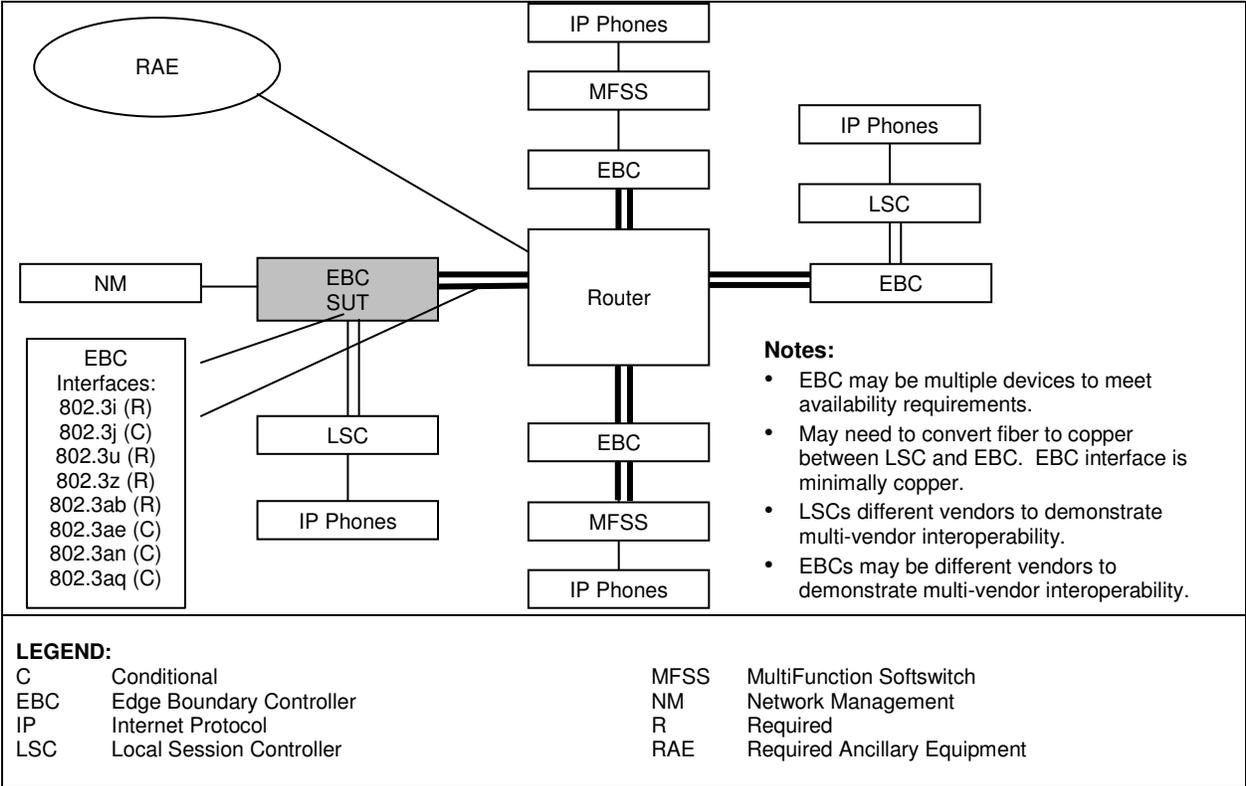


Figure 2-2. EBC Minimum Test Architecture

9. SYSTEM CONFIGURATIONS. Table 2-4 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 2-4. Tested System Configurations

CUBE on a Cisco 3845 ISR or Cisco 3945 ISR With IOS 15.1(20110111:230218) [15-1-3-17-T] EBC			
Component ¹	Release	Sub-component	Function
<u>Cisco 3845</u> , 3825, 2851, 2821, 2811, 2801 <u>Integrated Services Router</u> .	15.1 Engineering Special (C3845-ADVENTERPRISEK9_IVS-M), Version 15.1(20110111:230218) [15-1-3-17-T]	<u>CISCO3845 Cisco 3845 Integrated Services Router Chassis</u>	with 2 GbE
		<u>NM-2FE-2W</u>	2 Port FE Network Module
<u>Cisco 3945</u> , 3945E 3925E, 3925, 2951, 2921,2911,2901 <u>Integrated Services Router</u> Cisco	15.1 Engineering Special (C3900-UNIVERSALK9-M), Version 15.1(20110111:230218) [15-1-3-17-T]	<u>CISCO3945 Cisco 3945 Integrated Services Router Chassis</u>	with 3 GbE
		<u>NM-2FE-2W</u>	2 Port FE Network Module
Legend:			
ASAC	Assured Services Admission Control	GbE	Gigabit Ethernet
CUBE	Cisco Unified Border Element	IOS	Internetworking Operating System
EBC	Edge Boundary Controller	ISR	Integrated Services Router
FE	Fast Ethernet	NM	Network Management
NOTES:			
1. Components bolded and underlined were tested by JITC. The other components in the series were not tested; however, they utilize the same software and hardware and JITC analysis determined them to be functionally identical for interoperability certification purposes and they are also certified for joint use.			

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. The JITC was unable to test the Packet Transit Time requirement because it would require special test equipment that could communicate with an EBC using appropriate protocols and security processes. The 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. The vendor did submit a Packet Transit Time LoC that was reviewed by JITC. The JITC’s evaluation of the SUT’s Packet Transit Time capabilities is provided in paragraph 11.

b. Internet Protocol version 6 (IPv6). The JITC did not test the SUT’s ability to meet UCR IPv6 requirements. The vendor did submit an IPv6 LoC that was reviewed by JITC. The JITC’s evaluation of the SUT’s IPv6 capabilities is provided in paragraph 11.

c. Network Management (NM). The JITC did not test the SUT’s ability to meet UCR NM requirements. The vendor did submit an NM LoC that was reviewed by JITC. The 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 Unified Capabilities (UC) products listed on the 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 2-5.

Table 2-5. SUT Interface Requirements Status

Interface	Critical (See note 1.)	UCR Paragraph	Threshold CR/FR Requirements (See note 2.)	Status	Remarks (See note 3.)																																
WAN Interfaces																																					
1000Base-X	No	5.3.2.4 / 5.3.3.10.1.2	1-3	Certified	IEEE 802.3z																																
NM Interfaces																																					
10Base-X	No	5.3.2.4.4	4	Certified	IEEE 802.3i and IEEE 802.3j																																
100Base-X	No	5.3.2.4.4	4	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: 33%;">10Base-X</td> <td style="width: 33%;">Generic designation for 10 Mbps Ethernet</td> <td style="width: 33%;">FR</td> <td>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>Mbps</td> <td>Megabits per second</td> </tr> <tr> <td>802.3j</td> <td>IEEE Ethernet standard for 10 Mbps over fiber</td> <td>NM</td> <td>Network Management</td> </tr> <tr> <td>802.3u</td> <td>IEEE Ethernet Standard for 100 Mbps over twisted pair and fiber</td> <td>SUT</td> <td>System Under Test</td> </tr> <tr> <td>802.3z</td> <td>IEEE Ethernet standard for 1000 Mbps over fiber</td> <td>UCR</td> <td>Unified Capabilities Requirements</td> </tr> <tr> <td>CR</td> <td>Capability Requirement</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	Mbps	Megabits per second	802.3j	IEEE Ethernet standard for 10 Mbps over fiber	NM	Network Management	802.3u	IEEE Ethernet Standard for 100 Mbps over twisted pair and fiber	SUT	System Under Test	802.3z	IEEE Ethernet standard for 1000 Mbps over fiber	UCR	Unified Capabilities Requirements	CR	Capability Requirement	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	Mbps	Megabits per second																																		
802.3j	IEEE Ethernet standard for 10 Mbps over fiber	NM	Network Management																																		
802.3u	IEEE Ethernet Standard for 100 Mbps over twisted pair and fiber	SUT	System Under Test																																		
802.3z	IEEE Ethernet standard for 1000 Mbps over fiber	UCR	Unified Capabilities Requirements																																		
CR	Capability Requirement	WAN	Wide Area Network																																		

11.2 CR and 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 CRs and FRs Status

CR/FR ID	Capability/Function	Applicability (See note 1.)	UCR Paragraph	Status (See note 2.)	Remarks
1	EBC 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	This was verified through the vendor's LoC.
	Network Management	Required	5.3.2.15.3 5.3.2.17	Met	This was verified through the vendor's LoC.
	DSCP Policing	Required	5.3.2.15.4	Not Tested	See note 3.
	Codec Bandwidth Policing	Required	5.3.2.15.5	Not Tested	See note 3.
	Availability	Required	5.3.2.15.6	Met	The SUT met this requirement for the high availability without NLAS option. This was verified through the vendor's LoC.
	IEEE 802.1Q Support	Required	5.3.2.15.7	Met	
	Packet Transit Time	Required	5.3.2.15.8	Met	This was verified through the vendor's LoC.
ITU-T H.323 Support	Conditional	5.3.2.15.9	Not Tested	The SUT offers ITU-T H.323 support, however it was not tested and is not certified.	
2	AS-SIP Requirements				
	Requirements for AS-SIP Signaling Appliances	Required	5.3.4.7	Met	
	SIP Session Keep-Alive Timer	Required	5.3.4.8	Met	
	Session Description Protocol	Required	5.3.4.9	Met	
	Precedence and Preemption	Required	5.3.4.10	Met	
Calling Services	Required	5.3.4.13	Met		
3	IPv6 Requirements				
	Product Requirements	Required	5.3.5.4	Partially Met	This was verified through the vendor's LoC with the exceptions listed in note 4
4	NM Requirements				
	VVoIP NMS Interface Requirements	Required	5.3.2.4.4	Met	This was verified through the vendor's LoC.
	General Management Requirements	Required	5.3.2.17.2	Met	This was verified through the vendor's LoC.
	Requirement for FCAPS Management	Required	5.3.2.17.3	Met	This was verified through the vendor's LoC.
	NM requirements of Appliance Functions	Required	5.3.2.18	Met	This was verified through the vendor's LoC.

Table 2-6. SUT CRs and FRs Status (continued)

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. Paragraph 11 of Enclosure 2 provides detailed information pertaining to open TDRs and associated operational impacts			
3. The DISA adjudicated this discrepancy as having a low operational impact because vendors have until July 2011 to comply with this requirement.			
4. The LoC stated non-compliance with traffic engineering requirements listed in UCR 2008 Change 1 Section 5.3.5.4.11 paragraph 34. Per DISA clarification dated 21 April 2011, this requirement correlates to UCR 2008 Change 1 Section 5.3.2.15.5 (Codec Bandwidth Policing) which is a new requirement since UCR 2008, therefore the vendor has until July 2011 to comply with this requirement. DISA stated their intent to update this disparity in the next UCR errata change.			
LEGEND:			
802.1Q	IEEE VLAN tagging standard	IPv6	Internet Protocol version 6
AS-SIP	Assured Services Session Initiation Protocol	ITU-T	International Telecommunication Union -
CR	Capabilities Requirement		Telecommunication Standardization Sector
DISA	Defense Information Systems Agency	JITC	Joint Interoperability Test Command
DSCP	Differentiated Services Code Point	LoC	Letters of Compliance
EBC	Edge Boundary Controller	NM	Network Management
FCAPS	Fault, Configuration, Accounting, Performance, and Security	NMS	NM System
FR	Functional Requirement	RFC	Request for Comment
H.323	ITU-T recommendation that defines audio-visual session protocols	SIP	Session Initiation Protocol
ID	Identification	SUT	System Under Test
IEEE	Institute of Electrical and Electronics Engineers	UCR	Unified Capabilities Requirements
IPsec	IP Security	VVoIP	Voice and Video over Internet Protocol
		WAN	Wide Area Network

a. EBC Requirements

(1) AS-SIP Back-to-Back User Agent. In accordance with (IAW) Section 5.3.2.15.1 of UCR 2008 Change 1, the product shall act as an AS-SIP Back-to-Back User Agent (B2BUA) for interpreting the AS-SIP messages to meet its functions. The SUT met all requirements as an AS-SIP B2BUA.

(2) Call Processing Load. IAW Section 5.3.2.15.2 of UCR 2008 Change 1, 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 via LoC.

(3) Network Management (NM). IAW Section 5.3.2.15.3 of UCR 2008 Change 1, 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. NM requirements were met via a vendor-submitted LoC.

(4) Differentiated Services (DiffServ) Code Point (DSCP) Policing. IAW Section 5.3.2.15.4 of UCR 2008 Change 1, 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 Resource Priority Header. This was not tested at JITC; however, this represents a new feature in the UCR for which the 18-month rule applies. The vendor has until July 2011 to comply with this feature.

(5) Codec Bandwidth Policing. IAW Section 5.3.2.15.5 of UCR 2008 Change 1, 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. This was not tested at JITC; however, this represents a new feature in the UCR for which the 18-month rule applies. The vendor has until July 2011 to comply with this feature.

(6) Availability. There are four types of EBCs: High Availability with No Loss of Active Sessions (NLAS), High Availability without NLAS, Medium Availability, and Low Availability. IAW Section 5.3.2.15.6 of UCR 2008 Change 1, the EBC shall meet availability requirements as specified for the availability type. The SUT met the availability requirements for High Availability without NLAS, Medium Availability, and Low Availability with the following stipulations: High Availability without NLAS and Medium Availability are met with a dual chassis configuration, and Low Availability is met with a single chassis configuration. These requirements were met via a vendor-submitted LoC. The Low Availability requirements were met with a single chassis with a minimum mean time to repair of 3 hours or less.

(7) Institute of Electronics and Electrical Engineers (IEEE) 802.1Q Support. IAW Section 5.3.2.15.7 of UCR 2008 Change 1, the product shall be capable of supporting the IEEE 802.1Q 2-byte Tag Control Information Field 12-bit Virtual Local Area Network (VLAN) Identifier. The SUT met all requirements for IEEE 802.1Q VLAN Support.

(8) Packet Transit Time. IAW Section 5.3.2.15.8 of UCR 2008 Change 1, the product shall be capable of receiving, processing, and transmitting an UC packet within 2 ms to include executing all internal functions. The JITC was unable to test this feature because no test equipment is available to test this requirement. The JITC did not identify any issues that could be associated with packet transit time during operation of the SUT.

(9) H.323 Support. IAW Section 5.3.2.15.9 of UCR 2008 Change 1, if the EBC supports H.323 video, then the product shall be capable of processing and forwarding H.323 messages in accordance with Section 5.4, Information Assurance Requirements, of this document. This was not tested at JITC; however, because it is conditional requirement there is no operational impact.

b. Assured Services Session Initiation Protocol (SIP) Requirements

(1) Requirements for AS-SIP Signaling Appliances. IAW Section 5.3.4.7 of UCR 2008 Change 1, the EBC must meet all requirements for AS-SIP Signaling Appliances. The SUT met all requirements for AS-SIP signaling appliances.

(2) SIP session Keep-Alive Timer. IAW Section 5.3.4.8 of UCR 2008 Change 1, the AS-SIP signaling appliances must support the keep-alive mechanism for SIP sessions. The SUT met all requirements for SIP session Keep-Alive Timer.

(3) Session Description Protocol (SDP). IAW Section 5.3.4.9 of UCR 2008 Change 1, the EBC must meet the requirements for SDP. The SUT met all SDP requirements.

(4) Precedence and Preemption. IAW Section 5.3.4.10 of UCR 2008 Change 1, the EBC must meet the detailed requirements for the execution of preemption and the handling of precedence information. The SUT met all Precedence and Preemption requirements.

(5) Calling Services. IAW Section 5.3.4.10 of UCR 2008 Change 1, the EBC must meet the detailed requirements for the execution of calling services. The SUT met all calling services requirements. To insure Assured Services requirements are met, the the ASAC budgets must be configured not to exceed the maximum simultaneous call limits for each Integrated Services Router respectively as depicted in paragraph 5..

c. IPv6 Requirements. IAW Section 5.3.5.4 of UCR 2008 Change 1, the EBC must meet specified IPv6 requirements. The IPv6 requirements were verified through the vendor's LoC. The SUT met all of the critical IPv6 requirements with the minor exceptions listed below.

(1) The SUT does not comply with the traffic engineering requirements listed in section 5.3.5.4.11 paragraph 34. This paragraph states that for traffic engineering purposes, the bandwidth required per voice subscriber is calculated to be 110.0 kbps (each direction) for each IPv6 call. This represents a new feature in the UCR for which the 18-month rule applies. The vendor has until July 2011 to comply with this feature.

d. NM Requirements. IAW Sections 5.3.2.4, 5.3.2.17, and 5.3.2.18 of UCR 2008 Change 1, the EBC must meet the following NM Requirements. NM requirements were met via a vendor-submitted LoC.

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

(2) General Management Requirements. IAW Section 5.3.2.17.2 of UCR 2008 Change 1, 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. IAW Section 5.3.2.17.3 of UCR 2008 Change 1, 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. IAW Section 5.3.2.18 of UCR 2008 Change 1, the EBC must meet the NM requirements of Appliance Functions listed for an EBC. The SUT's NM LoC stated compliance to Section 5.3.2.18.

11.3 IA. The IA requirements are tested by DISA-led IA test teams and 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. The 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). The 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 testing is on the website at <http://jitc.fhu.disa.mil/tssi>. All associated data is available on the DISA Unified Capability Coordination Office (UCCO) website located at <http://www.disa.mil/ucco/>. 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 UCCO e-mail: ucco@disa.mil.

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 (FR) and Capability Requirements (CR) for EBCs are listed in Table 3-1. Detailed Information Assurance (IA) requirements are included in Reference (e) and are not listed below.

Table 3-1. EBC Capability/Functional Requirements Table

ID	Requirement	UCR Ref (UCR 2008 Change 1)	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	5.3.2.15.1 (6.b.1)	R

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

ID	Requirement	UCR Ref (UCR 2008 Change 1)	R/C
	Unavailable, or (504) Server Timeout response.		
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
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 1.	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	<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

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

ID	Requirement	UCR Ref (UCR 2008 Change 1)	R/C
27	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
28	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
29	The hostname of the SIP URI in the Contact header of a SIP request or response generated by an AS-SIPEI 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
30	The product shall support dual IPv4 and IPv6 stacks as described in RFC 4213.	5.3.5.4 (1)	R
31	Dual stack end points or Call Control Agents shall be configured to choose IPv4 over IPv6.	5.3.5.4 (1.1)	R
32	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
33	The product shall support the IPv6 format as described in RFC 2460 and updated by RFC 5095.	5.3.5.4 (2)	R
34	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
35	The product shall support Path MTU Discovery (RFC 1981).	5.3.5.4.1 (4)	R
36	The product shall support a minimum MTU of 1280 bytes (RFC 2460 and updated by RFC 5095).	5.3.5.4.1 (5)	R
37	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
38	The product shall not use the Flow Label field as described in RFC 2460.	5.3.5.4.2 (7)	R
39	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
40	The product shall not modify the Flow Label field when forwarding packets.	5.3.5.4.2 (7.2)	R
41	The product shall be capable of ignoring the Flow Label field when receiving packets.	5.3.5.4.2 (7.3)	R
42	The product shall support the IPv6 Addressing Architecture as described in RFC 4291.	5.3.5.4.3 (8)	R
43	The product shall support the IPv6 Scoped Address Architecture as described in RFC 4007.	5.3.5.4.3 (9)	R
	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
44	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
45	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
46	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
47	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

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

ID	Requirement	UCR Ref (UCR 2008 Change 1)	R/C
48	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
49	The product shall support the ability to configure the product to ignore Redirect messages.	5.3.5.4.5.1 (11.6)	R
50	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
51	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
52	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
53	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
54	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
55	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
56	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
57	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)	C
58	The product shall support manual assignment of IPv6 addresses.	5.3.5.4.6 (12.3)	R
59	The product shall support the ICMPv6 as described in RFC 4443.	5.3.5.4.7 (14)	R
60	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
61	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
62	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
63	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
64	The product shall support MLD as described in RFC 2710.	5.3.5.4.8 (21)	R
65	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
66	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
67	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
68	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
69	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
70	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

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

ID	Requirement	UCR Ref (UCR 2008 Change 1)	R/C
71	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
72	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
73	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
74	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
75	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
76	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
77	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
78	If RFC 4301 is supported, the product shall support the Encapsulating Security Payload (ESP) Protocol in accordance with RFC 4303.	5.3.5.4.9 (22.12)	C
79	If RFC 4303 is supported, the product shall be capable of enabling anti-replay.	5.3.5.4.9 (22.12.1)	C
80	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
81	If RFC 4301 is supported, the product shall support the cryptographic algorithms as defined in RFC 4308 for Suite Virtual Private Network (VPN)-B	5.3.5.4.9 (22.13)	C
82	If RFC 4301 is supported, the product shall support the use of AES-CBC with 128-bits keys for encryption.	5.3.5.4.9 (22.13.1)	C
83	If RFC 4301 is supported, the product shall support the use of HMAC-SHA1-96 for (Threshold) and AES-XCBC-MAC-96 (UCR 2010).	5.3.5.4.9 (22.13.2)	C
84	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
85	If the product supports IKEv2, it shall be capable of configuring the maximum User Datagram Protocol (UDP) message size.	5.3.5.4.9 (22.14.1)	C
86	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
87	If the product supports IKEv2, the product shall reject initial IKE messages unless they contain a Notify Payload of type COOKIE.	5.3.5.4.9 (22.14.5)	C
88	If the product supports IKEv2, the product shall close an SA instead of rekeying when its lifetime expires if there has been no traffic since the last rekey.	5.3.5.4.9 (22.14.6)	C
89	If the product supports IKEv2, the product shall not use the Extensible Authentication Protocol (EAP) method for IKE authentication.	5.3.5.4.9 (22.14.7)	C
90	If the product supports IKEv2, the product shall limit the frequency to which it responds to messages on UDP port 500 or 4500 when outside the context of a security association known to it.	5.3.5.4.9 (22.14.8)	C
91	If the product supports IKEv2, the product shall not support temporary IP addresses or respond to such requests.	5.3.5.4.9 (22.14.9)	C
92	If the product supports IKEv2, the product shall support the IKEv2 cryptographic algorithms defined in RFC 4307.	5.3.5.4.9 (22.14.10)	C
93	If the product supports IKEv2, the product shall support the VPN-B Suite as defined in RFC 4308 and RFC 4869 (UCR 2010).	5.3.5.4.9 (22.14.11)	C
94	If RFC 4301 is supported, 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.	5.3.5.4.9 (22.15)	C
95	If RFC 4301 is supported, the product shall support the ISAKMP as defined in RFC 2408.	5.3.5.4.9 (22.16)	C
96	If the product supports the IPSec Authentication Header Mode, the product shall support the IP Authentication Header (AH) as defined in RFC 4302.	5.3.5.4.9 (22.17)	C

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

ID	Requirement	UCR Ref (UCR 2008 Change 1)	R/C
97	If RFC 4301 is supported, the product shall support manual keying of IPSec.	5.3.5.4.9 (22.18)	C
98	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
99	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
100	If the product uses URIs, the product shall use the URI syntax described in RFC 3986.	5.3.5.4.10 (32)	C
101	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
102	The product shall forward packets using the same IP Version as the Version in the received packet.	5.3.5.4.12 (37)	R
103	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 1	5.3.5.4.13 (39)	C
104	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
105	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
106	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
107	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
108	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
109	The product shall be able to provide topology hiding (e.g., NAT) for IPv6 packets as described in Section 5.4, Information Assurance Requirements.	5.3.5.4.13 (45)	R
110	If the product supports Remote Authentication Dial In User Service (RADIUS) authentication, the product shall support RADIUS as defined in RFC 3162.	5.3.5.4.14 (47)	C
111	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
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	5.3.2.17.2	R

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

ID	Requirement	UCR Ref (UCR 2008 Change 1)	R/C
	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.		
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
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	Faults will be reported IAW RFCs 1215 and 3418.	5.3.2.18.1	R
129	Standard CM information shall be presented IAW RFCs 1213 and 3418.	5.3.2.18.1	R
130	Standard PM information shall be presented IAW RFCs 1213 and 3418.	5.3.2.18.1	R
131	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	R
132	SNMPv3 format.	5.3.2.18.1	R
133	The standard CM MIB variables shown in Table 5.3.2.18-1, Standard CM MIB Variables, are required for each EBC.	5.3.2.18.1.2	R
134	The standard PM MIB variables shown in Table 5.3.2.18-2, Standard PM MIB Variables, are required for each EBC per interface.	5.3.2.18.1.3	R
135	The standard TRAPs shown in Table 5.3.2.18-3, Standard TRAPs Required for EBC.	5.3.2.18.1.4	R

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

LEGEND:	
802.1Q	IEEE VLAN tagging standard
AES	Advanced Encryption Standard
AH	Authentication Header
AS-SIP	Assured Services Session Initiation Protocol
B2BUA	Back-to-Back User Agreement
C	Conditional
CCA-ID	Call Control Agent Identification?
CE	Customer Edge
CID	Craft Input Device
CM	
DAD	Duplicate Address Detection
DISA	Defense Information Systems Agency
DISN	Defense Information System Network
DoS	Denial of Service
DSCP	Differentiated Services Code Point
E2E	End to End
EBC	Edge Boundary Controller
EI	End Instrument
EMS	Element Management System
ESP	Encapsulating Security Payload
FCAPS	Fault, Configuration, Accounting, Performance, and Security
H.323	ITU-T recommendation that defines audio-visual session protocols
HMAC	Hash-based Message Authentication Code
IAW	in accordance with
ICMP	Internet Control Message Protocol
ICMPv6	Internet Control Message Protocol for IPv6
IEEE	Institute of Electrical and Electronics Engineers
IKE	Internet Key Exchange
IP	Internet Protocol
IPSEC	Internet Protocol Security
IPv4	Internet Protocol version 4
IPv6	Internet Protocol version 6
ISAKMP	Internet Security Association and Key Management Protocol
ITU-T	ITU-T recommendation that defines audio-visual session protocols
kbps	kilobits per second
LSC	Local Session Controller
MAC	Media Access Control
Mbps	Megabits per second
MFSS	Multifunction Softswitch
MIB	Management Information Base
MLD	Multicast Listener Discover
ms	millisecond
MTOSI	Multi-Technology Operations System(s) Interface
MTU	Maximum Transmission Unit
NAPT	Network Address Port Translation
NAT	Network Address Translation
NLAS	No Loss of Active Sessions
NM	Network Management
OA&M	Operations, Administration, and Maintenance
OSI	Open Systems Interconnect
PM	
R	Required
RADIUS	Remote Authentication Dial In User Service
RFC	Request for Comments
RPH	Resource-Priority Header
SA	Security Association
SAD	Security Association Database
SDP	Session Description Protocol
SHA1	
SIP	Session Initiation Protocol
SLAAC	Stateless Address Autoconfiguration
SPD	Security Policy Database
SNMPv3	Simple Network Management Protocol version 3
TCI	Tag Control Information
TCP/IP	Transmission Control Protocol/Internet Protocol
TLS	Transport Layer Security
TTL	Time to Live
UC	Unified Capabilities
UCR	Unified Capabilities Requirements
URI	Uniform Resource Identifier
VID	VLAN Identification
VLAN	Virtual Local Area Network
VPN	Virtual Private Network
VVoIP	Voice and Video over Internet Protocol
WAN	Wide Area Network
XML	Extensible Markup Language