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

IN REPLY REFER TO: Joint Interoperability Test Command (JTE) **13 Jan 15**

MEMORANDUM FOR DISTRIBUTION

SUBJECT: Joint Interoperability Certification of the Hewlett Packard (HP) 5900 with Software Release 7.1

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

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

2. **Conditions of Certification.** The HP 5900 Switch Series, Comware software release 7.1; hereinafter referred to as the System Under Test (SUT), meets the critical requirements of the Unified Capabilities Requirements (UCR), Reference (c), and is certified for joint use as an Assured Services Local Area Network (ASLAN) Core and Distribution Switch with the conditions described in Table 1. This certification expires upon changes that affect interoperability, but no later than three years from the date of the UC Approved Products List (APL) memorandum.

Table 1. Conditions

Condition	Operational Impact	Remarks
UCR Waivers		
None.		
Conditions of Fielding		
SUT is not compliant with IP6-000820. IPSec is not approved and not part of this certification until the SUT is compliant with IP6-000820.	Minor	See note 1.
Open Test Discrepancies		
The SUT does not meet the IP6-000730 requirement. The SUT is not capable of enabling and disabling the ability of the product to send an ICMP message informing the sender that an outbound packet was discarded.	None.	See note 2.

Table 1. Conditions (continued)

Condition	Operational Impact	Remarks
SUT is not compliant with IP6-000770 - The vendor is not compliant in providing management control to allow an administrator to enable or disable the ability of the product to send an IKE notification of an INVALID_SELECTORS as stated in the RFC 4301.	Minor	See note 3.
SUT is not compliant with IP6-000820. The vendor LoC requires for the SUT to prevent a Denial of Services (DoS) attack on the initiator of an IKE_SA, the initiator shall accept multiple responses to its first message, treat each as potentially legitimate, respond to it, and then discard all the invalid half-open connections when it receives a valid cryptographically protected response to any one of its requests. Once a cryptographically valid response is received, all subsequent responses shall be ignored whether or not they are cryptographically valid.	Minor	See note 1.

NOTES:
1. DISA has accepted and approved the vendor's POA&M and adjudicated this discrepancy as having a minor operational impact with the POA&M and CoF.
2. DISA has adjudicated this discrepancy as having no operational impact because this requirement has been marked for removal in the draft UCR Guide 2013 Change 1.
3. DISA has adjudicated this discrepancy as having a minor operational impact without a vendor POA&M since the SUT does not utilize IKE in an ASLAN environment.

LEGEND:

ASLAN	Assured Services Local Area Network	LACP	Link Aggregation Control Protocol
CoF	Condition of Fielding	LoC	Letter of Compliance
DISA	Defense Information Systems Agency	POA&M	Plans of Action and Milestones
IKE_SA	Internet Key Exchange Security Association	RFC	Request for Comment
IP	Internet Protocol	SUT	System Under Test
IPSec	IP Security	UCR	Unified Capabilities Requirements
IPv6	Internet Protocol Version 6		

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

Table 2. ASLAN Interface Status

Interface	Applicability			Threshold CRs/FRs (See note 1.)	Status	Remarks
	Co	D	A			
Network Management Interfaces (See note 2.)						
IEEE 802.3i (10BaseT UTP)	C	C	C	1 and 3	Met	
IEEE 802.3u (100BaseT UTP)	C	C	C	1 and 3	Met	
IEEE 802.3ab (1000BaseT UTP)	C	C	C	1 and 3	Met	
Access (User) Interfaces (See note 2.)						
IEEE 802.3i (10BaseT UTP)	C	C	R	1, 2, and 3	Not Tested	(See note 3.)
IEEE 802.3u (100BaseT UTP)	R	R	R	1, 2, and 3	Not Tested	(See note 3.)
IEEE 802.3u (100BaseFX)	C	C	R	1, 2, and 3	Not Tested	(See note 3.)
IEEE 802.3ab (1000BaseT UTP)	C	C	R	1, 2, and 3	Met	(See note 4.)
IEEE 802.3z (1000BaseX Fiber)	R	R	R	1, 2, and 3	Not Tested	(See note 5.)
IEEE 802.3ae (10GBaseX) (C)	O	O	O	1, 2, and 3	Met	(See note 4.)
Uplink (Trunk) Interfaces (See note 2.)						
IEEE 802.3u (100BaseT UTP)	R	R	R	1, 2, 3, and 4	Not Tested	(See note 3.)
IEEE 802.3u (100BaseFX)	C	C	R	1, 2, 3, and 4	Not Tested	(See note 3.)
IEEE 802.3ab (1000BaseT UTP)	C	C	R	1, 2, 3, and 4	Not Tested	(See note 4.)
IEEE 802.3z (1000BaseX Fiber)	R	R	R	1, 2, 3, and 4	Not Tested	(See note 4.)
IEEE 802.3ae (10GBaseX)	O	O	O	1, 2, 3, and 4	Met	
IEEE 802.3ba (40GbaseX)	O	O	O	1, 2, 3, and 4	Met	(See note 6.)
IEEE 802.3ba (100GbaseX)	O	O	O	1, 2, 3, and 4	Not Tested	(See note 3.)

Table 2. ASLAN Interface Status (continued)

Interface	Applicability			Threshold CRs/FRs (See note 1.)	Status	Remarks
	Co	D	A			
Wireless LAN Interfaces						
IEEE 802.11a IAW 802.11-2007 – 5 GHz	N/A	N/A	C	1 and 5	Not Tested	(See note 3.)
IEEE 802.11b IAW 802.11-2007 – 2.4GHz	N/A	N/A	C	1 and 5	Not Tested	(See note 3.)
IEEE 802.11g IAW 802.11-2007 – 2.4 GHz	N/A	N/A	C	1 and 5	Not Tested	(See note 3.)
IEEE 802.11n-2009 – 2.4 GHz and 5 GHz	N/A	N/A	C	1 and 5	Not Tested	(See note 3.)
IEEE 802.16-2012	N/A	N/A	C	1 and 5	Not Tested	(See note 3.)

NOTES:
1. The SUT high-level CR and FR ID numbers depicted in the Threshold CRs/FRs column can be cross-referenced in Table 3. These high-level CR/FR requirements refer to a detailed list of requirements provided in Enclosure 3.
2. Core and Distribution products must minimally support 100Base-X (802.3u) and 1000Base-X (802.3z). Access products must minimally support one of the following standards: 802.3i (10BaseT), 802.3j (10BaseF), 802.3u (100BaseT/F), 802.3z (1000BaseF), or 802.3ab (1000BaseT). Other rates and standards may be provided as conditional interfaces.
3. The SUT does not support this interface.
4. Traffic was successfully transmitted and received between the SUT and the test instrumentation. Therefore, this interface is included in the certification.
5. Although the SUT supports this interface, it was not tested and is not covered under this certification.
6. This interface was tested using bi-directional traffic between the SUT and the Brocade VDX6740.

LEGEND:

802.3ab	1000BaseT Gbps Ethernet over Twisted Pair at 1 Gbps	A	Access
		ASLAN	Assured Services Local Area Network
802.3ae	10 Gbps Ethernet	C	Conditional
802.3ba	40 and 100 Gigabit Ethernet Architecture	Co	Core
802.3i	10BaseT 10 Mbps Ethernet over Twisted Pair	CRs	Capability Requirements
802.3u	Standard for carrier sense multiple access with collision detection at 100 Mbps	D	Distribution
		FRs	Functional Requirements
		Gbps	Gigabits per second
802.3z	Gigabit Ethernet Standard	GHz	GigaHertz
10BaseT	10 Mbps (Baseband Operation, Twisted Pair) Ethernet	ID	Identification
		IEEE	Institute of Electrical and Electronics Engineers
100BaseT	100 Mbps (Baseband Operation, Twisted Pair) Ethernet	IP	Internet Protocol
		Mbps	Megabits per second
100BaseFX	100 Mbps Ethernet over Fiber	N/A	Not Applicable
1000BaseT	1000 Mbps (Baseband Operation, Twisted Pair) Ethernet	O	Optional
		R	Required
1000BaseX	1000 Mbps Ethernet over Fiber or Copper	SUT	System Under Test
10GBaseX	10000 Mbps Ethernet over Fiber or Copper	UTP	Unshielded Twisted Pair

Table 3. ASLAN Capability Requirements and Functional Requirements Status

CR/FR ID	UCR Requirement (High-Level) (See note 1.)	UCR 2013 Reference	Status
1	General LAN Switch and Router Product Requirements (R)	7.2.1	Partially Met (See notes 2 and 3.)
2	LAN Switch and Router Redundancy Requirements (R)	7.2.2	Met
3	LAN Product Requirements Summary (R)	7.2.3	Met
4	Multiprotocol Label Switching in ASLANs (O)	7.2.4	Not Tested
5	Wireless LAN Requirements (C)	7.3	Not Tested

Table 3. ASLAN Capability Requirements and Functional Requirements Status (continued)

NOTES:
1. The annotation of 'required' refers to a high-level requirement category. The applicability of each sub-requirement is provided in Enclosure 3.
2. The SUT met the requirements with the exceptions noted in Table 1. DISA adjudicated these exceptions as minor.
3. Security is tested by a DISA-led Information Assurance test team and the results published in a separate report, Reference (e).

LEGEND:

ASLAN	Assured Services Local Area Network	LAN	Local Area Network
C	Conditional	O	Optional
CR	Capability Requirement	R	Required
DISA	Defense Information Systems Agency	SUT	System Under Test
FR	Functional Requirement	UCR	Unified Capabilities Requirements
ID	Identification		

Table 4. UC APL Product Summary

Product Identification			
Product Name	Hewlett Packard (HP) 5900		
Software Release	Release 7.1.045		
UC Product Type(s)	ASLAN Core and Distribution IP Switch		
Product Description	ASLAN Core/Distribution Switch		
Product Components (See note 1.)	**Component Name**	**Version**	**Remarks**
ASLAN Core/Distribution Switch	5900	Release 7.1.045	

NOTES:
1. The detailed component and subcomponent list is provided in Enclosure 3.

LEGEND:

APL	Approved Products List	IP	Internet Protocol
ASLAN	Assured Services Local Area Network	UC	Unified Capabilities

4. **Test Details.** This certification is based on interoperability testing, review of the vendor's Letters of Compliance (LoC), and DISA Certifying Authority (CA) recommendation for inclusion on the UC APL. Testing was conducted at JITC, Fort Huachuca, Arizona, from 25 August through 26 September 2014 using test procedures derived from Reference (d). Review of the vendor's LoC was completed on 29 August 2014. DISA adjudication of outstanding TDRs was completed on 10 December 2014. DISA accepted and approved the vendor's POA&Ms and adjudicated the TDRs as having minor operational impact. Information Assurance testing was conducted by JITC-led IA test teams and the results published in a separate report, Reference (e). Enclosure 2 documents the test results and describes the tested network and system configurations. Enclosure 3 provides a detailed list of the interface, capability, and functional requirements.

5. **Additional Information.** JITC distributes interoperability information via the JITC Electronic Report Distribution (ERD) system, which uses Sensitive but Unclassified IP Data (formerly known as NIPRNet) e-mail. Interoperability status information is available via the JITC System Tracking Program (STP). STP is accessible by .mil/.gov users at https://stp.fhu.disa.mil/. Test reports, lessons learned, and related testing documents and references are on the JITC Joint Interoperability Tool (JIT) at https://jit.fhu.disa.mil/. Due to the

sensitivity of the information, the Information Assurance Accreditation Package (IAAP) that contains the approved configuration and deployment guide must be requested directly from the Unified Capabilities Certification Office (UCCO), e-mail: disa.meade.ns.list.unified-capabilities-certification-office@mail.mil. All associated information is available on the DISA UCCO website located at http://www.disa.mil/Services/Network-Services/UCCO.

6. **Point of Contact (POC).** The JITC point of contact is Mr. Cary Hogan, commercial telephone (520) 538-2589, DSN telephone 879-2589; e-mail address cary.v.hogan.civ@mail.mil; mailing address Joint Interoperability Test Command, ATTN: JTE (Mr. Cary Hogan) P.O. Box 12798, Fort Huachuca, AZ 85670-2798. The UCCO tracking number for the SUT is 1330903.

FOR THE COMMANDER:

3 Enclosures a/s

for RIC HARRISON
Chief
Networks/Communications and UC Portfolio

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

ADDITIONAL REFERENCES

(c) Office of the Department of Defense Chief Information Officer, "Department of Defense Unified Capabilities Requirements 2013, Errata 1," 1 July 2013
(d) Joint Interoperability Test Command, "Assured Services Local Area Network (ASLAN) Test Procedures Version 1.0 for Unified Capabilities Requirements (UCR) 2013 Errata 1," May 2014
(e) Joint Interoperability Test Command, "Information Assurance (IA) Assessment Report for Hewlett Packard (HP) 5900 Release (Rel.) 7.1 (Tracking Number 1330903)," Draft

CERTIFICATION SUMMARY

1. SYSTEM AND REQUIREMENTS IDENTIFICATION. The Hewlett Packard (HP) 5900 Series, Assured Services Local Area Network (ASLAN), Comware Software Release 7.1.045 is hereinafter referred to as the System Under Test (SUT). Table 2-1 depicts the SUT identifying information and requirements source.

Table 2-1. System and Requirements Identification

System Identification	
Sponsor	United States Army
Sponsor Point of Contact	PM I3C2, POC: Mr. Jordan Silk, USAISEC TIC, Building 53302, Fort Huachuca, Arizona 85613; e-mail: jordan.r.silk.civ@mail.mil.
Vendor Point of Contact	Stuart Alexander, Hewlett Packard, e-mail: stuart.m.alexander@hp.com
System Name	Hewlett Packard 5900
Increment and/or Version	Release 7.1.045 2310
Product Category	Assured Services Local Area Network (ASLAN) Core and Distribution Switch
System Background	
Previous certifications	None
Tracking	
UCCO ID	1330903
System Tracking Program ID	4949
Requirements Source	
Unified Capabilities Requirements	Unified Capabilities Requirements 2013, Errata 1
Remarks	None
Test Organization(s)	Joint Interoperability Test Command, Fort Huachuca, Arizona

LEGEND:

ASLAN	Assured Services Local Area Network	TIC	Technology Integration Center
ID	Identification	UCCO	Unified Capabilities Connection Office
OS	Operating System	USAISEC	United States Army Information Systems Engineering Command
PM	Program Manager		
POC	Point of Contact		

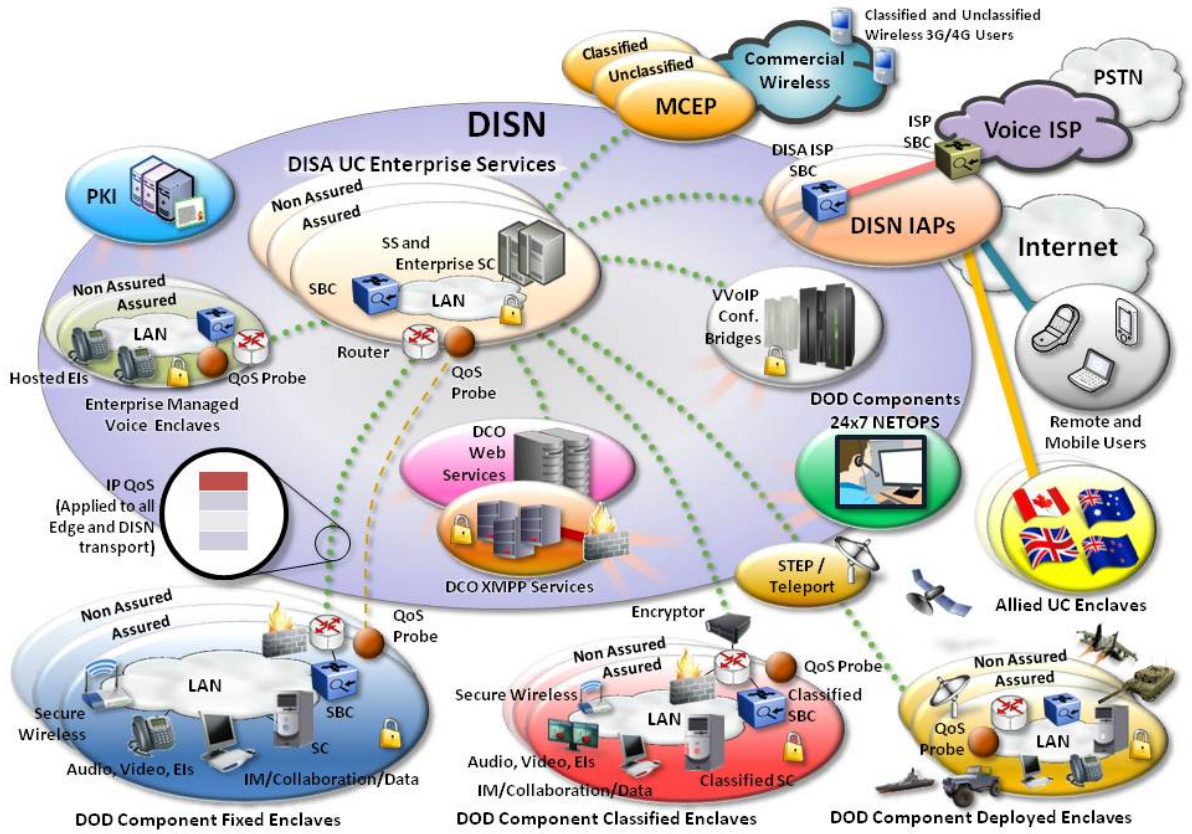
2. SYSTEM DESCRIPTION. The Unified Capabilities Requirements (UCR) 2013, Errata 1, defines two types of Local Area Networks (LANs): Assured Services Local Area Networks (ASLANs) and non-ASLANs. The Unified Capabilities (UC) LAN components are Core, Distribution, and Access switches. The core layer is a high-speed switching backbone designed to switch packets as quickly as possible. The distribution layer is the demarcation point between the access and core layers. The distribution layer helps to define and differentiate the core, provides boundary definition, and is the place at which packet manipulation can take place. The SUT is an ASLAN Core and Distribution switch providing Ethernet switching and routing capabilities with Quality of Service (QoS) capabilities for voice, video, and data networking environments over 48 SFP+ ports which can be configured as 1 Gigabit per second (Gbps) or 10Gbps and four 40Gbps QSFP+ interfaces.

3. OPERATIONAL ARCHITECTURE. The UC architecture is a two-level network hierarchy consisting of Defense Information Systems Network (DISN) backbone switches and Service/Agency installation switches. The Department of Defense (DoD), Chief Information

Officer (CIO) and Joint Staff policy and subscriber mission requirements determine which type of switch can be used at a particular location. The UC architecture, therefore, consists of several categories of switches. Figure 2-1 depicts the notional operational UC architecture in which the SUT may be used.

4. TEST CONFIGURATION. The test team tested the SUT at the Joint Interoperability Test Command (JITC), Fort Huachuca, Arizona in a manner and configuration similar to that of a notional operational environment. The system's required functions and features were tested using the test configuration depicted in Figure 2-3. Testing of the ASLAN components was conducted heterogeneously with Cisco Systems UC APL certified products. Figure 2-3 depicts a test network configuration typically used for Phase 2, and is performed by placing the SUT components into an ASLAN which is produced by a different manufacturer. SUT testing used in Phase 2 testing verifies the interoperability of the ASLAN components within Voice and Video over IP network (VVoIP). Information Assurance testing used the same configuration.

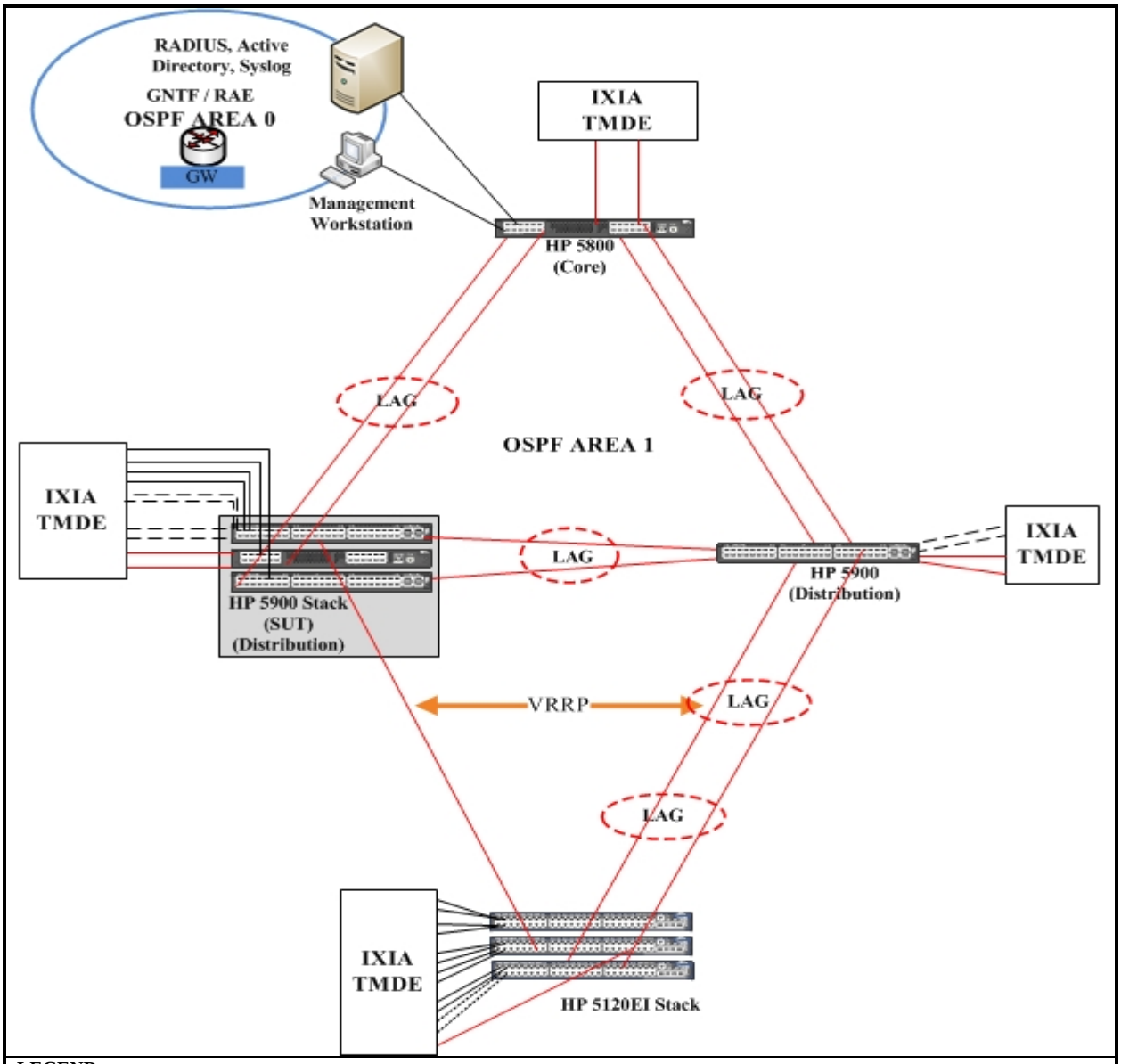
5. METHODOLOGY. Testing was conducted using ASLAN requirements derived from the UCR 2013, Errata 1, Reference (c), and ASLAN test procedures, Reference (d). In addition to testing, an analysis of the vendor's Letters of Compliance (LoC) verified that letter "R" requirements have been met. Any discrepancies noted were written up in Test Discrepancy Reports (TDRs). The vendor submitted Plan of Action and Milestones (POA&M) as required. The remaining open TDRs were adjudicated by DISA as minor. Any new discrepancy noted in the operational environment will be evaluated for impact on the existing certification. These discrepancies will be adjudicated to the satisfaction of DISA via a vendor POA&M, which will address all new critical TDRs within 120 days of identification.



LEGEND:

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

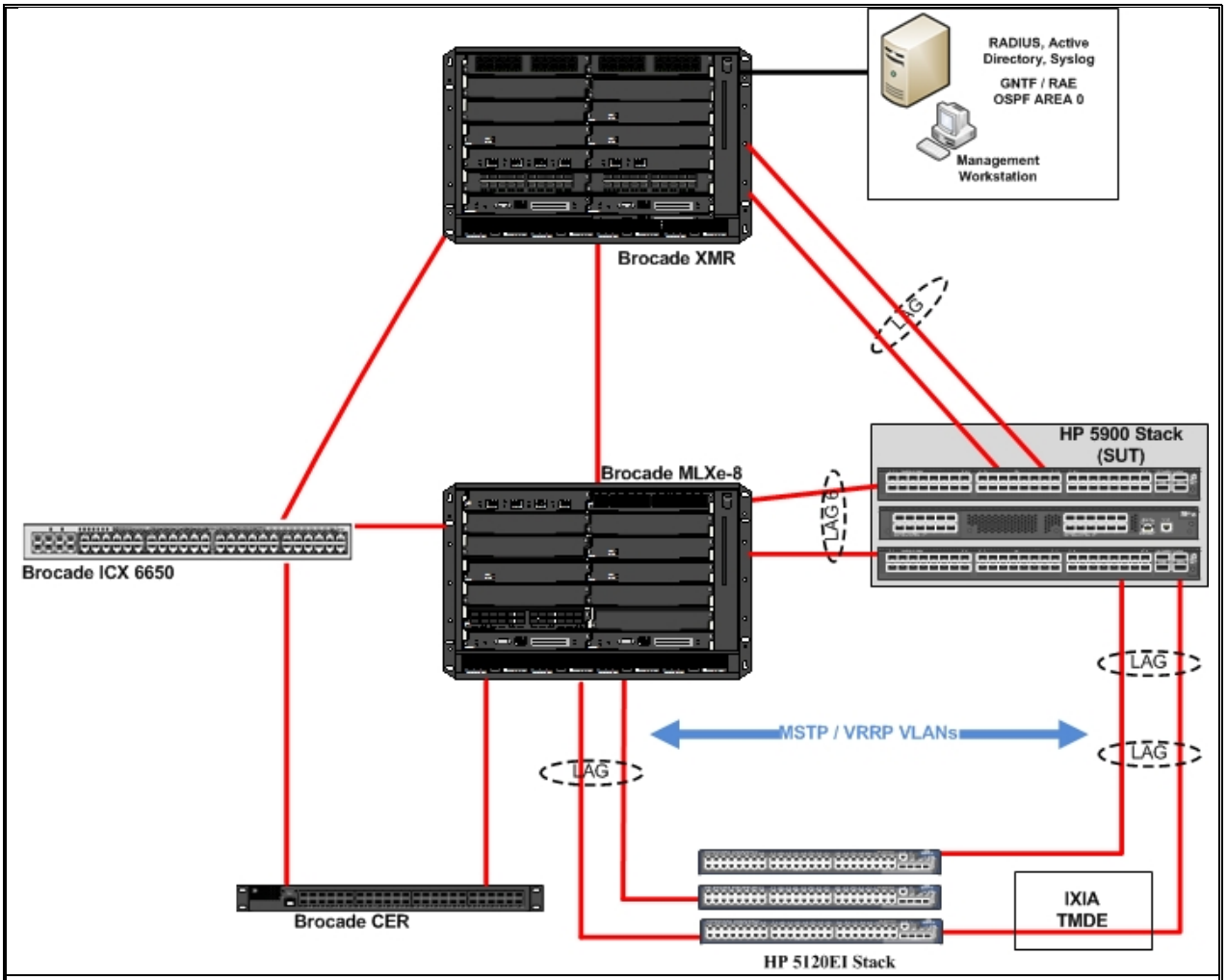
Figure 2-1. Notional UC Network Architecture



LEGEND:

GIG	Global Information Grid	RADIUS	Remote Dial-In User Service
GNTF	GIG Network Test Facility	RAE	Required Ancillary Equipment
GW	Gateway	SUT	System Under Test
HP	Hewlett Packard	TMDE	Test Measurement and Diagnostic Equipment
LAG	Link Aggregation Group	VRRP	Virtual Router Redundancy Protocol
OSPF	Open Shortest Path First		

Figure 2-2. Interoperability Homogeneous Test Configuration



LEGEND:

CER	Customer Edge Router	OSPF	Open Shortest Path First
GIG	Global Information Grid	RADIUS	Remote Dial-In User Service
GNTF	GIG Network Test Facility	RAE	Required Ancillary Equipment
GW	Gateway	SUT	System Under Test
HP	Hewlett Packard	TMDE	Test Measurement and Diagnostic Equipment
LAG	Link Aggregation Group	VLAN	Virtual Local Area Network
MSTP	Multiple Spanning Tree Protocol	VRRP	Virtual Router Redundancy Protocol

Figure 2-3. Interoperability Heterogeneous Test Configuration

6. INTEROPERABILITY REQUIREMENTS, RESULTS, AND ANALYSIS. The interface, Capability Requirements (CR) and Functional Requirements (FR), Information Assurance (IA), and other requirements for UC ASLAN are established by UCR 2013, Errata 1, sections 4, and 5, and 7.2.

a. The UCR 2013, Errata 1, section 7.2.1 includes the General LAN Switch and Router Product Requirements. The Core, Distribution, and Access products shall be capable of meeting the following parameters:

(1) The general requirements are listed in the subparagraphs below.

Non-blocking. All Core, Distribution, and Access products shall be non-blocking for their ports based on the following traffic engineering. Non-blocking is defined as the capability to send and receive a mixture of 64 to 1518 byte packets at full duplex rates from ingress ports to egress ports through the component's backplane without losing any packets. In a non-blocking switch, all ports can run at full wire speed without any loss of packets. Blocking factor is defined as the ratio of all traffic to non-blocked traffic (i.e., a blocking factor of 2-to-1 means that 50 percent of the traffic must be non-blocking). The blocking factor includes all hardware and software components. Each Core, Distribution, and Access product has up to three levels of performance: Minimum, Medium, and Maximum. The SUT met this requirement with testing and the vendor's LoC.

(a) Non-blocking results are contained in Enclosure 3, Table 3-3.

2. 1. Access Products. Access products shall not have a blocking factor that exceeds 8 to 1 (minimum). Medium performance level Access products shall not have a blocking factor that exceeds 2 to 1. Maximum performance level Access products shall be non-blocking. This requirement does not apply to the SUT as a Core and Distribution switch.

3. Distribution and Core Products. These products shall not have a blocking factor that exceeds 2 to 1 (minimum). Medium performance level products shall not have a blocking factor that exceeds 1.5 to 1. Maximum performance level products shall be non-blocking. The non-blocking test results for the SUT met the maximum performance level for a UC ASLAN Core and Distribution products.

(b) Latency. All Core, Distribution, and Access products shall have the capability to transport prioritized packets (media and signaling) as follows. The latency shall be achievable over any five-minute period measured from ingress ports to egress ports under congested conditions. A congested condition is defined as 100 percent bandwidth utilization. Prioritized packets are defined as packets having a service class above best effort. Voice packets may have no more than 2 milliseconds (ms) latency. Voice and video signaling packets may have no more than 2 ms latency. Video packets may have no more than 10 milliseconds (ms) latency. The SUT met this requirement with testing. The SUT measured latencies are shown in Table 2-2.

Table 2-2. SUT Measured Latency

Interface	SUT Measured Latency	UCR Requirement for Voice/Video
10BaseT	Not Tested (See note 1.)	2 ms / 10 ms
100BaseT	Not Tested (See note 1.)	2 ms / 10 ms
1000BaseX	.007 ms voice/.007 ms video latency	2 ms / 10 ms
10000BaseX	.002 ms voice/.002 ms video latency	2 ms / 10 ms
40000BaseX	.003 ms voice/.003 ms video latency	2 ms / 10 ms
100000BaseX	Not Tested (See note 1.)	2 ms / 10 ms

NOTES:
1. The SUT does not support this interface.

LEGEND:

JITC	Joint Interoperability Test Command	SUT	System Under Test
ms	millisecond	UCR	Unified Capabilities Requirements

(c) Jitter. All Core, Distribution, and Access products shall have the capability to transport prioritized packets (media and signaling) as follows. The jitter shall be achievable over any five-minute period measured from ingress ports to egress ports under congested conditions. Congested condition is defined as 100 percent bandwidth utilization. Voice packets may have no more than 1 ms jitter. Video packets may have no more than 10 ms jitter. The SUT met this requirement with testing. The SUT measured jitter for each interface is shown in Table 2-3.

Table 2-3. SUT Measured Jitter

Interface	SUT Measured Jitter	UCR Requirement for Voice/Video
10BaseT	Not Tested. (See note 1.)	1 ms / 10 ms
100BaseT	Not Tested. (See note 1.)	1 ms / 10 ms
1000BaseX	.003 ms voice/.001 ms video	1 ms / 10 ms
10000BaseX	.017 ms voice/.016 ms video	1 ms / 10 ms
40000BaseX	.002 ms voice/.003 ms video	1 ms / 10 ms
100000BaseX	Not Tested. (See note 1.)	1 ms / 10 ms

NOTES:
1. The SUT does not support this interface.

LEGEND:
ms millisecond UCR Unified Capabilities Requirements
SUT System Under Test

(d) Packet Loss. All Core, Distribution, and Access products shall have the capability to transport prioritized packets (media and signaling) as follows. The packet loss shall be achievable over any five-minute period measured from ingress ports to egress ports under congested conditions. Congested condition is defined as 100 percent bandwidth utilization. The SUT met this requirement with testing. The SUT measured packet loss for each interface is shown in Table 2-4.

Table 2-4. SUT Measured Packet Loss

Interface	SUT Measured Packet Loss				UCR Requirement			
	Voice	Video	Preferred Data	Best Effort Data	Voice	Video	Preferred Data	Best Effort Data
10BaseT	Not Tested. (See note 1.)				0.015%	0.05%	.005%	No minimum requirement in the UCR
100BaseT	Not Tested. (See note 1.)				0.015%	0.05%	.005%	
1000BaseX	0.00%	0.00%	0.00%	0.00%	0.015%	0.05%	.005%	
10000BaseX	0.00%	0.00%	0.00%	0.00%	0.015%	0.05%	.005%	
40000BaseX	0.00%	0.00%	0.00%	0.00%	0.015%	0.05%	.005%	
100000BaseX	Not Tested. (See note 1.)				0.015%	0.05%	.005%	

NOTES:
1. The SUT does not support this interface.

LEGEND:
SUT System Under Test UCR Unified Capabilities Requirements

(2) Port Interface Rates Requirements

(a) Minimally, Core and Distribution Products shall support the following interface rates, other rates and Institute of Electronics and Electrical Engineers (IEEE) standards may be provided as optional interfaces. Rates specified are the theoretical maximum data bit rate specified for Ethernet; link capacity and effective throughput is influenced by many factors. For

calculation purposes, link capacities are to be calculated IAW definitions contained in Request for Comments (RFC) 2330 and RFC 5136. Network Management (NM) interfaces are defined in Section 2.19. The product must minimally support the following interfaces. The SUT supports 1000Mbps as well as 10Gpbs and 40Gbps. This requirement does not apply to the SUT as a Core and Distribution switch. The SUT met this requirement with testing and the vendor's LoC for the 10/100/1000 Mbps interfaces.

- 100 Mbps in accordance with (IAW) IEEE 802.3u (for interconnection between the distribution-core and distribution-access)
- 1000 Mbps IAW IEEE 802.3z (for interconnection between the core to WAN, distribution-core, and distribution-access)

(b) Minimally, access products shall provide one of the following user-side interface rates (other rates and IEEE standards may be provided as optional interfaces). The SUT met the following requirements with the following minor exception. This requirement does not apply to the SUT as a Core and Distribution switch. However, the 1000 Mbps IAW IEEE 802.3ab interface was tested using bi-directional traffic between the SUT and the TMDE. Therefore, this interface is included in the certification.

- 10 Mbps IAW IEEE 802.3i.
- 10 Mbps IAW IEEE 802.3j.
- 100 Mbps IAW IEEE 802.3u.
- 1000 Mbps IAW IEEE 802.3z.
- 1000 Mbps IAW IEEE 802.3ab.

(c) Minimally, access products shall provide one of the following trunk-side interface rates (other rates and IEEE standards may be provided as optional interfaces). This requirement does not apply to the SUT as a Core and Distribution switch.

- 100 Mbps IAW IEEE 802.3u.
- 1000 Mbps IAW IEEE 802.3z.

(d) The Core, Distribution, and Access products may provide a fibre channel interface IAW American National Standards Institute (ANSI) International Committee for Information Technology Standards (INCITS) T11.2 and T11.3 (previously known as X3T9.3). If provided, the interface must meet the RFCs in the following subparagraphs. The SUT does not support these optional interfaces and therefore are not included in this certification.

- RFC 4338, Transmission of IPv6, IPv4, and Address Resolution Protocol (ARP) Packets over Fibre Channel.
- RFC 4044, Fibre Channel Management.

(e) The Core, Distribution, and Access products may provide one or more of the following wireless LAN interface rates. The SUT does not support these optional interfaces and therefore are not included in this certification.

- 54 Mbps IAW IEEE 802.11a.
- 11 Mbps IAW IEEE 802.11b.
- 54 Mbps IAW IEEE 802.11g.
- 300–600 Mbps IAW IEEE 802.11n.
- IEEE 802.16-2012: Broadband wireless communications standards for MANs.
- Other approved IEEE wireless interfaces may be implemented as optional interfaces.

(f) If any of the above wireless interfaces are provided, then the interfaces must support the requirements of Section 7.3, Wireless LAN. The SUT does not support the optional wireless interfaces.

(3) Port Parameter Requirements. The Core, Distribution, and Access products shall provide the parameters on a per port basis as specified in the following subparagraphs. These are required for core, distribution, and Layer 2 (L2)/Layer 3 (L3) access unless specified otherwise.

(a) Auto-negotiation IAW IEEE 802.3. All interfaces shall support auto-negotiation even when the IEEE802.3 standard has it as optional. This applies to 10/100/1000-T Ethernet standards (i.e., IEEE Ethernet Standard 802.3, 1993; or IEEE, Fast Ethernet Standard 802.3u, 1995; and IEEE, Gigabit Ethernet Standard 802.3ab, 1999). The SUT met this requirement with testing and the vendor's LoC.

(b) Force mode IAW IEEE 802.3. The SUT met this requirement with testing and the vendor's LoC.

(c) Flow control IAW IEEE 802.3x (Optional: Core). The SUT met this requirement with testing and the vendor's LoC.

(d) Filtering IAW appropriate RFC 1812 sections (sections applying to filtering). The SUT met this requirement with testing and the vendor's LoC.

(e) Link Aggregation IAW IEEE 802.1AX (applies to output/egress trunk-side ports only) (Optional Access). The SUT met this requirement with testing and the vendor's LoC.

(f) Spanning Tree Protocol IAW IEEE 802.1D (Optional: Core). The SUT met this requirement with testing and the vendor's LoC.

(g) Multiple Spanning Tree IAW IEEE 802.1s (Optional: Core). The SUT met this requirement with testing and the vendor's LoC.

(h) Rapid Reconfiguration of Spanning Tree IAW IEEE 802.1w (Optional: Core). The SUT met this requirement with the vendor's LoC.

(i) Port-Based Access Control IAW IEEE 802.1x (Optional: Core, Distribution, and Access). The SUT met this requirement with the vendor's LoC.

(j) Link Layer Discovery Protocol (LLDP) IAW IEEE 802.1AB (Optional Core, Distribution, and Access). The SUT met this requirement with testing and the vendor's LoC.

(k) Link Layer Discovery – Media Endpoint Discovery IAW ANSI/ Telecommunications Industry Association (TIA)-1057 (Optional Core, Distribution, and Access). The SUT met this requirement the vendor's LoC.

(l) Power over Ethernet (PoE) IAW either 802.3af-2003 or 802.3at-2009. (Required only for VVoIP solutions; for data applications or non-Assured Services (AS) solutions, PoE is optionally required.) The SUT met this requirement the vendor's LoC.

(4) Class of Service Markings Requirements

(a) The Core, Distribution, and Access products shall support Differentiated Services Code Points (DSCPs) IAW RFC 2474 for both Internet Protocol (IP) IPv4 and IPv6 Packets, as follows:

1. The Core and Distribution products shall be capable of accepting any packet tagged with a DSCP value (0-63) on an ingress port and assign that packet to a QoS behavior listed in Section 7.2.1.6, Quality of Service Features. The SUT met this requirement with testing and the vendor's LoC.

2. The Core and Distribution products shall be capable of accepting any packet tagged with a DSCP value (0-63) on an ingress port and reassign that packet to any new DSCP value (0-63). Current DSCP values are provided in Section 6.2.2, Differentiated Service Code Point. (Optional: Access products). The SUT met this requirement with testing and the vendor's LoC.

3. The Core and Distribution products must be able to support the prioritization of aggregate service classes with queuing according to Section 7.2.1.6, Quality of Service Features. The SUT met this requirement with testing and the vendor's LoC.

4. Access products shall be capable of supporting the prioritization of aggregate service classes with queuing according to Section 7.2.1.6, Quality of Service Features. The SUT met this requirement with testing and the vendor's LoC.

(b) The Core, Distribution, and Access products may support the 3-bit user priority field of the IEEE 802.1Q 2-byte Tag Control Information (TCI) field (see Figure 7.2-1, IEEE 802.1Q Tagged Frame for Ethernet, and Figure 7.2-2, TCI Field Description). Default values are provided in Table 7.2-1, 802.1Q Default Values. If provided, the following Class of Service (CoS) requirements apply:

1. The Core, Distribution, and access products shall be capable of accepting any frame tagged with a user priority value (0–7) on an ingress port and assign that frame to a QoS behavior listed in Section 7.2.1.6, Quality of Service Features. The SUT met this requirement with testing and the vendor's LoC.

2. The Core and Distribution products shall be capable of accepting any frame tagged with a user priority value (0-7) on an ingress port and reassign that frame to any new user priority value (0-7) (Optional: Distribution and Access). The SUT met this requirement with testing and the vendor's LoC.

(5) Virtual LAN Capabilities Requirements

(a) The Core, Distribution, and Access products shall be capable of the following:

1. Accepting Virtual Local Area Network (VLAN) tagged frames according to IEEE 802.1Q (see Figure 7.2-1, IEEE 802.1Q Tagged Frame for Ethernet, and Figure 7.2-2, TCI Field Description). The SUT met this requirement with testing and the vendor's LoC.

2. Configuring VLAN IDs (VIDs). VIDs on an ingress port shall be configurable to any of the 4094 values (except 0 and 4095). The SUT met this requirement with testing and the vendor's LoC.

3. Supporting VLANs types IAW IEEE 802.1Q. The SUT met this requirement with testing and the vendor's LoC.

(b) The UC products must be capable of accepting VLAN tagged frames and assigning them to the VLAN identified in the 802.1Q VID field (see Figure 7.2-4, IEEE 802.1Q-Based VLANs). The SUT met this requirement with testing and the vendor's LoC.

(6) Protocols Requirements. The Core, Distribution, and Access products shall meet protocol requirements for Internet Protocol version 4 (IPv4) and Internet Protocol version 6 (IPv6). The RFC requirements are listed in UCR 2013, Errata 1, Table 7.2-2, ASLAN Infrastructure RFC Requirements. Additional IPv6 requirements by product profile are listed in UCR 2013, Errata 1, Section 5, IPv6. These RFCs are not meant to conflict with Department of Defense (DoD) Information Assurance (IA) policy [e.g., Security Technical Implementation Guidelines (STIGs)]. Whenever a conflict occurs, DoD IA policy takes precedence. If there are conflicts with UCR 2013, Errata 1, Section 5, RFCs applicable to IPv6 in Section 5 take precedence. The SUT met this requirement for all protocols with the vendor's LoC.

(7) Quality of Service Features Requirements

(a) The Core, Distribution, and Access products shall be capable of the following QoS Features:

1. Providing a minimum of four queues. The SUT met this requirement with testing.

2. Assigning any incoming access/user-side "tagged" session to any of the queues for prioritization onto the egress (trunk-side/network-side) interface. The SUT met this requirement with testing and the vendor's LoC.

3. Supporting Differentiated Services (DS), Per-Hop Behaviors (PHBs), and traffic conditioning IAW RFCs 2474, 2597, and 3246. The SUT met this requirement with testing and the vendor's LoC.

4. All queues shall be capable of having a bandwidth (BW) assigned (i.e., queue 1: 200 kbps, queue 2: 500 kbps) or percentage of traffic (queue 1: 25 percent, queue 2: 25 percent). The BW or traffic percentage shall be fully configurable per queue from 0 to full BW or 0 to 100 percent. The sum of configured queues shall not exceed full BW or 100 percent of traffic. The SUT met this requirement with testing and the vendor's LoC.

5. Core, Distribution, and Access products shall meet the traffic conditioning (policing) requirements of Section 6.2.4. The SUT met this requirement with testing and the vendor's LoC.

(b) Providing a minimum of six queues is optional for Core, Distribution and Access. The six-queue model is an optional requirement; it was not tested and is not covered under this certification.

(c) The product shall support the DSCP plan, as shown in UCR 2013, Errata 1, Table 7.2-3, DSCP Assignments. DSCP assignments shall be software configurable for the full range of six bit values (0-63 Base10) for backwards compatibility with IP precedence environments that may be configured to use the Type of Service (TOS) field in the IP header but do not support DSCP. The SUT met this requirement with the vendor's LoC.

(8) Network Monitoring Requirements. The Core, Distribution and Access products shall support the following network monitoring features:

(a) Simple Network Management Protocol Version 3 (SNMPv3) IAW RFCs 3411, 3412, 3413, 3414, 3415, 3416, and 3417. The SUT met this requirement with testing and the vendor's LoC.

(b) Remote Monitoring (RMON) IAW RFC 2819. The product shall minimally support the following RFC 2819 groups: Ethernet statistics, history control, Ethernet history, and alarms. The SUT met this requirement with the vendor's LoC.

(c) Coexistence between Version 1, Version 2, and Version 3 of the Internet-standard Network Management Framework IAW RFC 3584. The SUT met this requirement with the vendor's LoC.

(d) The Advanced Encryption Standard (AES) Cipher Algorithm in the SNMP User-based Security Model IAW RFC 3826. Security was tested by DISA-led IA test teams and the results were published in a separate report, Reference (e).

(9) Security Requirements. The Core, Distribution and Access products shall meet the security protocol requirements listed in Section 4, Information Assurance, as follows: Core and Distribution products shall meet all requirements annotated as Router (R) and LAN Switch (LS). Access switches shall meet the IA requirements annotated for LS. In addition to wireless IA

requirements previously specified, Wireless Local Area Network Access Systems (WLASs) and Wireless Access Bridges (WABs) shall meet all IA requirements for LSs. Wireless End Instruments (WEIs) shall meet all IA requirements annotated for End Instruments (EIs). When conflicts exist between the UCR and STIG requirements, the STIG requirements will take precedence. The SUT met the requirements in the UCR 2013, Errata 1, Section 4, with the vendor's LoC. In addition, security was tested by the DISA-led IA test teams and the results are published in a separate report, Reference (e).

b. The UCR 2013, Errata 1, section 7.2.2 includes the LAN Switch and Router Redundancy Requirements. The ASLAN (High and Medium) shall have no single point of failure that can cause an outage of more than 96 IP telephony subscribers. A single point of failure up to and including 96 subscribers is acceptable; however, to support mission-critical needs, FLASH/FLASH OVERRIDE (F/FO) subscribers should be engineered for maximum availability. To meet the availability requirements, all switching/routing platforms that offer service to more than 96 telephony subscribers shall provide redundancy in either of two ways:

- The product itself (Core, Distribution, or Access) provides redundancy internally.
- A secondary product is added to the ASLAN to provide redundancy to the primary product (redundant connectivity required).

(1) Single Product Redundancy Requirements. If a single product is used to meet the redundancy requirements, then the requirements in the following subparagraphs are applicable to the product. The SUT does not meet the single product redundancy requirements.

- Dual Power Supplies
- Dual Processors (Control Supervisors)
- Termination Sparing
- Redundancy Protocol
- No Single Failure Point
- Switch Fabric or Backplane Redundancy

(2) Dual Product Redundancy Requirements. If the SUT provides redundancy through dual products, then the following requirements are applicable. The failover over to the secondary product must not result in any lost calls. The secondary product may be in "standby mode" or "active mode," regardless of the mode of operation the traffic engineering of the links between primary and secondary must meet the requirements provided in Section 7.5.19, Traffic Engineering. NOTE: In the event of a primary product failure, all calls that are active shall not be disrupted (loss of existing connection requiring redialing) and the failover to the secondary product must be restored within 5 seconds. The SUT meets this requirement when deployed in a stack configuration, in accordance with the CoF. The SUT met this requirement with testing and the vendor's LoC.

c. The UCR 2013, Errata 1, section 7.2.3 includes the LAN Product Requirements Summary. Table 7.2-4 summarizes the LAN product requirements. The SUT met these requirements with testing and the vendor's LoC.

d. The UCR 2013, Errata 1, section 7.2.4 includes the Multiprotocol Label Switching Requirements in ASLANs. The implementation of ASLANs sometimes may cover a large geographical area. For large ASLANs, a data transport technique referred to as Multiprotocol Label Switching (MPLS) may be used to improve the performance of the ASLAN core layer. The SUT does not support this optional requirement.

e. The UCR 2013, Errata 1, section 7.3 includes the Wireless Product Requirements. Wireless LAN implementations are considered extensions of the physical layer. The requirements in UCR 2013, Errata 1, section 7.3 apply to wireless LAN products. This section outlines the requirements when using wireless Ethernet technologies in a LAN to provide VoIP service to subscribers. In particular, this section defines four wireless areas that may apply to VoIP subscribers: Wireless End Instruments (WEIs), Wireless LAN Access System (WLAS), Wireless Access Bridges (WABs), and general requirements for wireless LANs (WLANs). For LANs supporting VoIP subscribers, wireless transport may be used only as the following: To provide wireless Access Layer functionality via a wireless access point. Between two or more LANs as a "bridge" technology. The components of a wireless network are certified along with an ASLAN, while wireless VoIP devices are certified with the VoIP solution. The SUT does not support this optional requirement.

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

8. TESTING LIMITATIONS. JITC's test team noted the following testing limitations including the impact on the certification:

a. HP 5900. The Test, Measurement, and Diagnostic Equipment did not have a sufficient quantity of 10 GbE ports to fully load the 48 ports for the 10Gbps interfaces on the HP 5900 switch. The 48-port SUT was tested with traffic sent bi-directional at line rate on forty of the 10GbE test ports to stress the Application Specific Integrated Circuits (ASICs) and backplane of the SUT. The 48-port SUT has only one ASIC. The SUT was also test by inserting bi-directional traffic and having that traffic traverse between ports using virtual router forwarding. Through testing and analysis this product is certified to meet the maximum blocking factor requirements as listed in Enclosure 3, Table 3-3.

b. HP 5920. The HP2920 switch has twenty-four 10Gbps with eight of those ports reserved for stack connection. The remaining 16 ports were tested at line rate by inserting bi-directional traffic. The switch only has one ASIC and was fully tested with all available ports. Through testing and analysis this product is certified to meet the maximum blocking factor requirements as listed in Enclosure 3, Table 3-3.

9. CONCLUSION(S). The SUT meets the critical interoperability requirements for Core and Distribution switches in accordance with the UCR and is certified for joint use with other UC Products listed on the Approved Products List (APL). The SUT meets the interoperability requirements for the interfaces listed in Table 3-1.

DATA TABLES

Table 3-1. Interface Status

Interface	Applicability			Threshold CRs/FRs (See note 1.)	Status	Remarks
	Co	D	A			
Network Management Interfaces (See note 2.)						
IEEE 802.3i (10BaseT UTP)	C	C	C	1 and 3	Met	
IEEE 802.3u (100BaseT UTP)	C	C	C	1 and 3	Met	
IEEE 802.3ab (1000BaseT UTP)	C	C	C	1 and 3	Met	
Access (User) Interfaces (See note 2.)						
IEEE 802.3i (10BaseT UTP)	C	C	R	1, 2, and 3	Not Tested	(See note 3.)
IEEE 802.3u (100BaseT UTP)	R	R	R	1, 2, and 3	Not Tested	(See note 3.)
IEEE 802.3u (100BaseFX)	C	C	R	1, 2, and 3	Not Tested	(See note 3.)
IEEE 802.3ab (1000BaseT UTP)	C	C	R	1, 2, and 3	Met	(See note 4.)
IEEE 802.3z (1000BaseX Fiber)	R	R	R	1, 2, and 3	Not Tested	(See note 5.)
IEEE 802.3ae (10GBaseX) (C)	O	O	O	1, 2, and 3	Met	(See note 4.)
Uplink (Trunk) Interfaces (See note 2.)						
IEEE 802.3u (100BaseT UTP)	R	R	R	1, 2, 3, and 4	Not Tested	(See note 3.)
IEEE 802.3u (100BaseFX)	C	C	R	1, 2, 3, and 4	Not Tested	(See note 3.)
IEEE 802.3ab (1000BaseT UTP)	C	C	R	1, 2, 3, and 4	Not Tested	(See note 4.)
IEEE 802.3z (1000BaseX Fiber)	R	R	R	1, 2, 3, and 4	Not Tested	(See note 4.)
IEEE 802.3ae (10GBaseX)	O	O	O	1, 2, 3, and 4	Met	
IEEE 802.3ba (40GbaseX)	O	O	O	1, 2, 3, and 4	Met	(See note 6.)
IEEE 802.3ba (100GbaseX)	O	O	O	1, 2, 3, and 4	Not Tested	(See note 3.)
	Co	**D**	**A**			
Wireless LAN Interfaces						
IEEE 802.11a IAW 802.11-2007 – 5 GHz	N/A	N/A	C	1 and 5	Not Tested	(See note 3.)
IEEE 802.11b IAW 802.11-2007 – 2.4GHz	N/A	N/A	C	1 and 5	Not Tested	(See note 3.)
IEEE 802.11g IAW 802.11-2007 – 2.4 GHz	N/A	N/A	C	1 and 5	Not Tested	(See note 3.)
IEEE 802.11n-2009 – 2.4 GHz and 5 GHz	N/A	N/A	C	1 and 5	Not Tested	(See note 3.)
IEEE 802.16-2012	N/A	N/A	C	1 and 5	Not Tested	(See note 3.)

NOTES:

1. The SUT high-level CR and FR ID numbers depicted in the Threshold CRs/FRs column can be cross-referenced in Table 3. These high-level CR/FR requirements refer to a detailed list of requirements provided in Enclosure 3.
2. Core and Distribution products must minimally support 100Base-X (802.3u) and 1000Base-X (802.3z). Access products must minimally support one of the following standards: 802.3i (10BaseT), 802.3j (10BaseF), 802.3u (100BaseT/F), 802.3z (1000BaseF), or 802.3ab (1000BaseT). Other rates and standards may be provided as conditional interfaces.
3. The SUT does not support this interface.
4. Traffic was successfully transmitted and received between the SUT and the test instrumentation. Therefore, this interface is included in the certification.
5. Although the SUT supports this interface, it was not tested and is not covered under this certification.
6. This interface was tested using bi-directional traffic between the SUT and the Brocade VDX6740.

LEGEND:

802.3ab	1000BaseT Gbps Ethernet over Twisted Pair at 1 Gbps	A	Access
		ASLAN	Assured Services Local Area Network
802.3ae	10 Gbps Ethernet	C	Conditional
802.3ba	40 and 100 Gigabit Ethernet Architecture	Co	Core
802.3i	10BaseT 10 Mbps Ethernet over Twisted Pair	CRs	Capability Requirements
802.3u	Standard for carrier sense multiple access with collision detection at 100 Mbps	D	Distribution
		FRs	Functional Requirements
802.3z	Gigabit Ethernet Standard	Gbps	Gigabits per second
10BaseT	10 Mbps (Baseband Operation, Twisted Pair) Ethernet	GHz	GigaHertz
		ID	Identification
100BaseT	100 Mbps (Baseband Operation, Twisted Pair) Ethernet	IEEE	Institute of Electrical and Electronics Engineers
		IP	Internet Protocol
100BaseFX	100 Mbps Ethernet over Fiber	Mbps	Megabits per second
1000BaseT	1000 Mbps (Baseband Operation, Twisted Pair) Ethernet	N/A	Not Applicable
		O	Optional
1000BaseX	1000 Mbps Ethernet over Fiber or Copper	R	Required
10GBaseX	10000 Mbps Ethernet over Fiber or Copper	SUT	System Under Test
		UTP	Unshielded Twisted Pair

Table 3-2. Capability and Functional Requirements and Status

CR/FR ID	Capability/Function	Applicability (See note 1.)	UCR Reference	Status
1	**General LAN Switch and Router Product**			
	Port Interface Rates	Required	7.2.1.1	Met
	Port Parameter	Required	7.2.1.2	Met
	Class of Service Markings	Required	7.2.1.3	Met
	Virtual LAN Capabilities	Required	7.2.1.4	Met
	Protocols	Required	7.2.1.5	Partially Met (See notes 2.)
	Quality of Service Features	Required	7.2.1.6	Met
	Network Monitoring	Required	7.2.1.7	Met
	Security	Required	7.2.1.8	Met (See notes 3.)
2	**LAN Switch and Router Redundancy**			
	Single Product Redundancy	Optional	7.2.2.1	Not Tested
	Dual Product Redundancy	Optional	7.2.2.2	Met
3	**LAN Product Requirements Summary**			
	LAN Product Requirements Summary	Optional	7.2.3	Met
4	**MPLS in ASLANs**			
	MPLS ASLAN	Optional	7.2.4.2	Not Tested
	MPLS VPN Augmentation to VLANs	Optional	7.2.4.3	Not Tested
5	**Wireless LAN**			
	General Wireless Product	Optional	7.3.1	Not Tested
	Wireless Interface	Optional	7.3.2	Not Tested
	Wireless End Instruments	Optional	7.3.3	Not Tested
	Wireless LAN Access System	Optional	7.3.4	Not Tested
	Wireless Access Bridge	Optional	7.3.5	Not Tested
	Survivability	Optional	7.3.6	Not Tested

NOTES:

1. The annotation of "required" refers to a high-level requirement category. The applicability of each sub-requirement is provided in Table 3-5.
2. The SUT is not compliant with IP6-000820 and IP6-000770. DISA has adjudicated these discrepancy as having a minor operational impact.
3. Security is tested by a DISA-led Information Assurance test team and the results published in a separate report, Reference (e).

LEGEND:

ASLAN	Assured Services Local Area Network	NLT	No Later Than
Base-T	Baseband Operation, Twisted Pair	OSPF	Open Shortest Path First
CoF	Condition of Fielding	POA&M	Plan Of Action & Milestones
CR	Capability Requirement	POE	Power over Ethernet
DISA	Defense Information Systems Agency	RADIUS	Remote Authentication Dial-in User Server
FR	Functional Requirements	RFC	Request for Comment
Gbps	Gigabit per second	SUT	System Under Test
ID	Identification	UCR	Unified Capabilities Requirements
IPv6	Internet Protocol version 6	VLAN	Virtual Local Area Network
LAN	Local Area Network	VPN	Virtual Private Network
LDP	Label Distribution Protocol	VVoIP	Voice and Video over Internet Protocol
MPLS	Multiprotocol Label Switching		

Table 3-3. SUT Hardware/Software/Firmware Version Identification with Interface Card Blocking Factors

Component (See note 1.)	Release	Sub-component (See note 1.)	Function	Non-Blocking Factor Level (See note 2.)	
				C/D (See note 3)	A
HP 5900	7.1.045	**JC772A/JG554A**	**HP 5900 Switch 48 10GbE SFP+ Ports + 4 Port 40GbE**	Maximum (See note 4.)	N/A
		JG510A	**HP 5900 Switch 48 autosensing 10/100/1000 ports + 4 Fixed 10GbE SFP+ Ports + 2 QSFP+ 40GbE Ports**	Maximum (See note 5.)	N/A
		JG336A	HP 5900 Switch 48 RJ45 1/10GbE Ports + 4 Port 40GbE QSFP+ Ports	N/A	N/A
		JG296A/JG55A	**HP5920 Switch 24 fixed 1000/10000 SFP+ Ports**	Maximum (See note 6.)	N/A
		JG838A	HP FlexFabric 5900CP-48XG-4QSFP+ Switch	N/A	N/A

NOTES:

1. Components bolded and underlined were tested by JITC. The other components in the family series were not tested; however, they utilize the same software and similar hardware. JITC analysis determined them to be functionally identical for interoperability certification purposes and are also certified for joint use.
2. There are three levels of non-blocking for core, distribution, and access switches. For core and distribution, the minimum level is 2 to 1, medium level is 1.5 to 1, and maximum level is 1 to 1 (100 percent non-blocking). For access, the minimum level is 8 to 1, medium level is 2 to 1, and maximum level is 1 to 1 (100 percent non-blocking).
3. The switches in the stack were tested individually. However, in order to meet the dual redundancy, the switches have to be a member of a stack.
4. The Test, Measurement, and Diagnostic Equipment did not have a sufficient quantity of 10 GbE ports to fully load the 48 ports for the 10Gbps interfaces on the HP 5900 switch. The 48-port SUT was tested with traffic sent bi-directional at line rate on forty of the 10GbE test ports to stress the Application Specific Integrated Circuits (ASICs) and backplane of the SUT. The 48-port SUT has only one ASIC. The SUT was also tested by inserting bi-directional traffic and having that traffic traverse between ports using virtual router forwarding. Through testing and analysis this product is certified to meet the maximum blocking factor requirements.
5. The HP5900 (JG510A) switch was successfully tested with 40 GB of bi-directional traffic on the 10GbE SFP+ ports. Through testing and analysis, this product is certified to meet the maximum blocking factor requirements.
6. The HP5920 switch has twenty-four 10Gbps with eight of those ports reserved for stack connection. The remaining 16 ports were tested at line rate by inserting bi-directional traffic. The switch only has one ASIC and was fully tested with all available ports. Through testing and analysis, this product is certified to meet the maximum blocking factor requirements.

LEGEND:

A	Access		
ASLAN	Assured Services Local Area Network	JITC	Joint Interoperability Test Command
Base-T	Baseband Operation, Twisted Pair	N/A	Not Applicable
C	Core	PoE	Power over Etherent
D	Distribution	SFP	Small Form-factor Pluggable
GbE	Gigabit Ethernet	XFP	10 Gigabit Small Form Factor Pluggable

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

System Name	Software Release	Function
Required Ancillary Equipment (site-provided)		
Active Directory		
Remote Authentication Dial-In User Server		
Syslog Server		
Management Workstation (Microsoft Windows 7 Professional Service Pack 1)		
Test Network Components		
Brocade ICX	8.0.10b	Distribution Switch 1
Brocade MLXe	5.6.0a	Distribution Switch 2
Brocade XMR	5.6.0a	Core Switch
Brocade CER	5.6.0a	Layer 3 Access Switch
Ixia IxNetwork	7.30.917.12 EA	Test, Measurement & Diagnostic Equipment

Table 3-5. ASLAN Component Capability/Functional Requirements

CR/FR ID	Requirement	UCR 2013 Reference (See note 1.)	LoC/ TP ID (See note 2.)	R/O/C
1	**7.2.1 – General LAN Switch and Router Product**			
1-1	**7.2.1 – General LAN Switch and Router Product Requirements**			
1	The Core, Distribution, and Access products shall be capable of meeting the following parameters: a. Non-blocking. All Core, Distribution, and Access products shall be non-blocking for their ports based on the following traffic engineering. Non-blocking is defined as the capability to send and receive a mixture of 64 to 1518 byte packets at full duplex rates from ingress ports to egress ports through the component's backplane without losing any packets. In a non-blocking switch, all ports can run at full wire speed without any loss of packets or cells. Blocking factor is defined as the ratio of all traffic to non-blocked traffic (i.e., a blocking factor of 8 to 1 means that 12.5 percent of the traffic must be nonblocking). Each Core, Distribution, and Access product has up to three levels of performance: Minimum, Medium, and Maximum. For certification purposes, products need only meet minimum performance levels. (1) Access Products. Access products shall not have a blocking factor that exceeds 8 to 1 (minimum). This blocking factor includes all hardware and software components. Medium performance level Access products shall not have a blocking factor that exceeds 2 to 1. This blocking factor includes all hardware and software components. Maximum performance level Access products shall be non-blocking. This blocking factor includes all hardware and software components. (2) Distribution and Core Products. These products shall not have a blocking factor that exceeds 2 to 1 (minimum). This blocking factor includes all hardware and software components. Medium performance level products shall not have a blocking factor that exceeds 1.5 to 1. This blocking factor includes all hardware and software components. Maximum performance level products shall be non-blocking. This blocking factor includes all hardware and software components.	7.2.1 EDG-000010	L/T IO-17	Core (R) Distro (R) Access (R)
2	b. Latency. All Core, Distribution, and Access products shall have the capability to transport prioritized packets (media and signaling) as follows. The latency shall be achievable over any 5-minute period measured from ingress ports to egress ports under congested conditions. Congested condition is defined as 100 percent bandwidth utilization. Prioritized packets are defined as packets having a service class above best effort. Latency numbers do not include serialization delay. Serialization delay may be added to below specified numbers. (1) Voice Packets. No more than 2 ms latency. (2) Voice and video signaling packets. No more than 2 ms latency. (3) Video Packets. No more than 10 ms latency. Video packets are defined as including video, voice associated with video session, and video signaling. Video packets include both video teleconferencing and streaming video. (4) Preferred Data Packets. N/A. Preferred data is defined in the UC Framework as preferred elastic traffic (see UC Framework 2013, Section 6, Network Infrastructure End-to-End Performance). (5) Best Effort Data. N/A.	7.2.1 EDG-000010	T IO-10 IO-11	Core (R) Distro (R) Access (R)
3	c. Jitter. All Core, Distribution, and Access products shall have the capability to transport prioritized packets (media and signaling) as follows. The jitter shall be achievable over any 5-minute period measured from ingress ports to egress ports under congested conditions. Congested condition is defined as 100 percent bandwidth utilization. (1) Voice Packets. No more than 1 ms jitter. (2) Video Packets. No more than 10 ms jitter. (3) Preferred Data Packets. N/A. (4) Best Effort Data. N/A.	7.2.1 EDG-000010	T IO-10 IO-11	Core (R) Distro (R) Access (R)

Table 3-5. ASLAN Component Capability/Functional Requirements (continued)

CR/FR ID	Requirement	UCR 2013 Reference (See note 1.)	LoC/ TP ID (See note 2.)	R/O/C
1-1	**7.2.1 – General LAN Switch and Router Product Requirements (continued)**			
4	d. Packet Loss. All Core, Distribution and Access products shall have the capability to transport prioritized packets (media and signaling) as follows. The packet loss shall be achievable over any 5-minute period measured from ingress ports to egress ports under congested conditions. Congested condition is defined as 100 percent bandwidth utilization. (1) Voice Packets. Allowed packet loss is dependent upon the queuing implemented (i.e., amount of properly traffic shaped bandwidth). Packet loss measured within the configured queuing parameters shall be measured to be no more than 0.015 percent for Access, Distribution, and Core products. (2) Video Packets. Allowed packet loss is dependent on the queuing implemented (i.e., amount of properly traffic shaped bandwidth). Packet loss measured within the configured queuing parameters shall be measured to be no more than 0.05 percent for Access, Distribution, and Core products. (3) Preferred Data packets. Allowed packet loss is dependent on the queuing implemented (i.e., amount of properly traffic shaped bandwidth). Packet loss measured within the configured queuing parameters shall be measured to be no more than 0.05 percent for Access, Distribution, and Core products. (4) Best Effort data packets. Best effort data has no packet loss requirements. Amount of loss is determined by traffic engineering and offered load.	7.2.1 EDG-000010	T IO-12	Core (R) Distro (R) Access (R)
1-2	**7.2.1.1 – Port Interface Rates**			
1	Minimally, Core and Distribution products shall support the following interface rates (other rates and IEEE standards may be provided as optional interfaces). Rates specified are the theoretical maximum data bit rate specified for Ethernet; link capacity and effective throughput is influenced by many factors. For calculation purposes, link capacities are to be calculated IAW definitions contained in RFC 2330 and RFC 5136. NM interfaces are defined in Section 2.19. The product must minimally support the following interfaces: (5) 100 Mbps IAW IEEE 802.3u (for interconnection between the distribution-core and distribution access). (6) 1000 Mbps IAW IEEE 802.3z (For interconnection between the core to WAN, distribution-core, and distribution-access).	7.2.1.1 EDG-000020	T IO-1	Core (R) Distro (R)
2	Minimally, Access products shall provide one of the following user-side interface rates (other rates and IEEE standards may be provided as optional interfaces): a. 10 Mbps IAW IEEE 802.3i. b. 10 Mbps IAW IEEE 802.3j. c. 100 Mbps IAW IEEE 802.3u. d. 1000 Mbps IAW IEEE 802.3z. e. 1000 Mbps IAW IEEE 802.3ab.	7.2.1.1 EDG-000030	T IO-1	Access (R)
3	Minimally, Access products shall provide one of the following trunk-side interface rates (other rates and IEEE standards may be provided as optional interfaces): a. 100 Mbps IAW IEEE 802.3u. b. 1000 Mbps IAW IEEE 802.3z.	7.2.1.1 EDG-000040	T IO-1	Access (R)
4	The Core, Distribution, and Access products may provide a fibre channel interface IAW ANSI International Committee for Information Technology Standards (INCITS) T11.2 and T11.3 (previously known as X3T9.3). If provided, the interface must meet the following: a. RFC 4338, Transmission of IPv6, IPv4, and Address Resolution Protocol (ARP) Packets over Fibre Channel. b. RFC 4044, Fibre Channel Management.	7.2.1.1 EDG-000050	L	Core (O) Distro (O) Access (O)
5	The Core, Distribution, and Access products may provide one or more of the following wireless LAN interface rates: a. 54 Mbps IAW IEEE 802.11a. b. 11 Mbps IAW IEEE 802.11b. c. 54 Mbps IAW IEEE 802.11g. d. 300–600 Mbps IAW IEEE 802.11n. e. IEEE 802.16-2012: Broadband wireless communications standards for MANs. f. Other approved IEEE wireless interfaces may be implemented as optional interfaces.	7.2.1.1 EDG-000060	Refer to Wireless TPs	Core (O) Distro (O) Access (O)
6	If any of the above wireless interfaces are provided, then the interfaces must support the requirements of Section 7.3, Wireless LAN.	7.2.1.1 EDG-000070	Refer to Wireless TPs	Core (C) Distro (C) Access (C)

Table 3-5. ASLAN Component Capability/Functional Requirements (continued)

CR/FR ID	Requirement	UCR 2013 Reference (See note 1.)	LoC/ TP ID (See note 2.)	R/O/C
1-3	**7.2.1.2 – Port Parameter**			
1	The Core, Distribution, and Access products shall provide the following parameters on a per port basis as specified: a. Auto-negotiation IAW IEEE 802.3. All interfaces shall support auto-negotiation even when the IEEE 802.3 standard has it as optional. This applies to 10/100/1000-T Ethernet standards (i.e., IEEE Ethernet Standard 802.3, 1993; or IEEE, Fast Ethernet Standard 802.3u, 1995; and IEEE, Gigabit Ethernet Standard 802.3ab, 1999). b. Force mode IAW IEEE 802.3. c. Flow control IAW IEEE 802.3x (Optional: Core). d. Filtering IAW appropriate RFC 1812 sections (sections applying to filtering). e. Link Aggregation IAW IEEE 802.1AX (applies to output/egress trunk-side ports only) (Optional Access). f. Spanning Tree Protocol IAW IEEE 802.1D (Optional: Core). g. Multiple Spanning Tree IAW IEEE 802.1s (Optional: Core). h. Rapid Reconfiguration of Spanning Tree IAW IEEE 802.1w (Optional: Core. i. Port-Based Access Control IAW IEEE 802.1x (Optional: Core, Distribution, and Access). j. Link Layer Discovery Protocol (LLDP) IAW IEEE 802.1AB (Optional Core, Distribution, and Access). k. Link Layer Discovery – Media Endpoint Discovery IAW ANSI/ Telecommunications Industry Association (TIA)-1057 (Optional Core, Distribution, and Access). l. Power over Ethernet (PoE) IAW either 802.3af-2003 or 802.3at-2009. (Required only for VVoIP solutions; for data applications or non-Assured Services (AS) solutions, PoE is optionally required.)	7.2.1.2 EDG-000080	L/T IO-14 IO-15	Core (R) Distro (R) Access (R)
1-4	**7.2.1.3 – Class of Service Marking**			
1	The Core, Distribution, and Access products shall support DSCPs IAW RFC 2474 for both IPv4 and IPv6 Packets, as follows: a. The Core and Distribution products shall be capable of accepting any packet tagged with a DSCP value (0-63) on an ingress port and assign that packet to a QoS behavior listed in Section 7.2.1.6, Quality of Service Features. b. The Core and Distribution products shall be capable of accepting any packet tagged with a DSCP value (0-63) on an ingress port and reassign that packet to any new DSCP value (0-63). Current DSCP values are provided in Section 6.2.2, Differentiated Service Code Point. (Optional: Access products) c. The Core and Distribution products must be able to support the prioritization of aggregate service classes with queuing according to Section 7.2.1.6, Quality of Service Features. d. Access products shall be capable of supporting the prioritization of aggregate service classes with queuing according to Section 7.2.1.6, Quality of Service Features. Queuing may be supported in either of the two following CoS methods: (1) Layer 3 CoS Layer 3 Cos involves support for DSCP IAW RFC 2474 for IPv4 and IPv6. Within this CoS method, the access product shall support queuing by either: a) queuing directly based on the DSCP within the IP header (IPv4 and IPv6). The original DSCP value must also be preserved and passed unaltered through the product; or, b) The product shall inspect the IP header (IPv4 and IPv6). Based on the DSCP value contained within the IP header, the product may map the DSCP value (0-63) to the Ethernet priority field (decimal values 0-7). Queuing may be based on the mapping of the DSCP to a layer 2 priority field value. Any received DSCP value (0-63) must be able to be mapped to any priority value (0-7). The original DSCP value must be preserved and passed unaltered through the product. (2) Layer 2 Cos. Layer 2 CoS shall use the Virtual LAN identification (VLAN ID), see Section 7.2.1.4, defined in IEEE 802.1Q to perform queuing assignment. Access devices shall be capable of assigning any VLAN ID (either directly or through the 3 Ethernet priority bits (decimal values 0 through 7) to any of the 4 queues.	7.2.1.3 EDG-000090	T IO-13	Core (R) Distro (R) Access (R)

Table 3-5. ASLAN Component Capability/Functional Requirements (continued)

<table>
<tr><th>CR/FR ID</th><th>Requirement</th><th>UCR 2013 Reference (See note 1.)</th><th>LoC/ TP ID (See note 2.)</th><th>R/O/C</th></tr>
<tr><td>1-4</td><td colspan="3">7.2.1.3 – Class of Service Marking (continued)</td><td></td></tr>
<tr><td>2</td><td>
The Core, Distribution, and Access products may support the 3-bit user priority field of the IEEE 802.1Q 2-byte Tag Control Information (TCI) field (see Figure 7.2-1, IEEE 802.1Q Tagged Frame for Ethernet, and Figure 7.2-2, TCI Field Description). Default values are provided in Table 7.2-1, 802.1Q Default Values. If provided, the following CoS requirements apply:
a. The Core, Distribution, and Access products shall be capable of accepting any frame tagged with a user priority value (0–7) on an ingress port and assign that frame to a QoS behavior listed in Section 7.2.1.6, Quality of Service Features.
b. The Core and Distribution products shall be capable of accepting any frame tagged with a user priority value (0-7) on an ingress port and reassign that frame to any new user priority value (0-7) (Optional: Distribution and Access).
IEEE 802.1Q Tagged Frame for Ethernet
<table>
<tr><th colspan="9">BYTES</th></tr>
<tr><td>7</td><td>1</td><td>6</td><td>6</td><td>2</td><td>2</td><td>2</td><td>42-1496</td><td>4</td></tr>
<tr><td>Preamble</td><td>SFD</td><td>DA</td><td>SA</td><td>TPID</td><td>TCI</td><td>Type Length</td><td>Data</td><td>CRC</td></tr>
</table>
802.1Q Default Values
<table>
<tr><th rowspan="2">AGGREGATE SERVICE CLASS</th><th rowspan="2">GRANULAR SERVICE CLASS</th><th colspan="2">Default 802.1Q COS TAG</th></tr>
<tr><th>Base 2</th><th>Base 10</th></tr>
<tr><td>Control</td><td>Network control</td><td>111</td><td>7</td></tr>
<tr><td rowspan="8">Inelastic/ Real-Time</td><td>User Signaling1</td><td>110</td><td>6</td></tr>
<tr><td>Circuit Emulation1</td><td>110</td><td>6</td></tr>
<tr><td>Short messages1</td><td>110</td><td>6</td></tr>
<tr><td>Voice2</td><td>101</td><td>5</td></tr>
<tr><td>Video/VTC</td><td>100</td><td>4</td></tr>
<tr><td>Streaming</td><td>011</td><td>3</td></tr>
<tr><td>Interactive Transactions
OA&M – SNMP</td><td>010</td><td>2</td></tr>
<tr><td>File Transfers
OA&M – Trap/SysLog</td><td>001</td><td>1</td></tr>
<tr><td>Preferred Elastic</td><td></td><td></td><td></td></tr>
<tr><td>Elastic</td><td>Default</td><td>000</td><td>0</td></tr>
</table>
</td><td>7.2.1.3
EDG-000100</td><td>L</td><td>Core (O)
Distro (O)
Access (O)</td></tr>
</table>

Table 3-5. ASLAN Component Capability/Functional Requirements (continued)

CR/FR ID	Requirement	UCR 2013 Reference (See note 1.)	LoC/ TP ID (See note 2.)	R/O/C
1-5	**7.2.1.4 – Virtual LAN Capabilities**			
1	The Core, Distribution, and Access products shall be capable of the following: a. Accepting VLAN tagged frames according to IEEE 802.1Q (see Figure 7.2-1, IEEE 802.1Q Tagged Frame for Ethernet, and Figure 7.2-2, TCI Field Description). b. Configuring VLAN IDs (VIDs). VIDs on an ingress port shall be configurable to any of the 4094 values (except 0 and 4095). c. Supporting VLANs types IAW IEEE 802.1Q. The VLANs offer the following features: • Broadcast Control. Just as switches isolate collision domains for attached hosts and forward only appropriate traffic out a particular port, VLANs refine this concept further and provide complete isolation between VLANs. A VLAN is a bridging domain, and all broadcast and multicast traffic is contained within it. • Security. The VLANs provide security in two ways: – High-security users can be grouped into a VLAN, possibly on the same physical segment, and no users outside of that VLAN can communicate with them. – The VLANs are logical groups that behave like physically separate entities; inter-VLAN communication is achieved through a router. When inter-VLAN communication occurs through a router, all the security and filtering functionality that routers traditionally provide can be used because routers are able to look at Layer 3 information. • Port-Based. Port-based VLANs are VLANs that are dependent on the physical port a product is connected to. All traffic that traverses the port is marked with the VLAN configured for that port. Each physical port on the switch can support only one VLAN. With port-based VLANs, no Layer 3 address recognition takes place. All traffic within the VLAN is switched, and traffic between VLANs is routed (by an external router or by a router within the switch). This type of VLAN is also known as a segment-based VLAN (see Figure 7.2-3, Port-Based VLAN). • IEEE 802.1Q. VLANs can be assigned by end products IAW the IEEE 802.1Q VLAN ID tag.	7.2.1.4 EDG-000110	T IO-13	Core (R) Distro (R) Access (R)
2	The UC products must be capable of accepting VLAN tagged frames and assigning them to the VLAN identified in the 802.1Q VID field (see Figure 7.2-4, IEEE 802.1Q-Based VLANs). • User-Defined Value. This type of VLAN is typically the most flexible, allowing VLANs to be defined based on the value of any field in a packet or frame. For example, VLANs could be defined on a protocol basis or could be dependent on a particular address (Layer 2 or Layer 3). The simplest form of this type of VLAN is to group users according to their Media Access Control (MAC) addresses (see Figure 7.2-5, User-Defined VLANs). The LAN shall be designed so that Real-Time Services (RTS) and data reside in separate VLANs. Whether a product is performing converged services or a single service will decide how VLANs are designed. The required VLAN types are port-based and IEEE 802.1Q tagged frames. For VoIP, video, and data end products, any end system that supports convergence (i.e., more than one media) requires that the end-system pre-assign the VLAN using IEEE 802.1Q tags before the frames entering the ASLAN. For end-systems that support just one media (i.e., voice or video or data), the LAN can assign the VLAN based on port-based VLAN assignment. Real-time services and data must be placed in separate VLANs for security purpose. The LAN may be designed with more than one VLAN per media type. Signaling for voice and video can be placed in the same VLAN as the respective media, or placed in an entirely different signaling VLAN.	7.2.1.4 EDG-000120	T IO-13	Core (R) Distro (R) Access (R)

Table 3-5. ASLAN Component Capability/Functional Requirements (continued)

CR/FR ID	Requirement	UCR 2013 Reference (See note 1.)	LoC/ TP ID (See note 2.)	R/O/C
1-6	**7.2.1.5 – Protocols**			
1	The Core, Distribution, and Access products shall meet protocol requirements for IPv4 and IPv6. RFC requirements are listed in Table 7.2-2, ASLAN Infrastructure RFC Requirements. Additional IPv6 requirements by product profile are listed in Section 5, IPv6. These RFCs are not meant to conflict with DoD IA policy (e.g., STIGs). Whenever a conflict occurs, DoD IA policy takes precedence. If there are conflicts with Section 5, RFCs applicable to IPv6 in Section 5 take precedence.	7.2.1.5 EDG-000130	L/T (refer to Table 3)	Core (R) Distro (R) Access (R)
1-7	**7.2.1.6 – Quality of Service Features**			
1	The Core, Distribution, and Access products shall be capable of the following QoS features: a. Providing a minimum of four queues (see Figure 7.2-6, Four-Queue Design). b. Assigning any incoming access/user-side "tagged" session to any of the queues for prioritization onto the egress (trunk-side/network-side) interface. c. Supporting Differentiated Services (DS), Per-Hop Behaviors (PHBs), and traffic conditioning IAW RFCs 2474, 2597, and 3246: (1) Expedited Forwarding (EF). (2) Assured Forwarding (AF). (3) Best Effort (BE). (4) Class Selector (CS). (5) PHB Identification Codes. d. All queues shall be capable of having a bandwidth (BW) assigned (i.e., queue 1: 200 Kbps, queue 2: 500 kbps) or percentage of traffic (queue 1: 25 percent, queue 2: 25 percent). The BW or traffic percentage shall be fully configurable per queue from 0 to full BW or 0 to 100 percent. The sum of configured queues shall not exceed full BW or 100 percent of traffic. e. Core, Distribution, and Access products shall meet the traffic conditioning (policing) requirements of Section 6.2.4 as follows: (1) The product shall calculate the bandwidth associated with traffic conditioning, which requires that the queue size should account for the Layer 3 header (i.e., IP header), but not the Layer 2 headers (i.e., Point-to-Point Protocol [PPP], MAC, and so on) within a margin of error of 10 percent. When the other queues are not saturated, the Best Effort traffic may surge beyond its traffic-engineered limit.	7.2.1.6 EDG-000140	T IO-13	Core (R) Distro (R) Access (R)

Table 3-5. ASLAN Component Capability/Functional Requirements (continued)

CR/FR ID	Requirement	UCR 2013 Reference (See note 1.)	LoC/ TP ID (See note 2.)	R/O/C
1-7	**7.2.1.6 – Quality of Service Features (continued)**			
2	Provide a minimum of six queues (see Six-Queue Design). a. Assigning any incoming access/user-side "tagged" session to any of the queues for prioritization onto the egress (trunk-side/network-side) interface. b. Supporting DS, PHBs, and traffic conditioning IAW RFCs 2474, 2597, and 3246: (1) Expedited Forwarding (EF). (2) Assured Forwarding (AF). (3) Best Effort (BE). (4) Class Selector (CS). (5) PHB Identification Codes. c. All queues shall be capable of having a bandwidth (BW) assigned (i.e., queue 1: 200 Kbps, queue 2: 500 kbps) or percentage of traffic (queue 1: 25 percent, queue 2: 25 percent). The BW or traffic percentage shall be fully configurable per queue from 0 to full BW or 0 to 100 percent. The sum of configured queues shall not exceed full BW or 100 percent of traffic. d. Core, Distribution, and Access products shall meet the traffic conditioning (policing) requirements of Section 6.2.4 as follows: (1) The product shall calculate the bandwidth associated with traffic conditioning in accordance with RFC 3246, which requires that the queue size should account for the Layer 3 header (i.e., IP header), but not the Layer 2 headers (i.e., PPP, MAC, etc.) within a margin of error of plus or minus 10 percent. When the other queues are not saturated, the Best Effort traffic may surge beyond its traffic-engineered limit. (2) Core and Distribution products have been engineered for a blocking factor not to exceed 2:1. The aggregation of the Assured Forwarding and Expedition Forwarding queues should be configured to guarantee prioritization correctly, given the blocking factor. Priority queues (EF, AF4, and AF3) shall be configured as not to exceed 50 percent of the egress link capacity. (3) Access devices have been engineered for a blocking factor of 8:1 or less. Traffic prioritization is accomplished primarily to minimize latency. VoIP traffic is estimated at 2 (for dual appearances) bidirectional calls at 100 Kbps each or 400 Kbps (0 percent of 100 Mbps); video traffic is estimated at 500 Kbps bidirectional or 1 Mbps total (1.0 percent). With estimated blocking factor (8:1), 12.5 percent of the traffic is non-blocking. Based on traffic engineering outlined, the three priority queues should be set up not to exceed 12 percent of the egress link capacity.	7.2.1.6 EDG-000150	T IO-13	Core (R) Distro (R) Access (R)
3	The product shall support the DSCP plan, as shown in Table 7.2-3, DSCP Assignments. DS assignments shall be software configurable for the full range of six bit values (0-63 Base10) for backwards compatibility with IP precedence environments that may be configured to use the Type of Service (TOS) field in the IP header but do not support DSCP.	7.2.1.6 EDG-000160	T IO-13	Core (R) Distro (R) Access (R)
1-8	**7.2.1.7 – Network Monitoring**			
1	The Core, Distribution, and Access products shall support the following network monitoring features: a. Simple Network Management Protocol Version 3 (SNMPv3) IAW RFCs 3411, 3412, 3413, 3414, 3415, 3416, and 3417. b. Remote Monitoring (RMON) IAW RFC 2819. The product shall minimally support the following RFC 2819 groups: Ethernet statistics, history control, Ethernet history, and alarms. c. Coexistence between Version 1, Version 2, and Version 3 of the Internet-standard Network Management Framework IAW RFC 3584. d. The Advanced Encryption Standard (AES) Cipher Algorithm in the SNMP User-based Security Model IAW RFC 3826.	7.2.1.7 EDG-000170	L/T IO-16	Core (R) Distro (R) Access (R)

Table 3-5. ASLAN Component Capability/Functional Requirements (continued)

CR/FR ID	Requirement	UCR 2013 Reference (See note 1.)	LoC/ TP ID (See note 2.)	R/O/C
1-9	**7.2.1.8 – Security**			
1	The Core, Distribution, and Access products shall meet the security protocol requirements listed in Section 4, Information Assurance, as follows: Core and Distribution products shall meet all requirements annotated as Router (R) and LAN Switch (LS). Access switches shall meet the IA requirements annotated for LS. In addition to wireless IA requirements previously specified, Wireless Local Area Network Access Systems (WLASs) and Wireless Access Bridges (WABs) shall meet all IA requirements for LSs. Wireless End Instruments (WEIs) shall meet all IA requirements annotated for End Instruments (EIs). When conflicts exist between the UCR and STIG requirements, the STIG requirements will take precedence. **(Refer to Table 3-7 for applicable IA requirements)**	7.2.1.8 EDG-000180	L	Core (R) Distro (R) Access (R)
2	**7.2.2 – LAN Switch and Router Redundancy**			
2-1	**7.2.2 – LAN Switch and Router Redundancy Requirements**			
1	The ASLAN (High and Medium) shall have no single point of failure that can cause an outage of more than 96 IP telephony subscribers. A single point of failure up to and including 96 subscribers is acceptable; however, to support mission-critical needs, FLASH/FLASH OVERRIDE (F/FO) subscribers should be engineered for maximum availability. To meet the availability requirements, all switching/routing platforms that offer service to more than 96 telephony subscribers shall provide redundancy in either of two ways: a. The product itself (Core, Distribution, or Access) provides redundancy internally. b. A secondary product is added to the ASLAN to provide redundancy to the primary product (redundant connectivity required).	7.2.2 EDG-000190	T IO-1	Core (R) Distro (R) Access (R)
2-2	**7.2.2.1 – Single product Redundancy**			
1	If a single product is used to meet the redundancy requirements, then the following requirements are applicable to the product: a. Dual Power Supplies. The platform shall provide a minimum of two power supplies, each with the power capacity to support the entire chassis. Loss of a single power supply shall not cause any loss of ongoing functions within the chassis. b. Dual Processors (Control Supervisors). The chassis shall support dual-control processors. Failure of any one processor shall not cause loss of any ongoing functions within the chassis (e.g., no loss of active calls). Failure of the primary processor to secondary must meet 5-second failover without loss of active calls. c. Termination Sparing. The chassis shall support a (N + 1) sparing capability for available 10/100 Base-T modules used to terminate to an IP subscriber. d. Redundancy Protocol. Routing equipment shall support a protocol that allows for dynamic rerouting of IP packets so that no single point of failure exists in the ASLAN that could cause an outage to more than 96 IP subscribers. Redundancy protocols will be standards based as specified in this document. e. No Single Failure Point. No single point shall exist in the LAN that would cause loss of voice service to more than 96 IP telephony instruments. f. Switch Fabric or Backplane Redundancy. Switching platforms within the ASLAN shall support a redundant (1 + 1) switching fabric or backplane. The second fabric's backplane shall be in active standby so that failure of the first shall not cause loss of ongoing events within the switch.	7.2.2.1 EDG-000200	1O-2 1O-3 1O-4 1O-5 1O-7 1O-8 1O-9	Core (O) Distro (O) Access (O)
2-3	**7.2.2.2 – Dual product Redundancy**			
1	If the System Under Test (SUT) provides redundancy through dual products, then the following requirements are applicable: a. The failover over to the secondary product must not result in any lost calls. The secondary product may be in "standby mode" or "active mode," regardless of the mode of operation the traffic engineering of the links between primary and secondary must meet the requirements provided in Section 7.5.19, Traffic Engineering.	7.2.2.2 EDG-000210	1O-2 1O-3 1O-4 1O-5 1O-7 1O-8 1O-9	Core (O) Distro (O) Access (O)
3	**7.2.3 LAN Product Requirements Summary**			
3-1	Core, Distribution, and Access products must meet the requirements summarized in Table 7.2-4.	7.2.3	L	Core (R) Distro (R) Access (R)

Table 3-5. ASLAN Component Capability/Functional Requirements (continued)

CR/FR ID	Requirement	UCR 2013 Reference (See note 1.)	LoC/ TP ID (See note 2.)	R/O/C
4	**7.2.4 – Multiprotocol Label Switching in ASLANs**			
4-1	**7.2.4.2 – MPLS ASLAN**			
1	An ASLAN product that implements MPLS must still meet all the ASLAN requirements for jitter, latency, and packet loss. The addition of the MPLS protocol must not add to the overall measured performance characteristics with the following caveats: a. The MPLS device shall reroute data traffic to a secondary pre-signaled LSP in less than 5 seconds upon indication of the primary LSP failure.	7.2.4.2 EDG-000220	T (See separate MPLS test plan)	Core (O) Distro (O)
2	Assured Services LAN Core and Distribution products are not required to support MPLS. Services and Agencies may choose to implement MPLS in the ASLAN to take advantage of the inherent technological advantages of MPLS. The ASLAN Core and Distribution products that will be used to provide MPLS services must support the RFCs contained in Table 7.2-5, ASLAN Product MPLS Requirements. RFCs are listed as being REQUIRED (R), OPTIONAL (O), or CONDITIONAL (C). Optionally required RFCs are based on implementation of a particular feature, such as Virtual Private Networks (VPNs).	7.2.4.2 EDG-000230	T (See separate MPLS test plan)	Core (O) Distro (O)
4-2	**7.2.4.3 – MPLS VPN Augmentation to VLANs**			
1	The ASLAN Core or Distribution products will provide Layer 2 MPLS VPNs by minimally supporting the following: a. RFC 4762, "Virtual Private LAN Service (VPLS) Using Label Distribution Protocol (LDP) Signaling." The product may additionally support the following: b. RFC 4761, "Virtual Private LAN Services (VPLS) Using BGP for Auto-Discovery and Signaling."	7.2.4.3.1 EDG-000240	T (See separate MPLS test plan)	Core (R) Distro (R)
2	The ASLAN products used to support L2VPNs, RFC 4761, or RFC 4762 may support RFC 5501, "Requirements for Multicast Support in Virtual Private LAN Services."	7.2.4.3.1 EDG-000250	L (See separate MPLS test plan)	Core (O) Distro (O)
3	The ASLAN Core or Distribution products will provide Layer 3 MPLS VPNs by supporting RFC 4364, "BGP/MPLS IP Virtual Private Networks (VPNs)."	7.2.4.3.2 EDG-000260	T (See separate MPLS test plan)	Core (R) Distro (R)
4	The ASLAN products used to support L3VPNs by RFC 4364 shall support the following RFCs: a. RFC 4382, "MPLS/BGP Layer 3 Virtual Private Network (VPN) Management Information Base." b. RFC 4577, "OSPF as the Provider/Customer Edge Protocol for BGP/MPLS IP Virtual Private Networks (VPNs)." c. RFC 4659, "BGP-MPLS IP Virtual Private Network (VPN) Extension for IPv6 VPN." d. RFC 4684, "Constrained Route Distribution for Border Gateway Protocol/Multiprotocol Label Switching (BGP/MPLS) Internet Protocol (IP) Virtual Private Networks (VPNs)."	7.2.4.3.2 EDG-000270	T (See separate MPLS test plan)	Core (R) Distro (R)
5	The MPLS device must support QoS in order to provide for assured services. The product must support one of the following QoS mechanisms: a. DSCP mapping to 3 bit EXP field (E-LSP). b. Label description of PHB (L-LSP).	7.2.4.3.3 EDG-000280	T (See separate MPLS test plan)	Core (R) Distro (R)

Table 3-5. ASLAN Component Capability/Functional Requirements (continued)

CR/FR ID	Requirement	UCR 2013 Reference (See note 1.)	LoC/ TP ID (See note 2.)	R/O/C
5	**7.3 – Wireless LANs**			
5-1	**7.3.1 – General Wireless Product**			
1	The following general wireless requirements must be ASLAN wireless components: a. If an IP interface is provided in any of the wireless components, then it shall meet the IP requirements detailed in the DoD Profile for IPv6. b. 802.11 wireless products must be WiFi Alliance Certified and shall be certified at the Enterprise level for WiFi Protected Access 2 (WPA2). The products will also be Wi-Fi multimedia (WMM) certified. c. For wireless products that provide transport to more than 96 (I/P) telephony users, the wireless products shall provide redundancy, and WLAS and/or associated controller/ switches that provide and/or control voice services to more than 96 WEIs shall provide redundancy through one of the following: (1) Single Product Redundancy. Shall have the following as a minimum: Dual power supplies/processors/radio systems/Ethernet ports and no single point of failure for more than 96 subscribers. It should be noted that single point of failure may exist for more than 96 subscribers if 96 or fewer are IP telephone subscribers (i.e., 50 data, 20 video, and 50 IP telephony = 120 subscribers). (2) Dual Product Redundancy. Shall be collocated or co-adjacent and shall have the following as a minimum: Traffic engineering to support all users on a single product upon failure of the other product. Secondary product may be on full standby or traffic sharing, supporting 50 percent of the traffic before failure rollover. Products must support a redundancy protocol. d. All wireless connections shall be Federal Information Processing Standard (FIPS) 140-2 Level 1 certified (connections may either be WEI to WLAS if both support FIPS 140-2 Level 1, or WEI to a FIPS 140-2 compliant product through a WLAS if the WLAS is not capable of FIPS 140-2 Level 1). Wireless products that comprise the WLAN shall be secured in accordance with their wireless security profile as follows: (1) FIPS 140-2, Level 1. Wireless components must be operated from within a "limited access, secure room" and be under user positive control at all times. However, if the wireless end item is designed to be left unattended or is designed as an item that can be left behind, such as a wireless free-standing desk telephone, then that wireless end item must be Level 2 compliant. (2) FIPS 140-2, Level 2. Wireless components can be operated in an open public area such as an "open hallway," but the use of a "limited access, secure room" if available and/or operationally feasible is recommended. e. The use of wireless in the LAN as a bridging function shall not increase latency by more than 10 ms for each bridging pair. The use of wireless via an access point shall not increase LAN latency by more than 15 ms (see UCR Framework 2013 on wireless). f. The wireless products shall support LAN Traffic Prioritization and QoS IAW the following based on the wireless interface type: (1) 802.11 Interfaces. Wireless products using 802.11 shall use the settable Service Class tagging/QoS parameters within 802.11-2012 to implement mapping to the prescribed DSCP values. The product shall support WMM. Wireless mobile devices shall also support WMM Power Save. (2) 802.16 Interfaces. Wireless products using 802.16 QoS/Service Class tagging shall meet the following requirements: (a) The WLAN products may use 802.16 (IAW 802.16-2012) to provide QoS over the wireless portion of the transport. (b) The WLAS and WABs shall mark traffic traversing into the wired portion of the LAN with appropriate wired DSCPs (see Table 7.3-1, 802.16 Service Scheduling).	7.3.1 EDG-000290	T (See separate Wireless test plan)	Wireless Product (R)

Table 3-5. ASLAN Component Capability/Functional Requirements (continued)

CR/FR ID	Requirement	UCR 2013 Reference (See note 1.)	LoC/ TP ID (See note 2.)	R/O/C
5-1	**7.3.1 – General Wireless Product (continued)**			
1 (continued)	g. Wireless products shall meet the security requirements as stipulated in the Wireless STIG and the following specified requirements: (1) All 802.11 wireless components shall do the following: (a) Use the AES-Counter with Cipher Block Chaining-Message Authentication Code Protocol (CCMP) (AES-CCMP). It will be implemented in 802.11-2012 system encryption modules. (b) Implement the Extensible Authentication Protocol – Transport Layer Security (EAP-TLS) mutual authentication for the EAP component of Wi-Fi Protected Access (WPA2). Wireless access systems shall meet the access product requirements in Section 7.2.	7.3.1 EDG-000290	L/T (See separate Wireless test plan)	Wireless Product (R)
2	Wireless systems may use the Control and Provisioning of Wireless Access Points (CAPWAP) Protocol IAW RFC 5415 and RFC 5416.	7.3.1 EDG-0001000.a	T (See separate Wireless test plan)	Wireless Products (O)
5-2	**7.3.2 Wireless Interfaces**			
1	If a wireless product is used, the wireless product shall support at least one of the following approved wireless LAN standards interfaces: a. 802.11a IAW 802.11-2007 – 5 GHz. b. 802.11b IAW 802.11-2007 – 2.4GHz. c. 802.11g IAW 802.11-2007 – 2.4 GHz. d. 802.11n-2009 – 2.4 GHz and 5 GHz. e. 802.16-2012.	7.3.2 EDG-000300	L/T (See separate Wireless test plan)	WEI (R) WLAS (R)
2	For any of the 802.11 interfaces, the wireless product must minimally support the following two 802.11 standards: a. 802.11e – Part 11. Wireless LAN Medium Access Control (MAC) and Physical Layer (PHY) specifications and Amendment 8: Medium Access Control (MAC) Quality of Service Enhancements. See, for priority bit assignment. b. 802.11i – Part 11. Wireless LAN Medium Access Control (MAC) and Physical Layer (PHY) specifications and Amendment 6: Medium Access Control (MAC) Security Enhancements.	7.3.2 EDG-000310	L/T (See separate Wireless test plan)	WEI (R) WLAS (R)
3	For the 802.11a interface, the wireless product must support the standard 802.11h – Part 11: Wireless LAN Medium Access Control (MAC) and Physical Layer (PHY) specifications, Amendment 5: Spectrum and Transmit Power Management Extensions in the 5 GHz band in Europe.	7.3.2 EDG-000320	L/T (See separate Wireless test plan)	WEI (R) WLAS (R)
4	For any of the 802.16-2012 interfaces, the wireless product must support the following 802.16-2012 standards dependent on whether the end item attached to the WLAS is "fixed" or "nomadic." Fixed WEIs are those WEIs that access a single WLAS during the session and are not expected to traverse between WLASs so that handoffs are not required. Fixed WEIs must support 802.16-2012 requirements. Nomadic WEIs are those WEIs that are mobile and may traverse different WLASs during a single session (i.e., handoffs are seamless from the user perspective). Nomadic WEIs must support 802.16-2012.	7.3.2 EDG-000330	T (See separate Wireless test plan)	WEI (R) WLAS (R)

Table 3-5. ASLAN Component Capability/Functional Requirements (continued)

CR/FR ID	Requirement	UCR 2013 Reference (See note 1.)	LoC/ TP ID (See note 2.)	R/O/C
5-3	**7.3.3 Wireless End Instruments**			
1	The following requirements apply. a. Wireless VoIP EIs are certified as part of the VoIP solution (i.e., Session Controller [SC]) unless they are wireless Audio End Instruments (Wireless Audio End Instruments shall meet all Audio End Instrument requirements as well as meet the wireless interface requirements listed in this section). b. Access to/from a WEI shall be provided by either 802.11 or 802.16. Two methods that an IP subscriber can use to access voice services are dedicated wireless service or shared wireless service (see Figure 7.3-1, Access Methods for the Wireless Access Layer End Item Product Telephones). The dedicated access method provides wireless access service for a single type of traffic (i.e., voice, video, or data – three devices are required to support all traffic types). The shared access method allows a single wireless WLAS to provide for all traffic types supported (i.e., voice, video, and data – one device provides all three traffic types), on all computer types and/or Personal Electronic Device (PED) to connect to the wireless WLAS. c. WEIs may use either method separately or a combination to provide wireless access (see Figure 7.3-1, Access Methods for the Wireless Access Layer End Item Product Telephones). d. WEIs or soft clients on workstations acting as WEIs shall authenticate to the VoIP system call control. Authentication shall be IAW UCR IA-specified requirements. e. The WEI is associated with the supporting IP telephone switch. The WEI shall be functionally identical to a traditional IP wired telephone and will be required to provide voice features and functionality IAW other UCR specified requirements unless explicitly stated. f. Minimally, all WEIs shall be FIPS 140-2 Level 2 compliant. g. If the WEI loses connection with the VoIP switch when using a WLAN, the call will be terminated by the VoIP switch. The termination period shall be determined by the VoIP switch using a configurable time-out parameter with a time-out range of 0–60 seconds; default shall be set to 5 seconds. The subscriber line will be treated as if it were out of service until communication is re-established with the wireless voice end instrument.	7.3.3 EDG-000340	T (See separate Wireless test plan)	WEI (R)

Table 3-5. ASLAN Component Capability/Functional Requirements (continued)

CR/FR ID	Requirement	UCR 2013 Reference (See note 1.)	LoC/ TP ID (See note 2.)	R/O/C
5-4	**7.3.4 Wireless LAN Access System**			
1	If a WLAS is used as part of the LAN design supporting VoIP subscribers, the following requirements must be met: a. Failure of a WLAS shall not cause the loss of a call as the connection transfers from the primary to alternate system. However, it may allow a single momentary 5-second delay in voice bearer traffic in both directions of the wireless link as wireless VoIP telephone clients are re-authenticated to the standby system. The 5-second voice delay will not be factored into the overall Mean Opinion Score (MOS). b. The WLAS shall support the following maximum number of EIs per Table 7.3-2, Maximum Number of EIs Allowed per WLAS, for converged or non-converged access for redundant and non-redundant WLAS; while not degrading any of the individual EIs' voice quality below the specified MOS of 3.8 for strategic, 3.4 for wireless strategic-tactical, and 3.0 for tactical. c. At the point when voice quality degradation occurs, defined as a MOS score below appropriate levels (i.e., Strategic 4.0, Strategic-to-Tactical 3.6, and Tactical-to-Tactical 3.2), when all telephones are off-hook simultaneously, this becomes the maximum number of telephones and/or other wireless non-voice end item products that the WLAS can support for the WLAS transmitter coverage distance. d. The WLAS shall not drop an active call as the WEI roams from one WLAS transmitter zone into another WLAS transmitter zone. The source and destination WLAS transmitters involved in the roaming are connected to the same WLAS controller or are otherwise part of the same WLAS. e. The addition of the WLAS shall not cause the one-way delay measured from ingress to egress to increase by more than 3 ms, averaged over any 5-minute period. f. The addition of WLAS shall not increase the LAN jitter requirements previously specified in this section by more than an additional 3 ms. g. Minimally, WLAS products shall provide one of the following trunk-side interface (ASLAN network side) rates (other rates and IEEE standards may be provided as optional interfaces): • 10 Mbps IAW IEEE 802.3i. • 10 Mbps IAW IEEE 802.3j. • 100 Mbps IAW IEEE 802.3u. • 1000 Mbps IAW IEEE 802.3z. • 1000 Mbps IAW IEEE 802.3ab.	7.3.4 EDG-000350	L	WLAS (R)

Table 3-5. ASLAN Component Capability/Functional Requirements (continued)

CR/FR ID	Requirement	UCR 2013 Reference (See note 1.)	LoC/ TP ID (See note 2.)	R/O/C
5-5	**7.3.5 Wireless Access Bridge**			
1	The WAB will be required to meet all the following requirements for each individual type interface. a. The WAB shall minimally provide one wireless interface that serves as the communication path between WAB components. The WAB shall also provide a wired interface to connect to the ASLAN components. Minimally, WAB products shall provide one of the following wired trunk-side (ASLAN network side) interface rates (other rates and IEEE standards may be provided as optional interfaces): • 10 Mbps IAW IEEE 802.3i. • 10 Mbps IAW IEEE 802.3j. • 100 Mbps IAW IEEE 802.3u. • 1000 Mbps IAW IEEE 802.3z. • 1000 Mbps IAW IEEE 802.3ab. In addition, the WAB must provide one of the following wireless interfaces: (1) 802.16 interfaces. If supported, the WAB must support 802.16-2012. The product must support 802.16 QoS specified in Section 7.3.1, General Wireless Product. (2) 802.11 interfaces, the WAB must meet a minimum of one of 802.11standards (802.11a, b, g, or n). The product must support 802.11 QoS specified in Section 7.3.1. (3) For the wireless interface, vendors may support a pair-wise proprietary wireless technology. The interface must support a QoS mechanism (e.g., DSCP or 802.1 L2 tag [aka 802.1p]) to support assured services transport of prioritized traffic (if congestion or over subscription is possible). The interface must transport and not modify the existing layer 3 DSCP value. b. The maximum number of voice calls transported across the WAB shall be in accordance with Section 7.15.19, Traffic Engineering. Maximum voice users will be determined by the smallest link size (i.e., Ethernet connection to the WAB or the WAB wireless link speed of the WAB itself). c. The introduction of WAB(s) shall not cause the End-to-End (E2E) average MOS to fall below appropriate levels (Strategic 4.0, Strategic-to-Tactical 3.6, and Tactical-to-Tactical 3.2) as measured over any 5-minute time interval. d. The introduction of WAB(s) shall not increase packet loss by more than 20 percent over the LAN requirement of 0.015 percent. e. The WAB shall not modify call control signals that are transported through it. f. The addition of WAB(s) shall not cause the one-way delay measured from ingress to egress to increase by more than 3 ms for each WAB used, averaged over any 5-minute period. g. The addition of WAB(s) shall not increase the LAN jitter requirements previously specified in this section by more than an additional 3 ms. a. A WAB may simultaneously act as a WLAS. h. A WAB may optionally support mesh networking. If provided, mesh networking must meet the requirements of IEEE 802.11s-2011.	7.3.5 EDG-000360	L/T (See separate Wireless test plan)	WAB (R)
2	The WLAS/WAB combination must meet all the requirements for access (WLAS) and bridging (WAB). a. The WAB(s) and/or WLAS/WAB shall support Service Class tagging/QoS as previously specified in this section.	7.3.5 EDG-000370	L/T (See separate Wireless test plan)	WLAS (R) WAB (R)

Table 3-5. ASLAN Component Capability/Functional Requirements (continued)

CR/FR ID	Requirement	UCR 2013 Reference (See note 1.)	LoC/ TP ID (See note 2.)	R/O/C
5-6	**7.3.6 Survivability**			
1	Network survivability refers to the capability of the network to maintain service continuity in the presence of faults within the network. This can be accomplished by recovering quickly from network failures quickly and maintaining the required QoS for existing services. For the ASLAN, survivability needs to be inherent in the design. The following guidelines are provided for the ASLAN: • Layer 3 Dynamic Rerouting. The ASLAN products that route (normally the Distribution and Core Layers) shall use routing protocols IAW the DoD Information Technology (IT) Standards Registry (DISR) to provide survivability. The minimum routing protocols that must be supported are as follows: • Border Gateway Protocol (BGP) for inter-domain routing (Required: Core products). • Open Shortest Path First (OSPF), Version 2, for IPv4 and OSPF Version 3 for IPv6, July 2008, and IAW RFC 5340 (Required: Core and Distribution products). • OSPFv2 Graceful restart (RFC 3623) and OSPFv3 Graceful Restart (RFC 5187) are required (18-month rule) for Core and Distribution products. It is not applicable to access devices unless routing (OSPF) provided. • Graceful Restart for BGP (RFC 4724) is required (18-month rule) for core and distribution infrastructure products. • Layer 2 Dynamic Rerouting: • Virtual Router Redundancy Protocol (VRRP) – RFCs 2787 and RFC 5798. VRRP is able to provide redundancy to Layer 2 switches that lose connectivity to a Layer 3 router. The Distribution product shall employ VRRP to provide survivability to any product running Layer 2 (normally the Access Layer).	7.3.6	L	

NOTES:
1. The requirements are derived from the UCR 2013, Errata 1, Reference (c).
2. Refers to the methodology for requirement verification via LoC "L", test "T", or both "L/T". Test items include test procedure number(s).

LEGEND:

AES	Advanced Encryption Standard
ANSI	American National Standards Institute
ASLAN	Assured Services Local Area Network
BGP	Border Gateway Protocol
BW	Bandwidth
C	Conditional
CoS	Class of Service
CR	Capability Requirement
DoD	Department of Defense
DS	Differentiated Services
DSCP	Differentiated Services Code Point
EI	End Instrument
FIPS	Federal Information Processing Standard
FR	Functional Requirement
GHz	GigaHertz
I/P	IMMEDIATE/PRIORITY
IA	Information Assurance
IAW	in accordance with
ID	Identification
IEEE	Institute of Electrical and Electronics Engineers
IP	Internet Protocol
IPv4	Internet Protocol version 4
IPv6	Internet Protocol version 6
kbps	kilobits per second
LAN	Local Area Network
LoC	Letters of Compliance
LSP	Label Switched Path
MAN	Metropolitan Area Network
Mbps	Megabits per second
MOS	Mean Opinion Score
MPLS	Multiprotocol Label Switching
ms	milliseconds
N/A	Not Applicable
NM	Network Management
O	Optional
PHB	Per Hop Behavior
PPP	Point-to-Point Protocol
QoS	Quality of Service
R	Required
RFC	Request for Comments
SNMP	Simple Network Management Protocol
STIG	Security Technical Implementation Guides
TP	Test Plan
UC	Unified Capabilities
UCR	Unified Capabilities Requirements
VID	VLAN ID
VLAN	Virtual Local Area Network
VoIP	Voice over Internet Protocol
VRRP	Virtual Router Redundancy Protocol
VVoIP	Voice and Video over Internet Protocol
WAB	Wireless Access Bridge
WAN	Wide Area Network
WEI	Wireless End Instrument
WLAS	Wireless LAN Access System

Table 3-6. ASLAN Component IPv6 Requirements

ID	Requirement	UCR 2013 Reference (See note 1.)	LoC/ TP ID (See note 2.)	R/O/C
UCR 2013 Section 5 IPv6 Requirements				
IP-1	**5.2.1 – Product**			
1	The product shall support dual IPv4 and IPv6 stacks as described in RFC 4213. [Conditional: LS] If the Local Area Network (LAN) Switch (LS) also supports a routing function, then the product shall also support dual IPv4 and IPv6 stacks as described in RFC 4213	5.2.1 IP6-000010	L/T IO-10 IO-11 IO-12	Core (R) Distro (C) Access (C)
2	Dual-stack end points shall be configured to choose IPv4 over IPv6.	5.2.1 IP6-000020	L	Core (C) Distro (R) Access (R)
3	All nodes and interfaces that are "IPv6-capable" must be carefully configured and verified that the IPv6 stack is disabled until it is deliberately enabled as part of a deliberate transition strategy. This includes the stateless autoconfiguration of link-local addresses. Nodes with multiple network interfaces may need to be separately configured per interface	5.2.1 IP6-000030	L	Core (R) Distro (R) Access (R)
4	If the LS supports a routing function, then the product shall support the manual tunnel requirements as described in RFC 4213.	5.2.1 IP6-000040	L	Core (C) Distro (C) Access (C)
5	The system shall provide the same (or equivalent) functionality in IPv6 as in IPv4 consistent with the requirements in the UCR for its Approved Products List (APL) category. NOTE: This requirement applies only to products that are required to perform IPv6 functionality and the feature parity is limited to the functionality tested in accordance with the distributed test laboratory approved test procedures for the category of the product.	5.2.1 IP6-000050	L/T IO-10 IO-11 IO-12	Core (R) Distro (R) Access (R)
6	Support IPv6 IAW RFCs 2460 and 5095 if routing functions are supported.	5.2.1 IP6-000060	L/T IO-10 IO-11 IO-12	Core (R) Distro (C) Access (C)
7	The product shall support the transmission of IPv6 packets over Ethernet networks using the frame format defined in RFC 2464.	5.2.1 IP6-000070	L/T IO-10 IO-11 IO-12	Core (R) Distro (R) Access (R)
IP1-1	**5.2.1.1 – Maximum Transmission Unit**			
1	The product shall support Path Maximum Transmission Unit (MTU) Discovery as described in RFC 1981.	5.2.1.1 IP6-000080	L	Core (R) Distro (R) Access (R)
2	The product shall support a minimum MTU of 1280 bytes as described in RFC 2460 and updated by RFC 5095.	5.2.1.1 IP6-000090	L/T IO-10 IO-11 IO-12	Core (R) Distro (R) Access (R)
IP1-2	**5.2.1.2 – Flow Label**			
1	The product shall not use the Flow Label field as described in RFC 2460.	5.2.1.2 IP6-000110	L	Core (R) Distro (R) Access (R)
2	The product shall be capable of setting the Flow Label field to zero when originating a packet.	5.2.1.2 IP6-000120	L	Core (R) Distro (R) Access (R)
3	The product shall not modify the Flow Label field when forwarding packets.	5.2.1.2 IP6-000130	L	Core (R) Distro (R) Access (R)
4	The product shall be capable of ignoring the Flow Label field when receiving packets.	5.2.1.2 IP6-000140	L	Core (R) Distro(R) Access (R)

Table 3-6. ASLAN Component IPv6 Requirements (continued)

ID	Requirement	UCR 2013 Reference (See note 1.)	LoC/ TP ID (See note 2.)	R/O/C
IP1-3	**5.2.1.3 – Address**			
1	The product shall support the IPv6 Addressing Architecture as described in RFC 4291.	5.2.1.3 IP6-000150	L/T IO-10 IO-11 IO-12	Core (R) Distro (R) Access (R)
2	The product shall support the IPv6 Scoped Address Architecture as described in RFC 4007.	5.2.1.3 IP6-000160	L/T IO-10 IO-11 IO-12	Core (R) Distro (R) Access (R)
3	If a scoped address (RFC 4007) is used, then the product shall use a scope index value of zero when the default zone is intended.	5.2.1.3 IP6-000170	L	Core (C) Distro (C) Access (C)
IP1-4	**5.2.1.4 – Dynamic Host Configuration Protocol**			
1	If Dynamic Host Configuration Protocol (DHCP) is supported within an IPv6 environment, then it shall be implemented in accordance with the DHCP for IPv6 (DHCPv6) as described in RFC 3315.	5.2.1.3 IP6-000180	L	Core (C) Distro (C) Access (C)
2	If the LS supports DHCP and a routing function, then the product shall support RFC 3315.	5.2.1.4 IP6-000190	L/T IO-10 IO-11 IO-12	Core (C) Distro (C) Access (C)
3	If the product supports DHCPv6 and uses authentication, then it shall discard unauthenticated DHCPv6 messages from UC products and log the event.	5.2.1.4 IP6-000270	L	Core (C) Distro (C) Access (C)
IP1-5	**5.2.1.5 – Neighbor Discovery**			
1	The product shall support Neighbor Discovery for IPv6 as described in RFC 4861.	5.2.1.4 IP6-000280	L	Core (R) Distro (C) Access (C
2	If the LS also supports a routing function, then the product shall support RFC 4861.	5.2.1.4 IP6-000290	L	Distro (C) Access (C)
3	The product shall not set the override flag bit in the Neighbor Advertisement message for solicited advertisements for any cast addresses or solicited proxy advertisements.	5.2.1.5 IP6-000300	L	Core (R) Distro (R) Access (R)
4	When a valid "Neighbor Advertisement" message is received by the product and the product neighbor cache does not contain the target's entry, the advertisement shall be silently discarded.	5.2.1.5 IP6-000310	L	Core (R) Distro (R) Access (R)
5	When a valid "Neighbor Advertisement" message is received by the product and the product neighbor cache entry is in the INCOMPLETE state when the advertisement is received and the link layer has addresses and no target link-layer option is included, the product shall silently discard the received advertisement.	5.2.1.5 IP6-000320	L	Core (R) Distro (R) Access (R)
6	When address resolution fails on a neighboring address, the entry shall be deleted from the product's neighbor cache.	5.2.1.5.1 IP6-000330	L	Core (R) Distro (R) Access (R)
7	If the product supports routing functions, then the product shall inspect valid router advertisements sent by other routers and verify that the routers are advertising consistent information on a link and shall log any inconsistent router advertisements.	5.2.1.5.2 IP6-000390	L	Core (R) Distro (C) Access (C)
8	If the product supports routing functions, then the product shall be capable of supporting the MTU value in the router advertisement message for all links in accordance with RFC 4861.	5.2.1.5.2 IP6-000410	L	Core (R) Distro (C) Access (C)

Table 3-6. ASLAN Component IPv6 Requirements (continued)

ID	Requirement	UCR 2013 Reference (See note 1.)	LoC/ TP ID (See note 2.)	R/O/C
IP1-6	**5.2.1.6 Stateless Address Autoconfiguration and Manual Address Assignment**			
1	If the product supports stateless IP address autoconfiguration including those provided for the commercial market, then the product shall support IPv6 Stateless Address Autoconfiguration (SLAAC) for interfaces supporting UC functions in accordance with RFC 4862.	5.2.1.6 IP6-000420	L	Core (C) Distro (C) Access (C)
2	If the product supports IPv6 SLAAC, then the product shall have a configurable parameter that allows the function to be enabled and disabled. Specifically, the product shall have a configurable parameter that allows the "managed address configuration" flag and the "other stateful configuration" flag to always be set and not perform stateless autoconfiguration.	5.2.1.6 IP6-000430	L	Core (C) Distro (C) Access (C)
3	If the product supports IPv6 SLAAC, then the product shall have the configurable parameter set not to perform stateless autoconfiguration.	5.2.1.6 IP6-000440	L	Core (C) Distro (C) Access (C)
4	While nodes are not required to autoconfigure their addresses using SLAAC, all IPv6 Nodes shall support link-local address configuration and Duplicate Address Detection (DAD) as specified in RFC 4862. In accordance with RFC 4862, DAD shall be implemented and shall be on by default. Exceptions to the use of DAD are noted in the following text.	5.2.1.6 IP6-000450	L	Core (R) Distro (R) Access (R)
5	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.	5.2.1.6 IP6-000460	L	Core (R) Distro (R) Access (R)
6	The product shall support manual assignment of IPv6 addresses.	5.2.1.6 IP6-000470	T IO-10 IO-11 IO-12	Core (R) Distro (R) Access (R)
7	If the product provides routing functions, then the product shall default to using the "managed address configuration" flag and the "other stateful flag" set to TRUE in their router advertisements when stateful autoconfiguration is implemented.	5.2.1.6 IP6-000490	L	Core (R) Distro (C) Access (C)
IP1-7	**5.2.1.7 – Internet Control Message Protocol**			
1	The product shall support the Internet Control Message Protocol (ICMP) for IPv6 as described in RFC 4443.	5.2.1.7 IP6-000520	T IO-10 IO-11 IO-12	Core (R) Distro (R) Access (R)
2	The product shall have a configurable rate-limiting parameter for rate limiting the ICMP error messages it originates.	5.2.1.7 IP6-000530	L	Core (R) Distro (R) Access (R)
3	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.	5.2.1.7 IP6-000540	L	Core (R) Distro (R) Access (R)
4	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.	5.2.1.7 IP6-000550	L	Core (R) Distro (R) Access (R)
5	The product shall validate ICMPv6 messages, using the information contained in the payload, before acting on them.	5.2.1.7 IP6-000560	L	Core (R) Distro (R) Access (R)
IP1-8	**5.2.1.8 – Routing Functions**			
1	If the product supports routing functions, then the product shall support the Open Shortest Path First (OSPF) for IPv6 as described in RFC 5340.	5.2.1.8 IP6-000570	L	Core (R) Distro (C) Access (C)
2	If the product supports routing functions, then the product shall support securing OSPF with IPSec as described for other IPSec instances in Section 4, Information Assurance.	5.2.1.8 IP6-000580	L	Core (R) Distro (C) Access (C)
3	If the product supports routing functions, then the product shall support router-to-router integrity using the IP Authentication Header with HMACSHA1- 96 within Encapsulating Security Payload (ESP) and Authentication Header (AH) as described in RFC 2404.	5.2.1.8 IP6-000590	L	Core (R) Distro (C) Access (C)
4	If the product supports interior routing functions of OSPFv3, then the product shall support RFC 4552.	5.2.1.8 IP6-000600	L	Core (R) Distro (C) Access (C)

Table 3-6. ASLAN Component IPv6 Requirements (continued)

ID	Requirement	UCR 2013 Reference (See note 1.)	LoC/ TP ID (See note 2.)	R/O/C
IP1-8	**5.2.1.8 – Routing Functions (continued)**			
5	If the product supports the Intermediate System to Intermediate System (IS-IS) routing protocol used in DoD backbone networks, then the product shall support the IS-IS for IPv6 as described in RFC 5308.	5.2.1.8 IP6-000610	L	Core (C) Distro (C) Access (C)
6	If the product supports IS-IS routing architecture (for IPv6-only or dual-stack operation), then the product shall support RFC 5304 and RFC 5310 and shall support RFC 6119 for IPv6 traffic engineering.	5.2.1.8 IP6-000620	L	Core (C) Distro (C) Access (C)
8	If the product supports routing functions, then the product shall support the Multicast Listener Discovery (MLD) process as described in RFC 2710 and extended in RFC 3810. a. If the product supports MLD process as described in RFC 2710 and extended in RFC 3810, then the product shall support RFC 2711.	5.2.1.8 IP6-000670	L	Core (R) Distro (C) Access (C)
IP1-9	**5.2.1.9 – IP Security**			
1	If the product uses IPSec, then the product shall be compatible with the Security Architecture for the IPSec described in RFC 4301. b. If RFC 4301 is supported, then the product shall support binding of a SA with a particular context. c. If RFC 4301 is supported, then the product shall be capable of disabling the BYPASS IPSec processing choice.	5.2.1.9 IP6-000690	L	Core (R) Distro (C) Access (C)
2	If RFC 4301 is supported, then the product shall not support the mixing of IPv4 and IPv6 in a SA.	5.2.1.9 IP6-000700	L	Core (R) Distro (C) Access (C)
3	If RFC 4301 is supported, then the product's security association database (SAD) cache shall have a method to uniquely identify a SAD entry.	5.2.1.9 IP6-000710	L	Core (R) Distro (C) Access (C)
4	If RFC 4301 is supported, then the product shall implement IPSec to operate with both integrity and confidentiality.	5.2.1.9 IP6-000720	L	Core (R) Distro (C) Access (C)
5	If RFC 4301 is supported, then the product shall be capable of enabling and disabling the ability of the product to send an ICMP message informing the sender that an outbound packet was	5.2.1.9 IP6-000730	L	Core (R) Distro (C) Access (C)
6	If an ICMP outbound packet message is allowed, then the product shall be capable of rate limiting the transmission of ICMP responses.	5.2.1.9 IP6-000740	L	Core (R) Distro (C) Access (C)
7	If RFC 4301 is supported, then the system's Security Policy Database (SPD) shall have a nominal, final entry that discards anything unmatched.	5.2.1.9 IP6-000750	L	Core (R) Distro (C) Access (C)
8	If RFC 4301 is supported, and the product receives a packet that does not match any SPD cache entries, and the product determines it should be discarded, then the product shall log the event and include the date/time, Security Parameter Index (SPI) if available, IPSec protocol if available, source and destination of the packet, and any other selector values of the packet.	5.2.1.9 IP6-000760	L	Core (R) Distro (C) Access (C)
9	If RFC 4301 is supported, then the product should include a management control to allow an administrator to enable or disable the ability of the product to send an IKE notification of an INVALID_SELECTORS.	5.2.1.9 IP6-000770	L	Core (R) Distro (C) Access (C)
10	If RFC 4301 is supported, then the product shall support the ESP Protocol in accordance with RFC 4303.	5.2.1.9 IP6-000780	L	Core (R) Distro (C) Access (C)
11	If RFC 4303 is supported, then the product shall be capable of enabling anti-replay.	5.2.1.9 IP6-000790	L	Core (R) Distro (C) Access (C)
12	If RFC 4303 is supported, then the product shall check, as its first check, after a packet has been matched to its SA whether the packet contains a sequence number that does not duplicate the sequence number of any other packet received during the life of the security association.	5.2.1.9 IP6-000800	L	Core (R) Distro (C) Access (C)
13	If RFC 4301 is supported, then the product shall support IKEv1 as defined in RFC 2409.	5.2.1.9 IP6-000810	L	Core (R) Distro (C) Access (C)

Table 3-6. ASLAN Component IPv6 Requirements (continued)

ID	Requirement	UCR 2013 Reference (See note 1.)	LoC/ TP ID (See note 2.)	R/O/C
IP1-9	**5.2.1.9 – IP Security (continued)**			
14	To prevent a Denial of Services (DoS) attack on the initiator of an IKE_SA, the initiator shall accept multiple responses to its first message, treat each as potentially legitimate, respond to it, and then discard all the invalid half-open connections when it receives a valid cryptographically protected response to any one of its requests. Once a cryptographically valid response is received, all subsequent responses shall be ignored whether or not they are cryptographically valid.	5.2.1.9 IP6-000820	L	Core (C) Distro (C) Access (C)
15	If RFC 4301 is supported, then the product shall support extensions to the Internet IP Security Domain of Interpretation for the Internet Security Association and Key Management Protocol (ISAKMP) as defined in RFC 2407.	5.2.1.9 IP6-000830	L	Core (R) Distro (C) Access (C)
16	If RFC 4301 is supported, then the product shall support the ISAKMP as defined in RFC 2408.	5.2.1.9 IP6-000840	L	Core (R) Distro (C) Access (C)
17	If the product supports the IPSec Authentication Header Mode, then the product shall support the IP Authentication Header (AH) as defined in RFC 4302.	5.2.1.9 IP6-000850	L	Core (R) Distro (C) Access (C)
18	If RFC 4301 is supported, then the product shall support manual keying of IPSec.	5.2.1.9 IP6-000860	L	Core (R) Distro (C) Access (C)
19	If RFC 4301 is supported, then the product shall support the ESP and AH cryptographic algorithm implementation requirements as defined RFC 4835	5.2.1.9 IP6-000870	L	Core (R) Distro (C) Access (C)
20	If RFC 4301 is supported, then the product shall support the IKEv1 security algorithms as defined in RFC 4109.	5.2.1.9 IP6-000880	L	Core (R) Distro (C) Access (C)
IP1-10	**5.2.1.10 – Network Management**			
1	If IPv6-compatible nodes are managed via Simple Network Management Protocol (SNMP) using IPv6, then the product shall comply with the Management Information Base (MIB) for IPv6 textual conventions and general group as defined in RFC 4293.	5.2.1.10 IP6-000890	L	Core (C) Distro (C) Access (C)
2	If the product performs routing functions and if IPv6-capable nodes are managed via SNMP management using IPv6, then the product shall support the SNMPv3 management framework as described in RFC 3411.	5.2.1.10 IP6-000900	L	Core (C) Distro (C) Access (C)
3	If the product performs routing functions and if IPv6-capable nodes are managed via SNMP management using IPv6, then the product shall support SNMPv3 message processing and dispatching as described in RFC 3412.	5.2.1.10 IP6-000910	L	Core (C) Distro (C) Access (C)
4	If the product performs routing functions and if IPv6-capable nodes are managed via SNMP management using IPv6, then the product shall support the SNMPv3 applications as described in RFC 3413.	5.2.1.10 IP6-000920	L	Core (C) Distro (C) Access (C)
5	If IPv6-compatible nodes are managed via SNMP using IPv6, then the product shall support the IP MIBs as defined in RFC 4293.	5.2.1.10 IP6-000930	L	Core (C) Distro (C) Access (C)
6	If IPv6-compatible nodes are managed via SNMP using IPv6, then the product shall support the Transmission Control Protocol (TCP) MIBs as defined in RFC 4022.	5.2.1.10 IP6-000940	L	Core (C) Distro (C) Access (C)
7	If IPv6-compatible nodes are managed via SNMP using IPv6, then the product shall support the User Datagram Protocol (UDP) MIBs as defined in RFC 4113.	5.2.1.10 IP6-000950	L	Core (C) Distro (C) Access (C)
8	If IPv6-compatible nodes are managed via SNMP using IPv6, and the product performs routing functions and tunneling functions, then the product shall support IP tunnel MIBs as described in RFC 4087.	5.2.1.10 IP6-000960	L	Core (C) Distro (C) Access (C)
9	If the product performs routing functions and is managed by SNMP using IPv6, then the product shall support the IP Forwarding MIB as defined in RFC 4292.	5.2.1.10 IP6-000970	L	Core (C) Distro (C) Access (C)
10	If the product supports routing functions, and the IPSec policy database is configured through SNMPv3 using IPv6, then the product shall support RFC 4807.	5.2.1.10 IP6-000980	L	Core (C) Distro (C) Access (C)

Table 3-6. ASLAN Component IPv6 Requirements (continued)

ID	Requirement	UCR 2013 Reference (See note 1.)	LoC/ TP ID (See note 2.)	R/O/C
IP1-10	**5.2.1.10 – Network Management (continued)**			
11	If the product uses Uniform Resource Identifiers (URIs) in combination with IPv6, then the product shall use the URI syntax described in RFC 3986.	5.2.1.10 IP6-000990	L	Core (C) Distro (C) Access (C)
IP1-11	**5.2.1.11 – Traffic Engineering**			
1	For traffic engineering purposes, the bandwidth required per voice subscriber is calculated to be 110.0 kbps (each direction) for each IPv6 call. This is based on G.711 (20 ms codec) with IP overhead (100 kbps) resulting in a 250-byte bearer packet plus 10 kbps for signaling, Ethernet Interframe Gap, and the Secure Real-Time Transport Control Protocol (SRTCP) overhead. Based on overhead bits included in the bandwidth calculations, vendor implementations may use different calculations and hence arrive at slightly different numbers.	5.2.1.11 IP6-001010	L	Core (R) Distro (R) Access (R)
2	Despite the differences in IPv6 and IPv4 packet sizes, for planning purposes, the number of VoIP subscribers per link size for IPv6 should be assumed to be approximately the same as for IPv4 and is defined in Table 7.6-2, LAN VoIP Subscribers for IPv4 and IPv6, in Section 7, Network Edge Infrastructure.	5.2.1.11 IP6-001020	L	Core (R) Distro (R) Access (R)
3	Despite the differences in IPv6 and IPv4 packet sizes, for planning purposes, the number of video subscribers per link size for IPv6 should be assumed to be approximately the same as for IPv4 and is defined in Section 7, Network Edge Infrastructure.	5.2.1.11 IP6-001030	L	Core (R) Distro (R) Access (R)
IP1-12	**5.2.1.14 – Miscellaneous**			
1	If the product supports Remote Authentication Dial-in User Service (RADIUS) authentication, then the product shall support RADIUS as defined in RFC 3162. [Conditional: LS] If the LS supports a routing function and supports RADIUS authentication, then the product shall support RADIUS as defined in RFC 3162.	5.2.1.14 IP6-001140	L	Core (R) Distro (C) Access (C)
2	The products shall support Differentiated Services as described in RFC 2474 for a voice and video stream in accordance with Section 2, Session Control Products, and Section 6, Network Infrastructure End-to-End Performance, plain text DSCP plan.	5.2.1.14 IP6-001150	L	Core (R) Distro (R) Access (R)
3	To support ASLAN assured services, all LAN switches that provide layer 3 functionality to the access layer shall support Virtual Router Redundancy protocol (VRRP) for IPv6 as detailed in RFC 5798.	5.2.1.14 IP6-001190	L/T IO-3 to IO-9	Core (C) Distro (R)
6	If the product supports ECN, then the product shall support RFC 3168 for the incorporation of ECN to TCP and IP, including ECN's use of two bits in the IP	5.2.1.14 IP6-001200	L	Core (C) Distro (C) Access (C)

NOTES:
1. The requirements are derived from the UCR 2013, Errata 1, Reference (c).
2. Refers to the methodology for requirement verification via LoC "L", test "T", or both "L/T". Test items include test procedure number(s).

Table 3-6. ASLAN Component IPv6 Requirements (continued)

LEGEND:			
ASLAN	Assured Services Local Area Network	LAN	Local Area Network
C2	Command and Control	LOC	Letter of Compliance
CPU	Central Processing Unit	LS	LAN Switch
DHCP	Dynamic Host Configuration Protocol	MPLS	Multiprotocol Label Switching
DISR	Department of Defense Information Technology Standards Registry	ms	Millisecond
		MTU	Maximum Transmission Unit
DSCP	Differentiated Services Code Point	NM	Network Management
FY	Fiscal Year	NMS	Network Management Systems
HMAC	Hash-based Message Authentication Code	OSI	Open Systems Interconnection
HRS	Hours	OSPFv3	Open Shortest Path First Version 3
HTTPS	Hyper Text Transfer Protocol, Secure	PHB	Per Hop Behavior
HTTP	Hypertext Transfer Protocol	PQ	Priority Queuing
IA	Information Assurance	RFC	Request for Comments
IAW	In Accordance with	SLAAC	Stateless Auto Address Configuration
ICMP	Internet Control Message Protocol	SNMP	Simple Network Management Protocol
ICMPv6	Internet Control Message Protocol for IPv6	SSH2	Secure Shell Version 2
IEEE	Institute Of Electrical and Electronics Engineers	TCI	Tag Control Information
IPv4	Internet Protocol Version 4	TP	Test Plan
IPv6	Internet Protocol Version 6	UCR	Unified Capabilities Requirements
MB/S	Megabits per Second	VLAN	Virtual Local Area Network
L3	OSI Layer 3	VPN	Virtual Private Network
LACP	Link Aggregation Control Protocol	WFQ	Weighted Fair Queuing

Table 3-7. ASLAN Component IA Requirements

ID	Requirement	UCR 2013 Reference (See note 1.)	LoC (See note 2.)	R/O/C
UCR 2013 Section 4 Information Assurance Requirements				
IA-1	**4.2.3 – User Roles**			
1	The product shall be capable of having at least three types of user roles: a system security administrator (e.g., auditor), a system administrator, and an application administrator.	4.2.3 IA-001000	L	Core (R) Distro (R) Access (C)
2	The product shall be capable of providing a mechanism for the appropriate administrator (not a user in the User role) to perform the following functions: IA-004010 Monitor the activities of a specific terminal, port, or network address of the system in real time. IA-004020 Define the events that may trigger an alarm, the levels of alarms, the type of notification, and the routing of the alarm. IA-004030 Provide a capability to monitor the system resources and their availabilities.	4.2.3 IA-004000	L	Core (R) Distro (R) Access (C)
IA-2	**4.2.4 – Ancillary Equipment**			
1	Products that use external Authentication, Authorization, and Accounting (AAA) services provided by the Diameter Base Protocol shall do so in accordance with (IAW) Request for Comment (RFC) 3588. IA-009010 that act as Diameter agents shall be capable of being configured as proxy agents. IA-009020 Systems that act as proxy agents shall maintain session state. IA-009030 All Diameter implementations shall ignore answers received that do not match a known Hop-by-Hop Identifier field. IA-009040 [Conditional: SS, SC, MG, SBC, R, LS, EI, AEI, SD] All Diameter implementations shall provide transport of its messages IAW the transport profile described in RFC 3539. IA-009050 Products that use the Extensible Authentication Protocol (EAP) within Diameter shall do so IAW RFC 4072.	4.2.4 IA-009000	L	Core (C) Distro (C) Access (C)
2	Products shall support the capability to use the Remote Authentication Dial In User Service (RADIUS) IAW RFC 2865 to provide AAA services. IA-010010 Products that use the EAP within RADIUS shall do so IAW RFC 3579. IA-010020 If the products support RADIUS based accounting, then the system shall do so IAW RFC 2866.	4.2.4 IA-010000	L	Core (R) Distro (R) Access (C)
3	Products that use external AAA services provided by the Terminal Access Controller Access Control System (TACACS+) shall do so IAW the TACACS+ Protocol Specification 1.78 (or later).	4.2.4 IA-011000	L	Core (C) Distro (C) Access (C)
4	Products that use external AAA services provided by port based network access control mechanisms shall do so IAW Institute of Electrical and Electronics Engineers (IEEE) 802.1X-2010 in combination with Protected Extensible Authentication Protocol (PEAP) and Extensible Authentication Protocol (EAP)-Transport Layer Security (TLS) support, at a minimum, plus any other desired secure EAP types [e.g., EAP-Tunneled TLS (TTLS)]. IA-013010 Products that use external EAP services provided by EAP shall do so IAW RFC 3748 and its RFC extensions.	4.2.4 IA-013000	L	Core (C) Distro (C) Access (C)

Table 3-7. ASLAN Component IA Requirements (continued)

ID	Requirement	UCR 2013 Reference (See note 1.)	LoC (See note 2.)	R/O/C
IA-2	**4.2.4 – Ancillary Equipment (continued)**			
5	Products that use external syslog services shall support the capability to do so IAW RFC 3164. IA-014010 Products that support syslog over UDP IAW RFC 3164 shall use UDP port 514 for the source port of the sender when using UDP for transport. IA-014020 If the product supports syslog, then the product shall support the capability to generate syslog messages that have all the parts of the syslog packet as described in Section 4.1 of RFC 3164. IA-014030 If the originally formed message has a TIMESTAMP in the HEADER part, then it shall support the capability to specify this field's value in the local time of the device within its time zone and support the ability to specify this field's value in Greenwich Mean Time (GMT). IA-014040 If the originally formed message has a HOSTNAME field, then it shall contain the hostname as it knows itself. If it does not have a hostname, then it shall contain its own IP address. IA-014050 If the originally formed message has a TAG value, then it shall be the name of the program or process that generated the message. IA-014060 [Conditional: SS, SC, MG, SBC, RSF, R, LS, FW, IPS, VPN, NAC] If products use Transmission Control Protocol (TCP) for the delivery of syslog events, then the system shall support the capability to do so IAW the Read and Write (RAW) profile defined in RFC 3195.	4.2.4 IA-014000	L	Core (C) Distro (C) Access (C)
6	If the product implements NTP, then the default versionproduct shall support interoperability with be Network Time Protocol (NTP) version 3 (NTPv3) at a minimum even if higher versions of NTP are supported.	4.2.4 IA-016000	L	Core (C) Distro (C) Access (C)
IA-3	**4.2.6 – VVoIP Authorization**			
1	The product shall have the capability of controlling the flow of traffic across an interface to the network based on the source/destination IP address, source/destination port number, Differentiated Services Code Point (DSCP), and protocol identifier ("6 tuple").	4.2.6 IA-026000	L	Core (R) Distro (R) Access (R)
2	The product shall be capable of supporting a minimum of five distinct VLANs for VVoIP.	4.2.6 IA-031000	L	Core (R) Distro (R) Access (R)
3	If DHCP is used, then the product shall be capable of using 802.1X in combination with a secure EAP type (defined within this UCR and the STIGs/SRGs) residing on the authentication server and within the operating system or application software of the EI and AEI to authenticate to the LAN.	4.2.6 IA-037000	L	Core (C) Distro (C)
IA-4	**4.2.7 – Public Key Infrastructure**			
1	The product shall be capable of generating asymmetric keys whose length is at least 2048 for Rivest Shamir Adleman (RSA).	4.2.7 IA-040000	L	Core (R) Distro (R) Access (R)
2	The product shall be capable of generating symmetric keys whose length is at least 128 bits.	4.2.7 IA-041000	L	Core (R) Distro (R) Access (R)
3	The product shall be capable of storing key pairs and their related certificates.	4.2.7 IA-042000	L	Core (R) Distro (R) Access (R)
4	The product shall operate with DoD-approved trust anchors (e.g., public keys and the associated certificates the relying party deems as reliable and trustworthy, typically root certification authorities [CAs]). IA-043010 Any system that performs PKI certificate validation operations must implement the basic steps outlined in Section 6.1.3 of the internet X.509 certificate specification Request for Comment (RFC) 5280.	4.2.7 IA-043000	L	Core (R) Distro (R) Access (R)
5	The product shall be capable of supporting end entity server and device certificates and populating all certificate fields IAW methods described in the "DoD PKI Functional Interface Specification."	4.2.7 IA-044000	L	Core (R) Distro (R) Access (R)
6	The product shall be capable of using the Lightweight Directory Access Protocol (LDAP) version 3 (LDAPv3), LDAP over TLS (LDAPS), Hypertext Transfer Protocol (HTTP), or HTTP Secure (HTTPS) as appropriate when communicating with DoD-approved PKIs.	4.2.7 IA-045000	L	Core (R) Distro (R) Access (R)

Table 3-7. ASLAN Component IA Requirements (continued)

ID	Requirement	UCR 2013 Reference (See note 1.)	LoC (See note 2.)	R/O/C
IA-4	**4.2.7 – Public Key Infrastructure (continued)**			
7	If Certificate Revocation Lists (CRLs) are used, then the product shall be capable of using either the date and time specified in the next update field in the CRL or using a configurable parameter to define the period associated with updating the CRLs.	4.2.7 IA-046000	L	Core (C) Distro (C) Access (C)
8	If CRLs are used, then the product shall be capable of obtaining the CRL from the CRL Distribution Point (CDP) extension of the certificate in question. The product shall be able to process HTTP pointers in the CDP field whereas the ability to process HTTPS and LDAP pointers is considered Objective and is not a hard requirement.	4.2.7 IA-047000	L	Core (C) Distro (C) Access (C)
9	If Online Certificate Status Protocol (OCSP) is used, then the product shall support the capability to use both the Delegated Trust Model (DTM), whereby the OCSP responder's signing certificates are signed by DoD approved PKI CAs, and the OCSP Trusted Responder model, where the OCSP responder uses a self-signed certificate to sign OCSP responses, IAW DoD PKI PMO guidance.	4.2.7 IA-048000	L	Core (C) Distro (C) Access (C)
10	If OCSP is used, then the OCSP responder shall be contacted based on the following information: IA-049010 The OCSP responder preconfigured in the application or toolkit; and IA-049020 The OCSP responder location identified in the OCSP field of the Authority Information Access (AIA) extension of the certificate in question. IA-049030 If both of the above are available, then the product shall be configurable to provide preference for one over the other. IA-049040 The product should (not shall) be configurable to provide preferences or a preconfigured OCSP responder based on the Issuer DN.	4.2.7 IA-049000	L	Core (C) Distro (C) Access (C)
11	The product shall support all of the applicable requirements in the latest DoD Public Key Enabled (PKE) Application Requirements specification published by the DoD PKI PMO.	4.2.7 IA-052000	L	Core (R) Distro (R) Access (R)
12	Systems that perform any PKI operations (e.g., certificate path processing, certificate validation, digital signature generation, and encryption) must support RSA keys up to 2048 bits with Secure Hash Algorithm (SHA)-1 and SHA-2 digital signatures as dictated by the National Institute of Standards and Technology (NIST) Special Publications (SP) 800-57, SP 800-78, and SP 800-131A and the DoD Certificate Policy. IA-053010 The product shall support the capability to verify certificates, CRLs, OCSP responses, or any other signed data produced by a DoD approved PKI using RSA in conjunction with the SHA-256 algorithm.	4.2.7 IA-053000	L	Core (R) Distro (R) Access (R)
13	The product shall log when a session is rejected due to a revoked certificate.	4.2.7 IA-054000	L	Core (R) Distro (R) Access (R)
14	The product shall be capable of supporting the development of a certificate path and be able to process the path. IA-055010 The path process shall fail when a problem that prohibits the validation of a path occurs.	4.2.7 IA-055000	L	Core (R) Distro (R) Access (R)
15	The product shall be capable of ensuring that the intended use of the certificate is consistent with the DoD-approved PKI extensions. IA-056010 The product shall be capable of ensuring that the key usage extension in the end entity certificate is set properly. IA-056020 The product shall be capable of ensuring that the digital signature bit is set for authentication uses. IA-056030 The product shall be capable of ensuring that the non-repudiation bit is set for nonrepudiation uses.	4.2.7 IA-056000	L	Core (R) Distro (R) Access (R)

Table 3-7. ASLAN Component IA Requirements (continued)

ID	Requirement	UCR 2013 Reference (See note 1.)	LoC (See note 2.)	R/O/C
IA-4	**4.2.7 – Public Key Infrastructure (continued)**			
16	Periodically, the system shall examine all of the certificates and trust chains associated with ongoing, long-lived, sessions. The system shall terminate any ongoing sessions based on updated revocation/trust information if it is determined that the corresponding certificates have been revoked, are no longer trusted, or are expired. IA-059010 [Conditional] If the system supports manual loading of a CRL or CTLs configured by an administrator, then the system shall check all ongoing sessions as soon as updates to the internally stored CRL or trust lists occur. IA-059020 [Conditional] If the system supports automated retrieval of a CRL from a CDP, then the system shall immediately check the certificates and trust chains associated with all ongoing sessions against the newly retrieved CRL. IA-059030 [Conditional] If the system supports automated retrieval of a CRL from a CDP, then the system shall support the ability to configure the interval in which the CRL is retrieved periodically. IA-059040 [Conditional] If the system supports queries against an online status check responder (an OCSP responder in the case of the DoD PKI), then the system shall periodically query the responder to determine if the certificates corresponding to any ongoing sessions have been revoked. IA-059050 [Conditional] If the system supports queries against an online status check responder (an OCSP responder in the case of the DoD PKI), by default, for each session, then the device shall query the online status check responder every 24 hours for as long as the session remains active. IA-059060 [Conditional] If the system supports queries against an online status check responder (an OCSP responder in the case of the DoD PKI), then the system shall support the ability to configure the interval at which the system periodically queries the online status check responder.	4.2.7 IA-059000	L	Core (R) Distro (R) Access (R)
17	The system shall be capable of sending an alert when installed certificates corresponding to trust chains, OCSP responder certificates, or any other certificates installed on the device that cannot be renewed in an automated manner, are nearing expiration. IA-060010 By default, the system shall be capable of sending this alert 60 days before the expiration of the installed credentials, which cannot be renewed automatically. This alert should be repeated periodically on a weekly or biweekly basis by default.	4.2.7 IA-060000	L	Core (R) Distro (R) Access (R)
IA-5	**4.2.8 – Integrity**			
1	The entire SNMPv3 message shall be checked for integrity and shall use the HMAC-SHA1-96 with 160-bit key length by default.	4.2.8 IA-066000	L	Core (R) Distro (R) Access (R)
2	If the product uses SSHv2, then the product shall use HMAC-SHA1-96 with 160 bit key length for data integrity.	4.2.8 IA-067000	L	Core (C) Distro (C) Access (C)
IA-6	**4.2.9 – Confidentiality**			
1	If IPSec is used, then the product shall be capable of using IKE for IPSec key distribution: IA-071010 The product shall be capable of using IKE version 1. IA-071030 If IPSec is used, then the product shall be capable of using the Quick Mode as the default Phase II Security Association mechanism for the IPSec service. IA-071040 If IPSec is used, then the product shall be capable of using and interpreting certificate requests for Public-Key Cryptography Standard #7 (PKCS#7) wrapped certificates as a request for the whole path of certificates. IA-071050 If IPSec is used, then the product shall be capable of using Main Mode associated with the Diffie-Hellman approach for key generation for the security association negotiation. IA-071060 If IPSec is used, then the product shall be capable of using Diffe-Hellman Groups 1, 2, and 14, at a minimum.	4.2.9 IA-071000	L	Core (C) Distro (C) Access (C)

Table 3-7. ASLAN Component IA Requirements (continued)

ID	Requirement	UCR 2013 Reference (See note 1.)	LoC (See note 2.)	R/O/C
IA-6	**4.2.9 – Confidentiality (continued)**			
2	If the product uses TLS, then the product shall do so in a secure manner as defined by the following subtended requirements. IA-073010 If the product uses TLS, then the system shall be capable of using TLS_RSA_WITH_AES_128_CBC_SHA as its default cipher suite. IA-073020 If the product uses TLS, then the system shall be capable of using a default of no compression. IA-073030 If the product uses TLS, then the system shall be capable of exchanging TLS messages in a single exchange or multiple exchanges. IA-073040 If TLS session resumption is used, then a timer associated with TLS session resumption shall be configurable and the default shall be 1 hour. IA-073050 If TLS session resumption is used, then the maximum time allowed for a TLS session to resume (session resumption) without repeating the TLS authentication/confidentiality/authorization process (e.g., a full handshake) is 1 hour. IA-073060 If the product supports SSL/TLS renegotiation, then the product shall support the capability to disable this feature or the product shall support RFC 5746.	4.2.9 IA-073000	L	Core (C) Distro (C) Access (C)
3	If the product uses Secure Shell (SSH), then the system shall do so in a secure manner as defined by the following subtended requirements. IA-074010 If the product uses SSH, then the system shall be capable of supporting the RSA 2,048-bit key algorithm and the Diffie-Hellman 2,048 bit key algorithm. IA-074020 If the product uses SSH, then a client shall close the session if it receives a request to initiate an SSH session whose version is less than . IA-074030 If the product uses SSH, then the SSH sessions shall rekey at a minimum every gigabyte of data received or every 60 minutes, whichever comes sooner. IA-074040 If the product uses SSH, then the SSH sessions shall rekey at a minimum every gigabyte of data transmitted or every 60 minutes, whichever comes sooner. IA-074050 If the product uses SSH, then the SSH sessions shall minimally support the AES 128-CBC algorithm as defined in RFC 4253. IA-074070 If the product uses SSH, then the SSH sessions shall use TCP as the underlying protocol. IA-074100 If the product uses SSH, then the product shall discard SSH packets that exceed the maximum packet size to avoid denial of service (DoS) attacks or buffer overflow attacks. IA-074110 If the product uses SSH, then the SSH packets shall use random bytes if packet padding is required. IA-074120 If the product uses SSH, then the system shall treat all SSH-encrypted packets sent in one direction as a single data stream. For example, the initialization vectors shall be passed from the end of one packet to the beginning of the next packet. IA-074130 If the product uses SSH, then the system shall be capable of setting Diffie-Hellman-Group14-SHA1 as the preferred key exchange mechanism for SSH.	4.2.9 IA-074000	L	Core (C) Distro (C) Access (C)
4	If the product uses SSH with X.509v3 certificates and provides an SSH server function, then the SSH server shall support the capability to use an X.509v3 certificate provided by a DoD-approved PKI. IA-075010 If the product uses SSH with X.509v3 certificates and provides an SSH server function, then the SSH Server function shall support, at a minimum, the “x509v3-ssh-rsa” and "x509v3-rsa2048- sha256” key types as defined in RFC 6187. IA-075020 If the product uses SSH with X.509v3 certificates and provides an SSH server function, then the SSH Server function shall support the capability to, in a configurable manner, specify the highest preferred key type advertised during the SSH_MSG_KEXINIT message exchange. IA-075030 If the product uses SSH with X.509v3 certificates and provides an SSH server function, then the SSH server function shall support the capability to deny SSH sessions when the session fails to negotiate a configured set of preferred key types.	4.2.9 IA-075000	L	Core (C) Distro (C) Access (C)

Table 3-7. ASLAN Component IA Requirements (continued)

ID	Requirement	UCR 2013 Reference (See note 1.)	LoC (See note 2.)	R/O/C
IA-6	**4.2.9 – Confidentiality (continued)**			
5	If the product uses SSH with X.509v3 certificates and provides an SSH server function, then the SSH client shall support the capability to use an X.509v3 certificate provided by a DoD-approved PKI. IA-076010 If the product provides an SSH client function and the SSH client has a CAC (or equivalent) reader, then the SSH client may use the X.509v3 certificate on the user's CAC to establish the encrypted session. IA-076020 If the product uses SSH and if the client has a CAC (or equivalent) reader and also has its own PKI certificate from a DoD-approved PKI, then the client may use either its certificate or the certificate on the user's CAC to establish the encrypted sessions. IA-076030 If the product uses SSH with X.509v3 certificates, and provides an SSH client function, then the SSH client shall support, at a minimum, the "x509v3-ssh-rsa" and "x509v3-rsa2048-sha256" key types as defined in RFC 6187.	4.2.9 IA-076000	L	Core (C) Distro (C) Access (C)
6	The product shall be capable of using SNMPv3 for all SNMP sessions. IA-077010 The security level for SNMPv3 in the DoD VVoIP environment shall be authentication with privacy – snmpSecurityLevel=authPriv. The product shall set snmpSecurityLevel=authPriv as the default security level used during initial configuration. IA-077020 The SNMPv3 implementation shall be capable of allowing an appropriate administrator to manually configure the snmpEngineID from the operator console. A default unique snmpEngineID may be assigned to avoid unnecessary administrative overhead, but this must be changeable. IA-077030 The security model for SNMPv3 shall be the User-Based Security Model – snmpSecurityModel =3. IA-077040 If the product receives SNMPv3 response messages, then the product shall conduct a timeliness check on the SNMPv3 message. IA-077050 An SNMPv3 engine shall perform time synchronization using authenticated messages. IA-077060 The message processing model shall be SNMPv3 – snmpMessageProcessingModel=3. IA-077070 For backwards compatibility, the product shall support the capability to use Data Encryption Standard- Cipher Block Chaining (DES-CBC) (usmDESPrivProtocol) with a 16 octet (128 bit) input key, as specified in RFC 3414, as an encryption cipher for SNMPv3. IA-077080 The product shall support the capability to use the CFB-AES128 encryption cipher usmAesCfb128PrivProtocol for SNMPv3 as defined in RFC 3826 and specify this as the default encryption cipher for SNMPv3. IA-077090 [Conditional] If the product receives SNMPv3 response messages, then the SNMPv3 engine shall discard SNMP response messages that do not correspond to any current outstanding Request messages. IA-077100 [Conditional] If the product receives SNMPv3 responses, then the SNMPv3 Command Generator Application shall discard any Response Class Protocol Data Unit (PDU) for which there is no outstanding Confirmed Class PDU. IA-077110 When using msgID for correlating Response messages to outstanding Request messages, the SNMPv3 engine shall use different msgIDs in all such Request messages that it sends out during a 150 second Time Window. IA-077120 An SNMPv3 Command Generator or Notification Originator Application shall use different request-ids in all Request PDUs that it sends out during a Time Window. IA-077130 When sending state altering messages to a managed authoritative SNMPv3 engine, a Command Generator Application should delay sending successive messages to that managed SNMPv3 engine until a positive acknowledgement is received from the previous message or until the message expires. IA-077140 The product using SNMPv3 shall implement the key-localization mechanism.	4.2.9 IA-077000	L	Core (R) Distro (R) Access (R)

Table 3-7. ASLAN Component IA Requirements (continued)

ID	Requirement	UCR 2013 Reference (See note 1.)	LoC (See note 2.)	R/O/C
IA-6	**4.2.9 – Confidentiality (continued)**			
7	If the product uses web browsers or web servers, then the product web browsers and web servers shall be capable of supporting TLS 1.0 or higher for confidentiality.	4.2.9 IA-078000	L	Core (C) Distro (C) Access (C)
8	The product shall be capable of using SSHv2 or TLS 1.0 or higher for remote configuration of appliances.	4.2.9 IA-079000	L	Core (R) Distro (R) Access (R)
IA-7	**4.2.10 Non-Repudiation**			
1	The security log shall be capable of using a circular (or equivalent) recording mechanism (i.e., oldest record overwritten by newest).	4.2.9 IA-084000	L	Core (R) Distro (R) Access (R)
2	Only the System Security Administrator and System Administrator roles shall have the ability to retrieve, print, copy, and upload the security log(s)	4.2.9 IA-085000	L	Core (R) Distro (R) Access (R)
3	The product/system shall be able to generate a human understandable presentation of any audit data stored in the audit trail.	4.2.9 IA-086000	L	Core (R) Distro (R) Access (R)
4	The product shall provide a mechanism to locally store audit log/event data when communication with the management station is unavailable.	4.2.9 IA-087000	L	Core (R) Distro (R) Access (R)

NOTES:
1. The requirements are derived from the UCR 2013, Errata 1, Reference (c).
2. All requirements are verified with the vendor's LoC. In addition, security is tested by separate Information Assurance test teams and the results published in a separate report.

LEGEND:

AAA	Authorization and Accounting	MTU	Maximum Transmission Unit
AES	Advanced Encryption Standard	NIST	National Institute of Standards and Technology
ANSI	American National Standards Institute	NM	Network Management
AS	Assured Services	NTP	Network Transfer Protocol
ASLAN	Assured Service Local Area Network	NTPv3	Network Transfer Protocol version 3
BW	Bandwidth	OCSP	Online Certificate Status Protocol
C	Conditional	PDU	Protocol Data Unit
CDP	Certificate Revocation List Distribution Point	PEAP	Protected Extensible Authentication Protocol
CRL	Certificate Revocation List	PKE	Public Key Enable
DoD	Department of Defense	PKI	Public Key Infrastructure
DS	Differentiated Services	PPP	Point-to-Point Protocol
DSCP	Differentiated Services Code Point	QoS	Quality of Service
EAP	Extensible Authentication Protocol	R	Required
F	Flash	RADIUS	Remote Authentication Dial in User Service
FO	Flash Override	RFC	Request for Comments
GMT	Greenwich Mean Time	RSA	Rivest Shamir Adleman
HTTP	Hypertext Transfer Protocol	RTS	Real-Time Services
IA	Information Assurance	SNMPv3	Simple Network Management Protocol version 3
IAW	In Accordance With	SP	Special Publication
IEEE	Institute of Electronics and Electrical Engineers	SSH	Secure Shell
INCITS	International Committee for Information Technology Standards	STIGs	Security Technical Implementation Guideline
		TACACS	Terminal Access Control Access Control System
IP	Internet Protocol	TCP	Transmission Control Protocol
IPv4	Internet Protocol version 4	TIA	Telecommunications Industry Association
IPv6	Internet Protocol version 6	TLS	Transport Layer Security
LAN	Local Area Network	TOS	Type of Service
LDAPv3	Lightweight Directory Access Protocol version 3	UC	Unified Capabilities
L-LSP	Label Only Inferred Label Switched Path	UCR	Unified Capabilities Requirement
LoC	Letter of Compliance	UDP	User Datagram Protocol
LS	Local Area Network Switch	VLAN	Virtual Local Area Network
LSP	Label Switched Path	VPLS	Virtual Private Local Area Network Service
MAC	Media Access Control	VPN	Virtual Private Network
MAN	Metropolitan Area Network	VVoIP	Voice and Video over Internet Protocol
Mbps	Megabits per second	WABs	Wireless Access Bridges
MPLS	Multiprotocol Label Switching	WAN	Wide Area Network
ms	milliseconds	WLAS	Wireless Local Area Network Access System