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

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

MEMORANDUM FOR DISTRIBUTION **15 Jun 11**

SUBJECT: Special Interoperability Test Certification of the Cisco Catalyst 3750X series Switch Release Internetwork Operating System (IOS) 12.2(55)SE1

References: (a) DoD Directive 4630.05, "Interoperability and Supportability of Information Technology (IT) and National Security Systems (NSS)," 5 May 2005
(b) CJCSI 6212.01E, "Interoperability and Supportability of Information Technology and National Security Systems," 15 December 2008
(c) through (e), see Enclosure 1

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

2. The Cisco WS-C3750X-48P/-24P Switch Release IOS 12.2(55)SE1 is hereinafter referred to as the system under test (SUT). The SUT meets all of its critical interoperability requirements and is certified for joint use within the Defense Information System Network (DISN) in a single or stackable configuration up to nine switches, as an Assured Services Local Area Network (ASLAN) Layer 2 access switch. The SUT is certified as interoperable for joint use with other ASLAN components listed on the Unified Capabilities (UC) Approved Products List (APL) with the following interfaces: 10GBaseX, 1000BaseSX/LX, 100BaseFX, and 10/100/1000BaseT. The SUT meets the critical interoperability requirements set forth in Reference (c), using test procedures derived from Reference (d). The Cisco WS-C3750X-48PF, WS-C3750X-48T, and WS-C3750X-24T employ the same software and similar hardware as the SUT. The JITC analysis determined these switches to be functionally identical to the SUT for interoperability certification purposes and they are also certified for joint use.

The SUT is certified to support Defense Switched Network (DSN) Assured Services over Internet Protocol. If a component meets the minimum requirements for deployment in an ASLAN, it also meets the lesser requirements for deployment in a non-ASLAN. Non-ASLANs are "commercial grade" and provide support to Command and Control (C2) (ROUTINE only calls), (C2(R)), or non-C2 voice subscribers. The SUT is certified for joint use deployment in a non-ASLAN for C2(R) and non-C2 traffic. When deployed in a non-ASLAN, the SUT may also be used to receive all levels of precedence but is limited to supporting calls that are originated at ROUTINE precedence only. Non-ASLANs do not meet the availability or redundancy requirements for C2 or Special C2 users and therefore are not authorized to support precedence calls originated above ROUTINE.

Testing of the SUT did not include video services or data applications; however, simulated preferred data, best effort data, and video traffic were generated during testing to determine the SUT's ability to prioritize and properly queue voice media and signaling traffic. No other configurations, features, or functions, except those cited within this document, are certified by the JITC. This certification expires upon changes that affect interoperability but no later than three years from the date of the DISA Certification and Accreditation (CA) provided a positive Recommendation.

3. This finding is based on interoperability testing conducted by the United States Army Information Systems Engineering Command, Technology Integration Center (USAISEC TIC), DISA adjudication of open test discrepancy reports (TDRs), review of the vendor's Letters of Compliance (LoC), and the DISA CA Recommendation. Interoperability testing was conducted by the USAISEC TIC, Fort Huachuca, Arizona, from 31 January through 25 February 2011. Review of the vendor's LoC was completed on 10 May 2011. DISA adjudication of outstanding TDRs was completed on 31 May 2011. The DISA CA provided a positive recommendation on 3 June 2011 based on the security testing completed by DISA-led IA test teams and published in a separate report, Reference (e).

4. Table 1 provides the SUT's interface status. The SUT's capability and functional requirements are listed in Table 2.

Table 1. SUT Interface Status

Interface	Applicability Access	CRs/FRs (See note 1.)	Status Access
Network Management Interfaces for Layer 2 Access Switches			
EIA/TIA (Serial) 232	R	EIA/TIA-232	Met
IEEE 802.3i (10BaseT UTP)	C[2]	7-18, 25-28, 32-36, 44-46, 55-57, 72-75	Met
IEEE 802.3u (100BaseT UTP)	C[2]	7-18, 25-28, 32-36, 44-46, 55-57, 72-75	Met
IEEE 802.3ab (1000BaseT UTP)	C[2]	7-18, 25-28, 32-36, 44-46, 55-57, 72-75	Met
Uplink Interfaces for Layer 2 Access Switches			
IEEE 802.3u (100BaseT UTP)	C[2]	7-18, 28, 44-46, 55-57, 72-75	Met
IEEE 802.3u (100BaseFX)	C[2]	10-18, 28, 44-46, 55-57, 72-75	Met
IEEE 802.3ab (1000BaseT UTP)	C[2]	7-18, 28, 44-46, 55-57, 72-75	Met
IEEE 802.3z1000BaseX Fiber	C[2]	10-18, 28, 44-46, 55-57, 72-75	Met
IEEE 802.3ae (10GBaseX)	C[2]	10-18, 28, 44-46, 55-57, 72-75	Met
Access Interfaces for Layer 2 Access Switches			
IEEE 802.3I (10BASET UTP)	C[2]	7-18, 28, 44-46, 55-57, 72-75	Met
IEEE 802.3u (100BaseT UTP)	C[2]	7-18, 28, 44-46, 55-57, 72-75	Met
IEEE 802.3u (100BaseFX)	C[2]	10-18, 28, 44-46, 55-57, 72-75	Met
IEEE 802.3ab (1000BaseT UTP)	C[2]	7-18, 28, 44-46, 55-57, 72-75	Met
IEEE 802.3z (1000BaseX Fiber)	C[2]	10-18, 28, 44-46, 55-57, 72-75	Met
Generic Requirements for all Interfaces			
Generic Requirements not associated with specific interfaces	R	30-32, 35, 36, 40, 69-71	Met
DoD IPv6 Profile Requirements	R	UCR Section 5.3.5.5	Met
Security	R	79-82	Met[3]

Table 1. SUT Interface Status (continued)

NOTES:

1 The SUT's specific capability and functional requirement ID numbers depicted in the CRs/FRs column can be cross-referenced in Table 2. These requirements are for the following Cisco switch models, which are certified in the ASLAN Access layer: **WS-C3750X-48P**, **WS-C3750X-24P**, WS-C3750X-48PF, WS-C3750X-48T, and WS-C3750X-24T. The other devices listed that are not bolded or underlined are in the same family series as the SUT but were not tested; however, they utilize the same OS software and similar hardware, and JITC analysis determined these switches to be functionally identical for interoperability certification purposes.
2 Access layer switches are required to support only one of the following IEEE interfaces: 802.3i, 802.3j, 802.3u, 802.3ab, or 802.3z.
3 Security testing is accomplished via DISA-led Information Assurance test teams, and the results are published in a separate report, Reference (e).

LEGEND:

802.3ab	1000BaseT Gbps Ethernet over twisted pair at 1 Gbps (125 Mbps)	EIA-232	Standard for defining the mechanical and electrical characteristics for connecting Data Terminal Equipment (DTE) and Data Circuit-terminating Equipment (DCE) data communications devices
802.3ae	10 Gbps Ethernet		
802.3i	10BaseT Mbps over twisted pair		
802.3u	Standard for carrier sense multiple access with collision detection at 100 Mbps	FRs	Functional Requirements
		Gbps	Gigabits per second
802.3z	Gigabit Ethernet Standard	ICMP	Internet Control Message Protocol
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	IPv6	Internet Protocol version 6
		JITC	Joint Interoperability Test Command
100BaseFX	100 Mbps Ethernet over fiber	Mbps	Megabits per second
1000BaseFX	1000 Mbps Ethernet over fiber	OS	Operating System
1000BaseT	1000 Mbps (Baseband Operation, Twisted Pair) Ethernet	POAM	Plan of Action and Milestones
		PWR	Power over Ethernet
10GBaseX	10000 Mbps Ethernet over Category 5 Twisted Pair Copper	R	Required
		RFCs	Request for Comments
ASLAN	Assured Services Local Area Network	SFP	Small Form Factor Pluggable
C	Conditional	SNMP	Simple Network Management Protocol
CRs	Capability Requirements	SUT	System Under Test
DISA	Defense Information Systems Agency	TIA	Telecommunications Industry Association
DoD	Department of Defense	UCR	Unified Capabilities Requirements
EIA	Electronic Industries Alliance	UTP	Unshielded Twisted Pair

Table 2. SUT Capability and Functional Requirements

ID	Requirement (See note.)		UCR Reference
1	ASLAN components can have no single point of failure for >96 users for C2 and Special C2 users. Non-ASLAN components can have a single point of failure for C2(R) and non-C2 users. (R)		5.3.1.2.1, 5.3.1.7.7
2	Non-blocking of any voice or video traffic at 12.5% for access layer switches. (R)		5.3.1.3
3	Maximum of 1 ms of jitter for voice and 10 ms for video for all ASLAN components. (R) Does not apply to preferred data and best effort data.		5.3.1.3
4	Maximum of .015% packet loss for voice and .05 % for video and preferred data for all ASLAN components. (R) Does not apply to best effort data.		5.3.1.3
5	Maximum of 2 ms latency for voice, 10 ms for video, and 15 ms for preferred data for all ASLAN components. (R) Does not apply to best effort data.		5.3.1.3
6	At least one of the following IEEE interfaces for access layer components: 802.3i, 802.3j, 802.3u, 802.3ab, and 802.3z. (R)		5.3.1.3.1
7	Force mode and auto-negotiation IAW IEEE 802.3, filtering IAW RFC 1812, and flow control IAW IEEE 802.3x. (R)		5.3.1.3.2
8	Port Parameter Requirements	Auto-negotiation IAW IEEE 802.3. (R)	5.3.1.3.2
9		Force mode IAW IEEE 802.3. (R)	
10		Flow control IAW IEEE 802.3x. (R)	
11		Filtering IAW RFC 1812. (R)	
12		Link Aggregation IAW IEEE 802.3ad (output/egress ports only). (R)	
13		Spanning Tree Protocol IAW IEEE 802.1D. (R)	
14		Multiple Spanning Tree IAW IEEE 802.1s. (R)	
15		Rapid Reconfiguration of Spanning Tree IAW IEEE 802.1w. (R)	
16	LACP link Failover and Link Aggregation IAW IEEE 802.3ad (uplink ports only) (R)		5.3.1.3.2, 5.3.1.7.7.1

Table 2. SUT Capability and Functional Requirements (continued)

17	Class of Service Marking: Layer 3 DSCPs IAW RFC 2474. (R) Layer 2 3-bit user priority field of the IEEE 802.1Q 2-byte TCI field. (C)		5.3.1.3.3
18	VLAN Capabilities IAW IEEE 802.1Q. (R)		5.3.1.3.4
19	Protocols IAW DISR profile (IPv4 and IPv6). IPv4 (R: LAN Switch, Layer 2 Switch): IPv6 (R: LAN Switch, C: Layer 2 Switch). Note: Layer 2 switch is required to support only RFC 2460, 5095, 2464, and be able to queue packets based on DSCPs in accordance with RFC 2474.		5.3.1.3.5
20	QoS Features	Shall support minimum of 4 queues. (R)	5.3.1.3.6
21		Must be able to assign VLAN tagged packets to a queue. (R)	
22		Support DSCP PHBs per RFCs 2474, 2597, 2598, and 3246. (R: LAN Switch). Note: Layer 2 switch is required to support RFC 2474 only.	
23		Support a minimum of one of the following: Weighted Fair Queuing (WFQ) IAW RFC 3662, Priority Queuing (PQ) IAW RFC 1046, or Class-Based WFQ IAW RFC 3366. (R)	
24		Must be able to assign a bandwidth or percent of traffic to any queue. (R)	
25	Network Monitoring	SNMP IAW RFCs 1157, 2206, 3410, 3411, 3412, 3413, and 3414. (R)	5.3.1.3.7
26		SNMP traps IAW RFC1215. (R)	
27		Remote monitoring IAW RFC1281 and Advanced Encryption Standard (AES) Cipher Algorithm in the SNMP User-based Security Model IAW RFC 3826. (R)	
28	Product Requirements Summary IAW UCR 2008, Change 2, Table 5.3.1-5. (R)		5.3.1.3.9
29	E2E Performance (Voice)	No more than 6 ms latency over any 5-minute period measured under 100% congestion. (R)	5.3.1.4.1
		No more than 3 ms jitter over any 5-minute period measured under 100% congestion. (R)	
		Packet loss not to exceed .045% engineered (queuing) parameters over any 5-minute period under 100% congestion. (R)	
30	E2E Performance (Video)	No more than 30 ms latency over any 5-minute period measured under 100% congestion. (R)	5.3.1.4.2
		No more than 30 ms jitter over any 5-minute period measured under 100% congestion. (R)	
		Packet loss not to exceed .15% engineered (queuing) parameters over any 5-minute period under 100% congestion. (R)	
31	E2E Performance (Data)	No more than 45 ms latency over any 5-minute period measured under 100% congestion (R)	5.3.1.4.3
		Packet loss not to exceed .15% engineered (queuing) parameters over any 5-minute period under 100% congestion. (R)	
32	LAN Network Management	Configuration Control for ASLAN and non-ASLAN. (R)	5.3.1.6.1
33		Operational Controls for ASLAN and non-ASLAN. (R)	5.3.1.6.2
34		Performance Monitoring for ASLAN and non-ASLAN. (R)	5.3.1.6.3
35		Alarms for ASLAN and non-ASLAN. (R)	5.3.1.6.4
36		Reporting for ASLAN and non-ASLAN. (R)	5.3.1.6.5
37	Redundancy	Redundant Power Supplies. (Required on standalone redundant products.)	5.3.1.7.7
38		Chassis Failover. (Required on standalone redundant products.)	
39		Switch Fabric Failover. (Required on standalone redundant products.)	
40		Non-LACP Link Failover. (R)	
41		Fiber Blade Failover. (R)	
42		Stack Failover. (C) (Required if the stack supports more than 96 users.)	
43		CPU (routing engine) blade Failover. (R)	
44	Support IPv6 packets over Ethernet IAW RFC2464. (R)		5.3.5.4
45	Site Requirements	Engineering Requirements: Physical Media for ASLAN and non-ASLAN. (R) (Site requirement)	5.3.1.7.1
46		Battery Back up. Two hours for non-ASLAN components and eight hours for ASLAN components. (R) (Site requirement)	5.3.1.7.5
47		Availability of 99.999 percent (Special C2), and 99.997 percent (C2) for ASLAN (R), and 99.9 percent (non-C2 and C2(R) for non-ASLAN. (R) (Site requirement)	5.3.1.7.6
48	IA Security requirements	Port-Based access Control IAW IEEE 802.1x. (R)	5.3.1.3.2
49		Secure methods for network configuration. SSH2 instead of Telnet and support RFCs 4251-4254. Must use HTTPS instead of HTTP, and support RFCs 2660 and 2818 for ASLAN and non-ASLAN. (R)	5.3.1.6
50		Security (R)	5.3.1.3.8
51		Must meet IA requirements IAW UCR 2008, Change 2, Section 5.4 for ASLAN and non-ASLAN. (R)	5.3.1.5

Table 2. SUT Capability and Functional Requirements (continued)

LEGEND:

ASLAN	Assured Services Local Area Network	HTTPS	HyperText Transfer Protocol, Secure	PHB	Per Hop Behavior
C	Conditional	IA	Information Assurance	QoS	Quality of Service
C2	Command and Control	IAW	in accordance with	R	Required
C2(R)	Command and Control ROUTINE only	ID	Identification	RFC	Request for Comments
CPU	Central Processing Unit	IEEE	Institute of Electrical and Electronics Engineers	SNMP	Simple Network Management Protocol
DISR	Department of Defense Information Technology Standards Registry	IPv4	Internet Protocol version 4	SSH2	Secure Shell Version 2
		IPv6	Internet Protocol version 6	SUT	System Under Test
		LACP	Link Aggregation Control Protocol	TCI	Tag Control Information
DSCP	Differentiated Services Code Point			UCR	Unified Capabilities Requirements
E2E	End-to-End	LAN	Local Area Network	VLAN	Virtual Local Area Network
HTTP	HyperText Transfer Protocol	ms	millisecond		

5. In accordance with the Program Manager's request, no detailed test report was developed. The JITC distributes interoperability information via the JITC Electronic Report Distribution (ERD) system, which uses Unclassified-But-Sensitive Internet Protocol Router Network (NIPRNet) e-mail. More comprehensive interoperability status information is available via the JITC System Tracking Program (STP). The STP is accessible by .mil/gov users on the NIPRNet at https://stp.fhu.disa.mil. Test reports, lessons learned, and related testing documents and references are on the JITC Joint Interoperability Tool (JIT) at https://jit.fhu.disa.mil (NIPRNet). Information related to DSN testing is on the Telecom Switched Services Interoperability (TSSI) website at http://jitc.fhu.disa.mil/tssi. Due to the sensitivity of the information, the Information Assurance Accreditation Package (IAAP) that contains the approved configuration and deployment guide must be requested directly from U.S. Government civilian or uniformed military personnel at the Unified Capabilities Certification Office (UCCO), e-mail: ucco@disa.mil.

6. The JITC point of contact is Mr. Edward Mellon, DSN 879-5159, commercial (520) 538-5159, FAX DSN 879-4347, or e-mail to Edward.Mellon@disa.mil. The JITC's mailing address is P.O. Box 12798, Fort Huachuca, AZ 85670-2798. The Tracking Number for the SUT is 1025206.

JITC Memo, JTE, Special Interoperability Test Certification of the Cisco Catalyst 3750X series Switch Release IOS 12.2(55)SE1

FOR THE COMMANDER:

2 Enclosures a/s

for BRADLEY A. CLARK
Chief
Battlespace Communications Portfolio

Distribution (electronic mail):
Joint Staff J-6
Joint Interoperability Test Command, Liaison, TE3/JT1
Office of Chief of Naval Operations, CNO N6F2
Headquarters U.S. Air Force, Office of Warfighting Integration & CIO, AF/XCIN (A6N)
Department of the Army, Office of the Secretary of the Army, DA-OSA CIO/G-6 ASA (ALT), SAIS-IOQ
U.S. Marine Corps MARCORSYSCOM, SIAT, MJI Division I
DOT&E, Net-Centric Systems and Naval Warfare
U.S. Coast Guard, CG-64
Defense Intelligence Agency
National Security Agency, DT
Defense Information Systems Agency, TEMC
Office of Assistant Secretary of Defense (NII)/DOD CIO
U.S. Joint Forces Command, Net-Centric Integration, Communication, and Capabilities Division, J68
Defense Information Systems Agency, GS23

ADDITIONAL REFERENCES

(c) Office of the Assistant Secretary of Defense, "Department of Defense Unified Capabilities Requirements 2008 Change 2," 31 December 2010
(d) Joint Interoperability Test Command, "Defense Switched Network Generic Switch Test Plan (GSTP), Change 2," 2 October 2006
(e) Joint Interoperability Test Command, "Information Assurance (IA) Assessment of Cisco Catalyst WS-C3750X-48P/-24P (Tracking Number 1025206)," 3 June 2011

CERTIFICATION TESTING SUMMARY

1. SYSTEM TITLE. Cisco Catalyst 3750X series Switch Release Internetwork Operating System (IOS) 12.2(55)SE1, hereinafter referred to as the system under test (SUT).

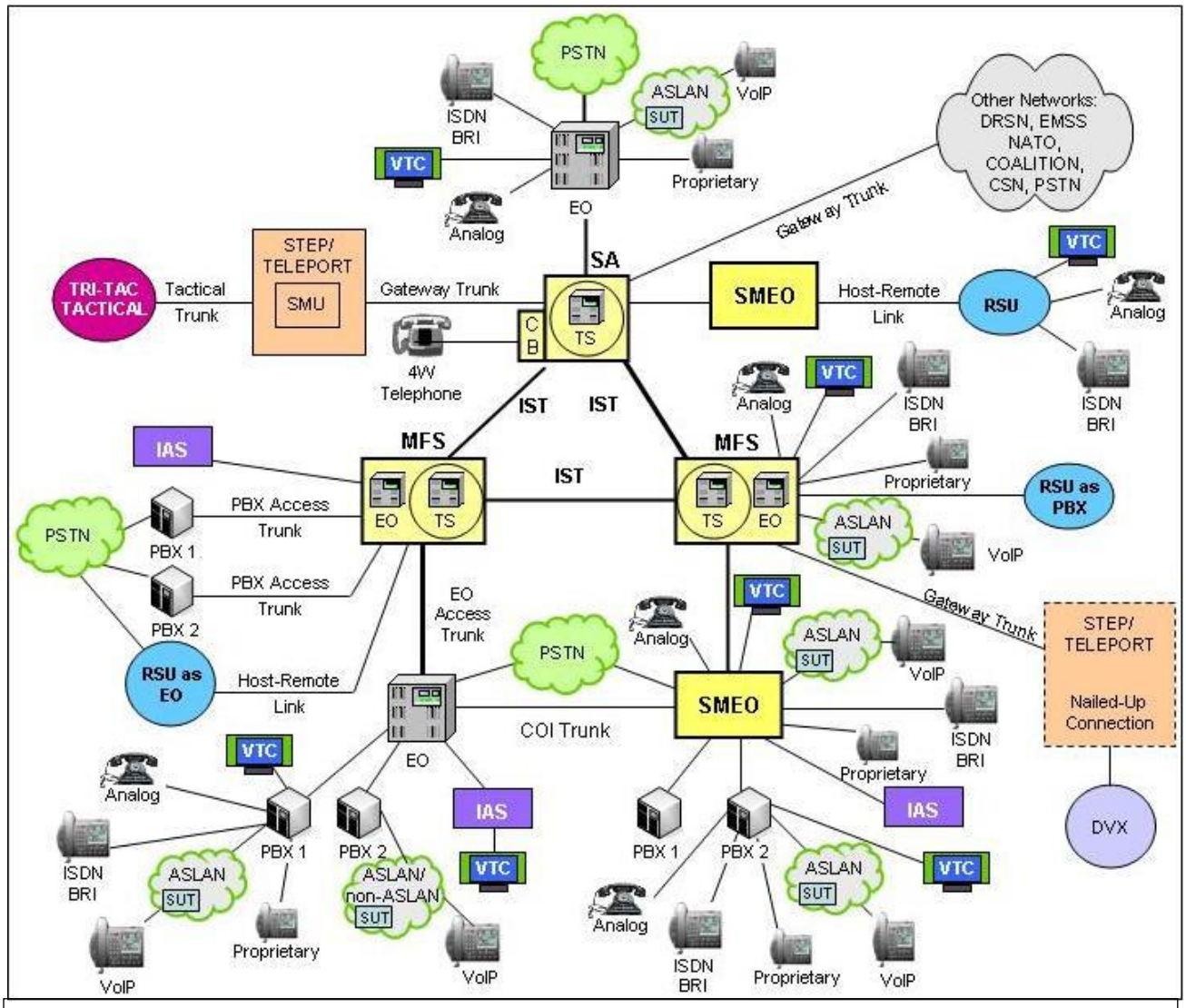
2. PROPONENT. Headquarters, United States Army Information Systems Engineering Command (HQUSAISEC).

3. PROGRAM MANAGER. Mr. Jordan Silk, ELIE-ISE-TI, Building 53302 Arizona Street, Fort Huachuca, AZ 85613-5300; email: Jordan.Silk @us.army.mil.

4. TESTER. U.S. Army Information Systems Engineering Command, Technology Integration Center (USAISEC-TIC), Fort Huachuca, Arizona.

5. SYSTEM UNDER TEST DESCRIPTION. The SUT is used to transport voice signaling and media as part of an overall Voice over Internet Protocol (VoIP) system. The SUT provides availability, security, and Quality of Service (QoS) to meet the operational requirements of the network and Assured Services for the warfighter. The SUT is certified in a single or stackable, up to nine switches, configuration as an Assured Services Local Area Network (ASLAN) Layer 2 (L2) access switch and is interoperable for joint use with other ASLAN components listed on the Unified Capabilities (UC) Approved Products List (APL) with the following interfaces: 10GBaseX, 1000 Base SX/LX, 100BaseFX, and 10/100/1000 BaseT. The Cisco WS-C3750X-48P and WS-C3750X-24P (stacked) was the system tested; however, the Cisco WS-C3750X-48PF, WS-C3750X-48T, and WS-C3750X-24T switches employ the same software and similar hardware as the SUT. The JITC analysis determined these switches to be functionally identical to the SUT for interoperability certification purposes.

6. OPERATIONAL ARCHITECTURE. The Defense Switched Network (DSN) architecture is a two-level network hierarchy consisting of DSN backbone switches and Service/Agency installation switches. Service/Agency installation switches have been authorized to extend voice services over Internet Protocol (IP) infrastructures. The Unified Capabilities Requirements (UCR) operational DSN Architecture shown in Figure 2-1 illustrates the relationship of the ASLAN and non-ASLAN to the DSN switch types.



LEGEND:

4W	4-Wire
ASLAN	Assured Services Local Area Network
BRI	Basic Rate Interface
CB	Channel Bank
COI	Community of Interest
CSN	Canadian Switch Network
DRSN	Defense Red Switch Network
DSN	Defense Switched Network
DVX	Deployable Voice Exchange
EMSS	Enhanced Mobile Satellite System
EO	End Office
IAS	Integrated Access Switch
IP	Internet Protocol
ISDN	Integrated Services Digital Network
IST	Interswitch Trunk
MFS	Multifunction Switch
NATO	North Atlantic Treaty Organization
PBX	Private Branch Exchange
PBX 1	Private Branch Exchange 1
PBX 2	Private Branch Exchange 2
PC	Personal Computer
PSTN	Public Switched Telephone Network
RSU	Remote Switching Unit
SMEO	Small End Office
SMU	Switched Multiplex Unit
STEP	Standardized Tactical Entry Point
TDM/P	Time Division Multiplex/Packetized
Tri-Tac	Tri-Service Tactical Communications Program
TS	Tandem Switch
VoIP	Voice over Internet Protocol
VTC	Video Teleconferencing
	System Under Test

Figure 2-1. DSN Architecture

7. REQUIRED SYSTEM INTERFACES. The SUT capability and functional requirements are listed in Table 2-1. These requirements are derived from the *UCR 2008, Change 2* and verified by means of JITC testing as well as reviews of the vendor's Letters of Compliance (LoC).

Table 2-1. SUT Capability and Functional Requirements

ID	Requirement		UCR Reference
1	ASLAN components can have no single point of failure for >96 users for C2 and Special C2 users. Non-ASLAN components can have a single point of failure for C2(R) and non-C2 users. (R)		5.3.1.2.1, 5.3.1.7.7
2	Non-blocking of any voice or video traffic at 12.5% for access layer switches. (R)		5.3.1.3
3	Maximum of 1 ms of jitter for voice and 10 ms for video for all ASLAN components. (R) Does not apply to preferred data and best effort data.		5.3.1.3
4	Maximum of .015% packet loss for voice and .05 % for video and preferred data for all ASLAN components. (R) Does not apply to best effort data.		5.3.1.3
5	Maximum of 2 ms latency for voice, 10 ms for video, and 15 ms for preferred data for all ASLAN components. (R) Does not apply to best effort data.		5.3.1.3
6	At least one of the following IEEE interfaces for access layer components: 802.3i, 802.3j, 802.3u, 802.3ab, and 802.3z. (R)		5.3.1.3.1
7	Force mode and auto-negotiation IAW IEEE 802.3, filtering IAW RFC 1812, and flow control IAW IEEE 802.3x. (R)		5.3.1.3.2
8	Port Parameter Requirements	Auto-negotiation IAW IEEE 802.3. (R)	5.3.1.3.2
9		Force mode IAW IEEE 802.3. (R)	
10		Flow control IAW IEEE 802.3x. (R)	
11		Filtering IAW RFC 1812. (R)	
12		Link Aggregation IAW IEEE 802.3ad (output/egress ports only). (R)	
13		Spanning Tree Protocol IAW IEEE 802.1D. (R)	
14		Multiple Spanning Tree IAW IEEE 802.1s. (R)	
15		Rapid Reconfiguration of Spanning Tree IAW IEEE 802.1w. (R)	
16	LACP link Failover and Link Aggregation IAW IEEE 802.3ad (uplink ports only) (R)		5.3.1.3.2, 5.3.1.7.7.1
17	Class of Service Marking: Layer 3 DSCPs IAW RFC 2474. (R) Layer 2 3-bit user priority field of the IEEE 802.1Q 2-byte TCI field. (C)		5.3.1.3.3
18	VLAN Capabilities IAW IEEE 802.1Q. (R)		5.3.1.3.4
19	Protocols IAW DISR profile (IPv4 and IPv6). IPv4 (R: LAN Switch, Layer 2 Switch): IPv6 (R: LAN Switch, C: Layer 2 Switch). Note: Layer 2 switch is required to support only RFC 2460, 5095, 2464, and be able to queue packets based on DSCPs in accordance with RFC 2474.		5.3.1.3.5
20	QoS Features	Shall support minimum of 4 queues. (R)	5.3.1.3.6
21		Must be able to assign VLAN tagged packets to a queue. (R)	
22		Support DSCP PHBs per RFCs 2474, 2597, 2598, and 3246. (R: LAN Switch). Note: Layer 2 switch is required to support RFC 2474 only.	
23		Support a minimum of one of the following: Weighted Fair Queuing (WFQ) IAW RFC 3662, Priority Queuing (PQ) IAW RFC 1046, or Class-Based WFQ IAW RFC 3366. (R)	
24		Must be able to assign a bandwidth or percent of traffic to any queue. (R)	
25	Network Monitoring	SNMP IAW RFCs 1157, 2206, 3410, 3411, 3412, 3413, and 3414. (R)	5.3.1.3.7
26		SNMP traps IAW RFC1215. (R)	
27		Remote monitoring IAW RFC1281 and Advanced Encryption Standard (AES) Cipher Algorithm in the SNMP User-based Security Model IAW RFC 3826. (R)	
28	Product Requirements Summary IAW UCR 2008, Change 2, Table 5.3.1-5. (R)		5.3.1.3.9
29	E2E Performance (Voice)	No more than 6 ms latency over any 5-minute period measured under 100% congestion. (R)	5.3.1.4.1
		No more than 3 ms jitter over any 5-minute period measured under 100% congestion. (R)	
		Packet loss not to exceed .045% engineered (queuing) parameters over any 5-minute period under 100% congestion. (R)	
30	E2E Performance (Video)	No more than 30 ms latency over any 5-minute period measured under 100% congestion. (R)	5.3.1.4.2
		No more than 30 ms jitter over any 5-minute period measured under 100% congestion. (R)	
		Packet loss not to exceed .15% engineered (queuing) parameters over any 5-minute period under 100% congestion. (R)	
31	E2E Performance (Data)	No more than 45 ms latency over any 5-minute period measured under 100% congestion (R)	5.3.1.4.3
		Packet loss not to exceed .15% engineered (queuing) parameters over any 5-minute period under 100% congestion. (R)	

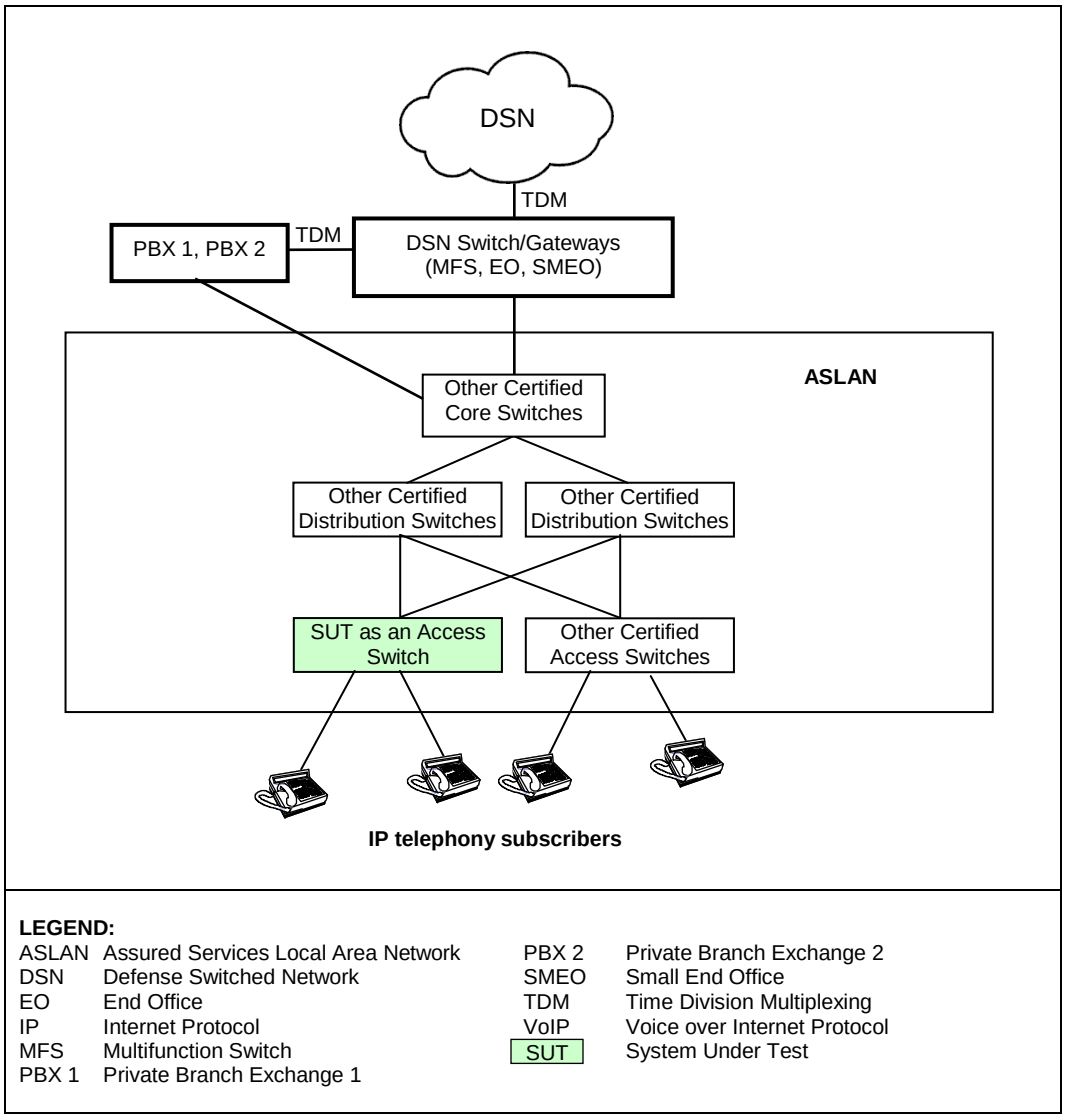
Table 2-1. SUT Capability and Functional Requirements (continued)

ID	Requirement		UCR Reference
32	LAN Network Management	Configuration Control for ASLAN and non-ASLAN. (R)	5.3.1.6.1
33		Operational Controls for ASLAN and non-ASLAN. (R)	5.3.1.6.2
34		Performance Monitoring for ASLAN and non-ASLAN. (R)	5.3.1.6.3
35		Alarms for ASLAN and non-ASLAN. (R)	5.3.1.6.4
36		Reporting for ASLAN and non-ASLAN. (R)	5.3.1.6.5
37	Redundancy	Redundant Power Supplies. (Required on standalone redundant products.)	5.3.1.7.7
38		Chassis Failover. (Required on standalone redundant products.)	
39		Switch Fabric Failover. (Required on standalone redundant products.)	
40		Non-LACP Link Failover. (R)	
41		Fiber Blade Failover. (R)	
42		Stack Failover. (C) (Required if the stack supports more than 96 users.)	
43		CPU (routing engine) blade Failover. (R)	
44	Support IPv6 packets over Ethernet IAW RFC2464. (R)		5.3.5.4
45	Site Requirements	Engineering Requirements: Physical Media for ASLAN and non-ASLAN. (R) (Site requirement)	5.3.1.7.1
46		Battery Back-up. Two hours for non-ASLAN components and eight hours for ASLAN components. (R) (Site requirement)	5.3.1.7.5
47		Availability of 99.999 percent (Special C2), and 99.997 percent (C2) for ASLAN (R), and 99.9 percent (non-C2 and C2(R) for non-ASLAN. (R) (Site requirement)	5.3.1.7.6
48	IA Security requirements	Port-Based access Control IAW IEEE 802.1x. (R)	5.3.1.3.2
49		Secure methods for network configuration. SSH2 instead of Telnet and support RFCs 4251-4254. Must use HTTPS instead of http, and support RFCs 2660 and 2818 for ASLAN and non-ASLAN. (R)	5.3.1.6
50		Security (R)	5.3.1.3.8
51		Must meet IA requirements IAW UCR 2008, Change 2, Section 5.4 for ASLAN and non-ASLAN. (R)	5.3.1.5

LEGEND:

ASLAN	Assured Services Local Area Network	HTTP	HyperText Transfer Protocol	ms	millisecond
C	Conditional	HTTPS	HyperText Transfer Protocol, Secure	PHB	Per Hop Behavior
C2	Command and Control	IA	Information Assurance	QoS	Quality of Service
C2(R)	Command and Control ROUTINE only	IAW	in accordance with	R	Required
CPU	Central Processing Unit	ID	Identification	RFC	Request for Comments
DISR	Department of Defense Information Technology Standards Registry	IEEE	Institute of Electrical and Electronics Engineers	SNMP	Simple Network Management Protocol
DSCP	Differentiated Services Code Point	IPv4	Internet Protocol version 4	SSH2	Secure Shell Version 2
E2E	End-to-End	IPv6	Internet Protocol version 6	SUT	System Under Test
		LACP	Link Aggregation Control Protocol	TCI	Tag Control Information
		LAN	Local Area Network	UCR	Unified Capabilities Requirements
				VLAN	Virtual Local Area Network

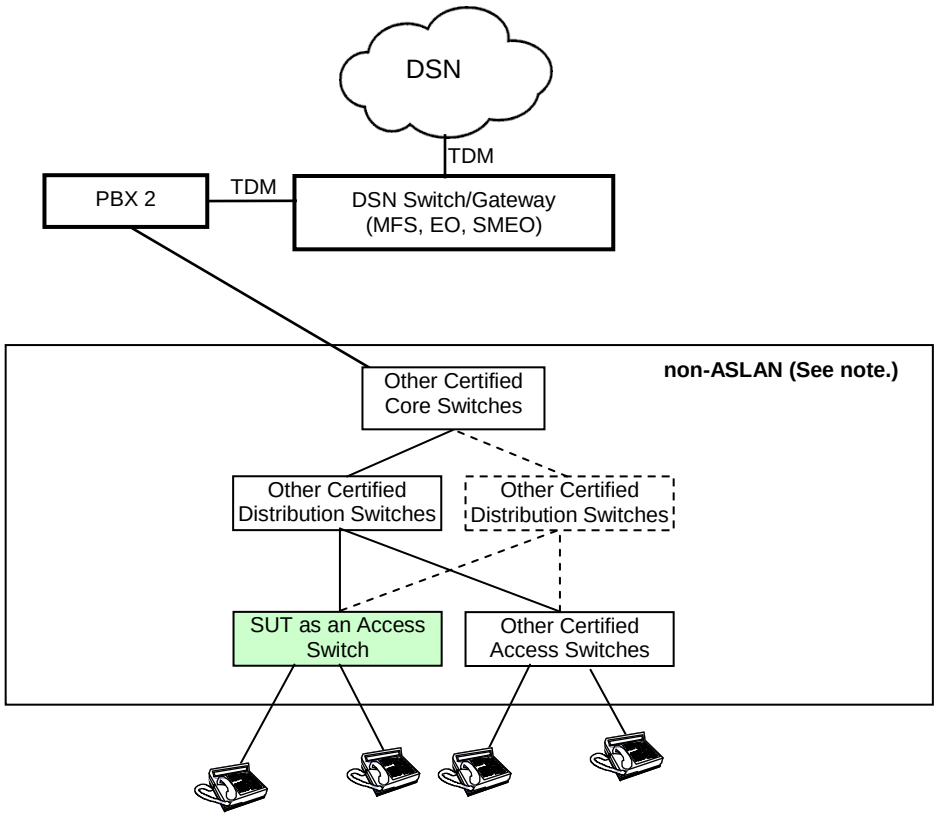
8. TEST NETWORK DESCRIPTION. The SUT was tested at the U.S. Army Information Systems Engineering Command's Technology Integration Center (USAISEC TIC), a DOD Component Test Lab, in a manner and configuration similar to those of the DSN operational environment. A notional diagram of the SUT within an ASLAN VoIP architecture is depicted in Figure 2-2, and the Notional non-ASLAN VoIP architecture is depicted in Figure 2-3. The notional ASLAN and non-ASLAN combined VoIP architecture is depicted in Figure 2-4. The ASLAN test configuration used to test the SUT in a homogeneous network is depicted in Figure 2-5, and the heterogeneous test network configurations are depicted in Figures 2-6 and 2-7.



LEGEND:

ASLAN	Assured Services Local Area Network	PBX 2	Private Branch Exchange 2
DSN	Defense Switched Network	SMEO	Small End Office
EO	End Office	TDM	Time Division Multiplexing
IP	Internet Protocol	VoIP	Voice over Internet Protocol
MFS	Multifunction Switch	SUT	System Under Test
PBX 1	Private Branch Exchange 1		

Figure 2-2. SUT Notional ASLAN VoIP Architecture

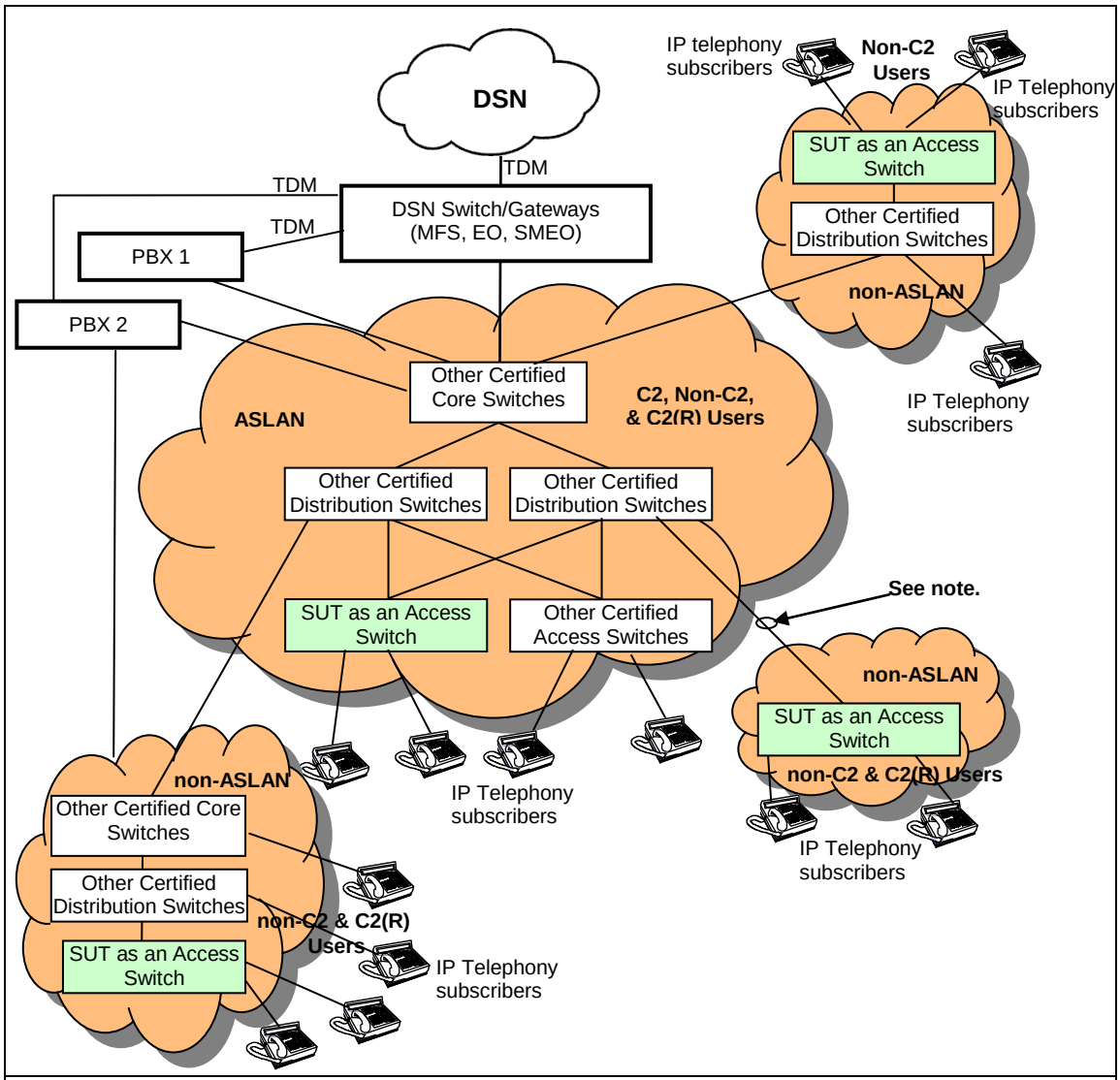


NOTE: Dotted lines denote optional links/components not required for a non-ASLAN. A single point of failure, which could impact more than 96 telephony subscribers, is permitted, and switch modularity is not required.

LEGEND:

ASLAN	Assured Services Local Area Network	PBX 2	Private Branch Exchange 2
DSN	Defense Switched Network	SMEO	Small End Office
EO	End Office	TDM	Time Division Multiplexing
IP	Internet Protocol	VoIP	Voice over Internet Protocol
MFS	Multifunction Switch	SUT	System Under Test

Figure 2-3. SUT Notional Non-ASLAN VoIP Architecture

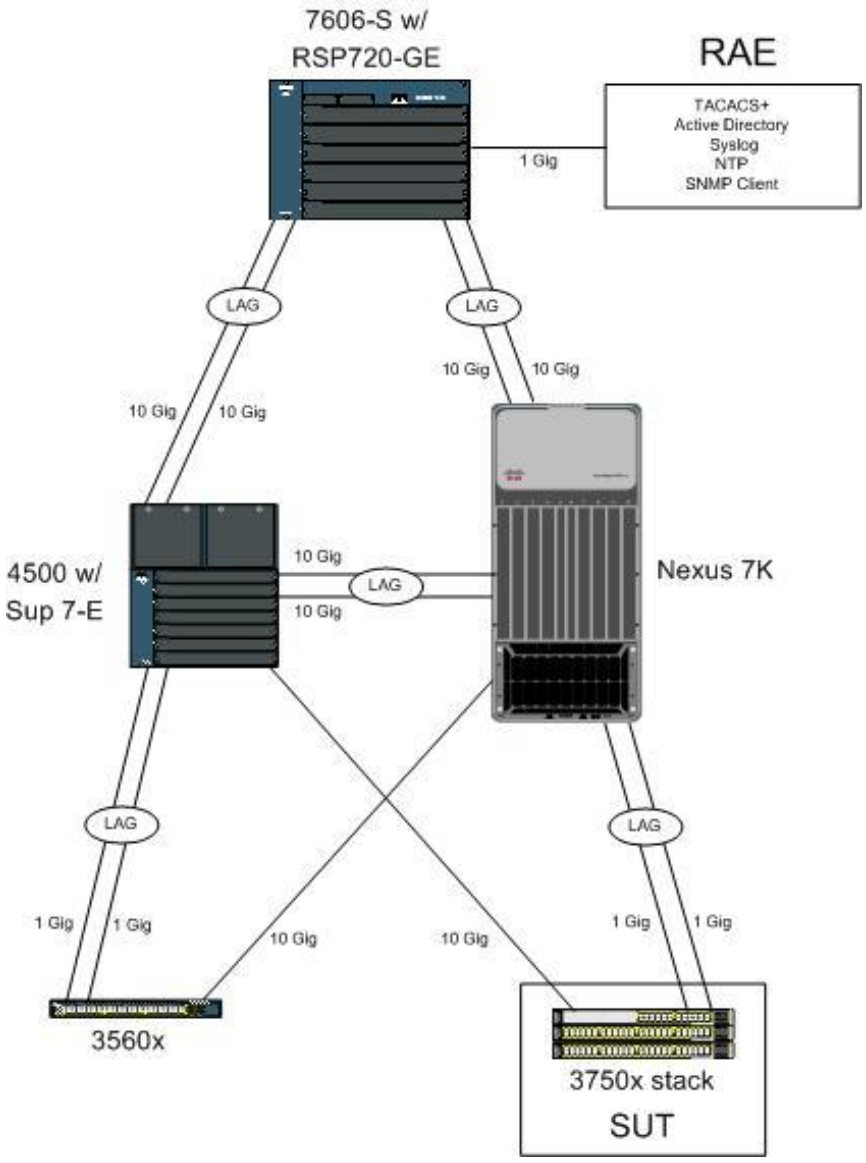


NOTE: A non-ASLAN switch can connect to an ASLAN switch at any layer, provided that the connection does not cause the ASLAN to exceed the traffic engineering limits. A single point of failure, which could impact more than 96 telephony subscribers, is permitted, and switch modularity is not required.

LEGEND:

ASLAN	Assured Services Local Area Network	MFS	Multifunction Switch
C2	Command and Control	PBX 1	Private Branch Exchange 1
C2(R)	Command and Control ROUTINE Only	PBX 2	Private Branch Exchange 2
DSN	Defense Switched Network	SMEO	Small End Office
DUT	Device Under Test	TDM	Time Division Multiplexing
EO	End Office	VoIP	Voice over Internet Protocol
IP	Internet Protocol	SUT	System Under Test

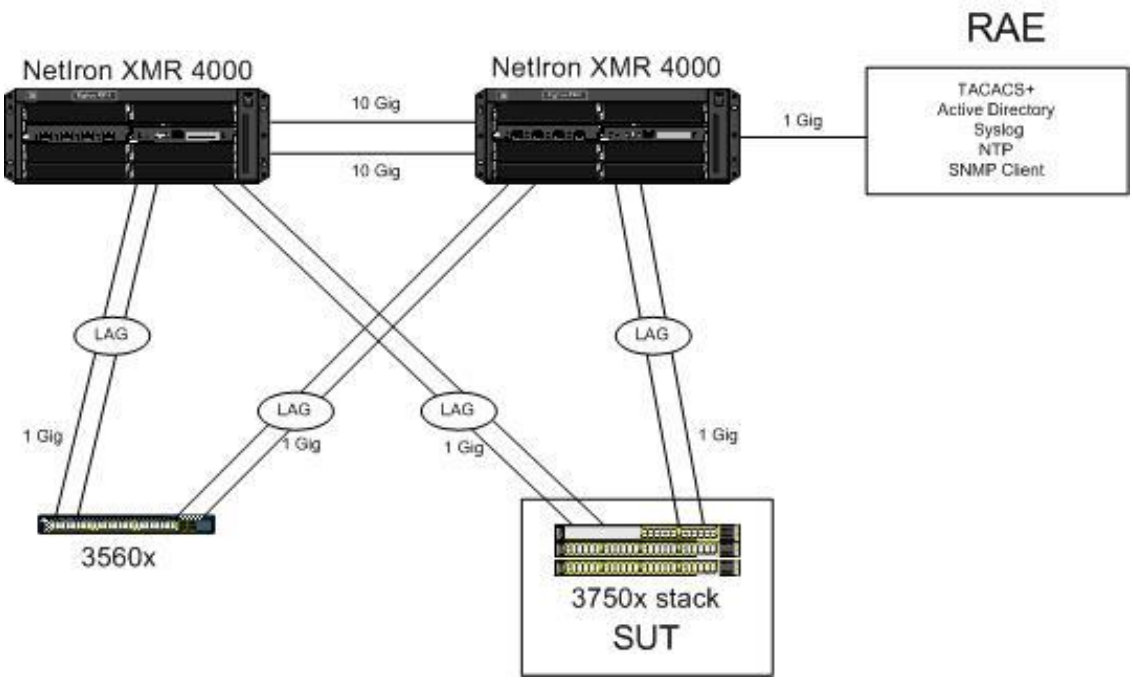
Figure 2-4. SUT Notional ASLAN and non-ASLAN Combined VoIP Architecture



LEGEND:

Gig	Gigabit
LAG	Link Aggregation Group
NTP	Network Time Protocol
RAE	Required Ancillary Equipment
SNMP	Simple Network Management Protocol
SUT	System Under Test
TACACS+	Terminal Access Controller Access-Control System Plus

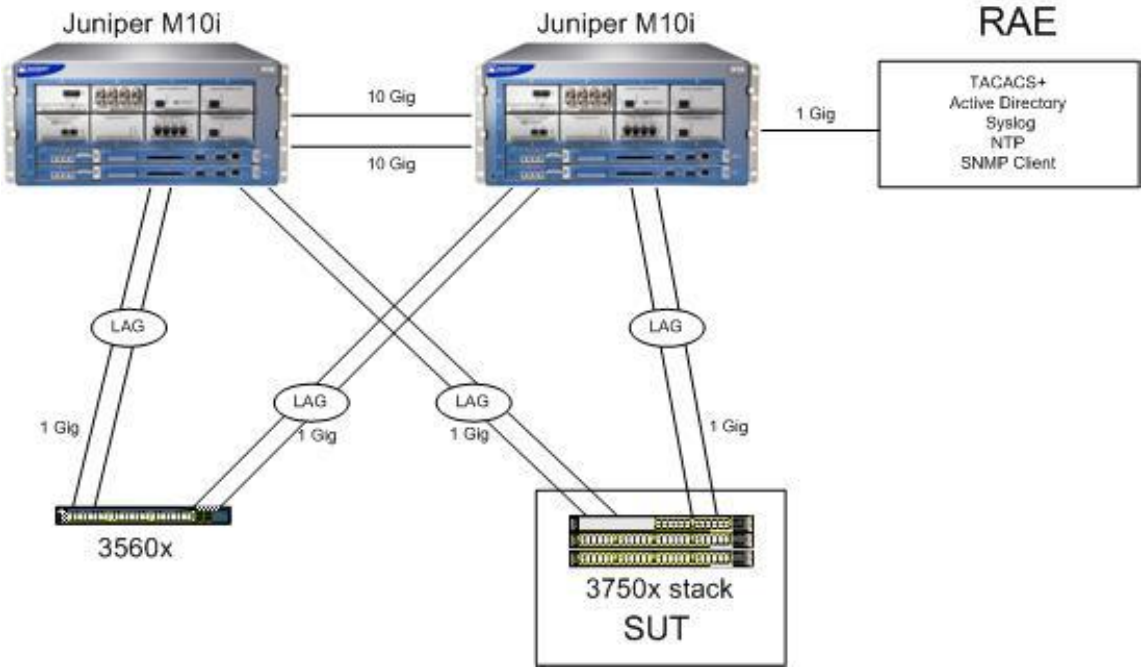
Figure 2-5. Homogeneous Test Configuration



LEGEND:

Gig	Gigabit
LAG	Link Aggregation Group
NTP	Network Time Protocol
RAE	Required Ancillary Equipment
SNMP	Simple Network Management Protocol
SUT	System Under Test
TACACS+	Terminal Access Controller Access-Control System Plus
XMR	Brocade NetIron XMR

Figure 2-6. Heterogeneous Test Configuration with Brocade



LEGEND:

Gig	Gigabit
LAG	Link Aggregation Group
NTP	Network Time Protocol
RAE	Required Ancillary Equipment
SNMP	Simple Network Management Protocol
SUT	System Under Test
TACACS+	Terminal Access Controller Access-Control System Plus

Figure 2-7. Heterogeneous Test Configuration with Juniper

9. SYSTEM CONFIGURATIONS. Table 2-2 provides the system configurations, hardware, and software components tested with the SUT. The SUT is certified with other IP systems listed on the UC APL that are certified for use with an ASLAN or non-ASLAN.

Table 2-2. Tested System Configuration

System Name			Release	
Cisco 7606-S w/ RSP720-GE			12.2(33)SRE2	
Cisco Nexus 7000			NX-OS 5.1(1a)	
Cisco Catalyst 4500 w/ Sup 7-E			IOS XE 3.1(1)SG	
Cisco Catalyst 3560X			IOS 12.2(55)SE1	
Brocade NetIron XMR-4000			FI 4.0.0f	
Juniper M10i			Junos 8.5 R4.3	
SUT (See note)	**Release**	**Function**	**Sub-component**	**Description**
Cisco Catalyst 3750X				
WS-C3750X-48P **WS-C3750X-24P** WS-C3750X-48PF WS-C3750X-48T WS-C3750X-24T	IOS 12.2(55) SE1	Access (Stackable)	N/A	**Catalyst 3750X 48 Port PoE**
				Catalyst 3750X 24 Port PoE
				Catalyst 3750X 48 Port Full PoE
				Catalyst 3750X 48 Port Data
				Catalyst 3750X 24 Port Data
Catalyst 3750x Network Module			**C3KX-NM-10G**	**Catalyst 3K-X 10G Network Module**
			C3KX-NM-1G	**Catalyst 3K-X 1G Network Module**

NOTE: Components bolded and underlined were tested by USAISEC TIC. The other components in the family series were not tested; however, they utilize the same software and hardware, and JITC analysis determined these switches to be functionally identical for interoperability certification purposes. As such, they are also certified for joint use.

LEGEND:

JITC	Joint Interoperability Test Command	SUT	System Under Test
POE	Power over Ethernet	USAISEC TIC	U.S. Army Information Systems Engineering Command Technology Integration Center
SFP	Small Form Factor Pluggable	XMR	Brocade NetIron XMR

10. TESTING LIMITATIONS. None.

11. TEST RESULTS

a. Test Conduct. The SUT was tested as a stacked Layer 2 access switch with both homogeneous and heterogeneous ASLAN configurations. It met all of the requirements by means of testing and/or the vendor's LoC, as outlined in the sub-paragraphs below.

(1) The *UCR 2008, Change 2,* paragraphs 5.3.1.2.1, 5.3.1.7.7, 5.3.1.7.7.1, 5.3.1.7.7.2, state that ASLAN components can have no single point of failure for more than 96 users for C2 and Special C2 users. The *UCR 2008, Change 2,* paragraph 5.3.1.7.7, states the following Redundancy requirements: Redundancy can be met if the product itself provides redundancy internally or if a secondary product is added to the ASLAN to provide redundancy to the primary product. In the event of a component

failure in the network, all calls that are active shall not be disrupted (loss of existing connection requiring redialing), and the path through the network shall be restored within five seconds. If a secondary product has been added to provide redundancy to a primary product, the failover to the secondary product must meet the same requirements. Non-ASLAN components can have a single point of failure for C2(R) and non-C2 users. The SUT supports either 24 or 48 users, depending on the model, and can support more than 96 users in a stacked configuration. The SUT is equipped with redundant uplinks. A standard load of 100 percent of the total bandwidth was used, with 50 percent each of IPv4 and IPv6 traffic. Non-LACP link failover was achieved within 1.32 seconds. For a heterogeneous network using Brocade switches, the maximum Non-LACP link failover time was 3.70 seconds. For a heterogeneous network using Juniper switches, the maximum non-LACP failover was 1.29 seconds. The LACP failover was 0.181 seconds in a homogeneous network, 1.932 seconds in a heterogeneous network using Brocade switches, and 0.054 seconds in a heterogeneous network using Juniper switches. Stack failover occurred in 0.613 seconds in a homogeneous network, 2.008 seconds in a heterogeneous network using Brocade switches, and 0.037 seconds in a heterogeneous network using Juniper switches.

(2) The *UCR 2008, Change 2,* paragraph 5.3.1.3, states that the ASLAN infrastructure components shall meet the requirements in the subparagraphs below. The SUT was tested using 100 percent of the total aggregate uplink bandwidth with 50 percent each of IPv4 and IPv6 traffic. The test included 24.9 percent each of best effort data, OAM, and video traffic; 20.9 percent voice, and 2 percent each of network management and voice/video signaling.

(a) The SUT shall be non-blocking for a minimum of 12.5 percent (maximum voice and video traffic) of its maximum rated output capacity for egress ports that interconnect (trunk) the product to other products. Non-blocking is defined as the capability to send and receive 64- to 1518-byte packets at full duplex rates from ingress ports to egress ports without losing any packets. The SUT met this requirement for all of the test cases by ensuring that higher-priority traffic was queued above lower-priority traffic and best effort data.

(b) The SUT shall have the capability to transport prioritized voice packets (media and signaling) with no more than 1 ms jitter across all switches. All ASLAN infrastructure components shall have the capability to transport prioritized video packets (media and signaling) with no more than 10 ms jitter across all switches. The jitter shall be achievable over any five-minute period measured from ingress ports to egress ports under congested conditions. The SUT met this requirement with a measured jitter of .006 ms for both video and voice.

(c) All core, distribution, and access products shall have the capability to transport prioritized voice packets with no more than .015 percent packet loss. All core, distribution, and access products shall have the capability to transport prioritized video

and preferred data packets with no more than .05 percent packet loss. The packet loss shall be achievable over any five-minute period measured from ingress ports to egress ports under congested conditions. The SUT met this requirement with a measured packet loss of 0.00 percent for voice, video, and preferred traffic.

(d) The SUT shall have the capability to transport prioritized voice packets (media and signaling), with no more than 2 ms latency. All ASLAN infrastructure components shall have the capability to transport prioritized video packets (media and signaling), with no more than 10 ms latency. The latency shall be achievable over any five-minute period measured from ingress ports to egress ports under congested conditions. The SUT met this requirement with a measured latency of 0.028 ms or less for all traffic types with the 1 GB interface.

(3) The *UCR 2008, Change 2,* paragraph 5.3.1.3.1, states that, at a minimum, access products shall provide the following interface rates, and other rates may be provided as conditional interfaces: 10 Mbps in accordance with IEEE 802.3i, and 100 Mbps in accordance with IEEE 802.3u. Refer to Table 2-3 for a detailed list of interfaces that were tested. The SUT met these requirements.

Table 2-3. SUT Interface Status

Interface	Applicability	CRs/FRs (See note 1.)	Status
	Access		Access
Network Management Interfaces for Layer 2 Access Switches			
EIA/TIA (Serial) 232	R	EIA/TIA-232	Met
IEEE 802.3i (10BaseT UTP)	C[2]	7-18, 25-28, 32-36, 44-46, 55-57, 72-75	Met
IEEE 802.3u (100BaseT UTP)	C[2]	7-18, 25-28, 32-36, 44-46, 55-57, 72-75	Met
IEEE 802.3ab (1000BaseT UTP)	C[2]	7-18, 25-28, 32-36, 44-46, 55-57, 72-75	Met
Uplink Interfaces for Layer 2 Access Switches			
IEEE 802.3u (100BaseT UTP)	C[2]	7-18, 28, 44-46, 55-57, 72-75	Met
IEEE 802.3u (100BaseFX)	C[2]	10-18, 28, 44-46, 55-57, 72-75	Met
IEEE 802.3ab (1000BaseT UTP)	C[2]	7-18, 28, 44-46, 55-57, 72-75	Met
IEEE 802.3z1000BaseX Fiber	C[2]	10-18, 28, 44-46, 55-57, 72-75	Met
IEEE 802.3ae (10GBaseX)	C[2]	10-18, 28, 44-46, 55-57, 72-75	Met
Access Interfaces for Layer 2 Access Switches			
IEEE 802.3l (10BASET UTP)	C[2]	7-18, 28, 44-46, 55-57, 72-75	Met
IEEE 802.3u (100BaseT UTP)	C[2]	7-18, 28, 44-46, 55-57, 72-75	Met

Table 2-3. SUT Interface Status (continued)

Interface	Applicability Access	CRs/FRs (See note 1.)	Status Access
IEEE 802.3u (100BaseFX)	C[2]	10-18, 28, 44-46, 55-57, 72-75	Met
IEEE 802.3ab (1000BaseT UTP)	C[2]	7-18, 28, 44-46, 55-57, 72-75	Met
IEEE 802.3z (1000BaseX Fiber)	C[2]	10-18, 28, 44-46, 55-57, 72-75	Met
Generic Requirements for all Interfaces			
Generic Requirements not associated with specific interfaces	R	30-32, 35, 36, 40, 69-71	Met
DoD IPv6 Profile Requirements	R	UCR Section 5.3.5.5	Met
Security	R	79-82	Met[3]

NOTES:
1 The SUT's specific capability and functional requirement ID numbers depicted in the CRs/FRs column can be cross-referenced in Table 2. These requirements are for the following Cisco switches, which are certified in the ASLAN Access layer: **WS-C3750X-48P** 48-port, **WS-C3750X-24P** 24-port, WS-C3750X-48PF 48-port, WS-C3750X-48T 48-port, and WS-C3750X-24T 24-port. The other devices listed (not bolded or underlined) are in the same family series as the SUT but were not tested. However, they utilize the same OS software and hardware as the SUT, and JITC analysis determined them to be functionally identical for interoperability certification purposes.
2 Access layer switches are required to support only one of the following IEEE interfaces: 802,3i, 802.3j, 802.3u, 802.3ab, or 802.3z.
3 Security testing is accomplished via DISA-led Information Assurance test teams, and the results are published in a separate report, Reference (e).

LEGEND:

802.3ab	1000BaseT Gbps Ethernet over twisted pair at 1 Gbps (125 Mbps)	EIA-232	Standard for defining the mechanical and electrical characteristics for connecting Data Terminal Equipment (DTE) and Data Circuit-terminating Equipment (DCE) data communications devices
802.3ae	10 Gbps Ethernet		
802.3i	10BaseT Mbps over twisted pair		
802.3u	Standard for carrier sense multiple access with collision detection at 100 Mbps	FRs	Functional Requirements
		Gbps	Gigabits per second
802.3z	Gigabit Ethernet Standard	ICMP	Internet Control Message Protocol
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	IPv6	Internet Protocol version 6
		JITC	Joint Interoperability Test Command
100BaseFX	100 Mbps Ethernet over fiber	Mbps	Megabits per second
1000BaseFX	1000 Mbps Ethernet over fiber	OS	Operating System
1000BaseT	1000 Mbps (Baseband Operation, Twisted Pair) Ethernet	POAM	Plan of Action and Milestones
		PWR	Power over Ethernet
10GBaseX	10000 Mbps Ethernet over Category 5 Twisted Pair Copper	R	Required
		RFCs	Request for Comments
ASLAN	Assured Services Local Area Network	SFP	Small Form Factor Pluggable
C	Conditional	SNMP	Simple Network Management Protocol
CRs	Capability Requirements	SUT	System Under Test
DISA	Defense Information Systems Agency	TIA	Telecommunications Industry Association
DoD	Department of Defense	UCR	Unified Capabilities Requirements
EIA	Electronic Industries Alliance	UTP	Unshielded Twisted Pair

(4) The *UCR 2008, Change 2,* paragraph 5.3.1.3.2, states that the ASLAN infrastructure components shall provide the following parameters on a per port basis: auto-negotiation, force mode, flow control, filtering, link aggregation, multiple spanning tree, and port-based access control. The SUT was unable to demonstrate proper auto-negotiation. The vendor advises that to avoid this situation, PoE should be disabled on all ports where PoE support for legacy Cisco IP phones is not required. This discrepancy was adjudicated by DISA as having a minor operational impact. The SUT met the remainder of these requirements by means of testing and the vendor's LoC.

(5) The *UCR 2008, Change 2,* paragraph 5.3.1.3.3, states that the ASLAN infrastructure components shall support Differentiated Services Code Points (DSCP) in accordance with Request for Comment (RFC) 2474, as stated in the subparagraphs below:

(a) The ASLAN infrastructure components shall be capable of accepting any packet with a DSCP value (0-63) on an ingress port and assign that packet to a QoS behavior listed in Section 5.3.1.3.6. Using an IP traffic generator, the SUT prioritized traffic for queuing from lowest to highest with distinct IPv4 DSCP values as follows. The IP load included 100 percent of the total aggregate uplink bandwidth with 50 percent each of IPv4 and IPv6 traffic. The test included 24.9 percent each of best effort data, OAM, and video traffic; 20.9 percent voice, and 2 percent each of network management and voice/video signaling. The IP traffic generator/measurement tool recorded that the higher-prioritized traffic was properly queued by the SUT above lower-prioritized best effort traffic. In addition, per the vendor's LoC, the SUT is capable of assigning a DSCP value from 0-63 for each type of traffic, which meets this requirement.

(b) The ASLAN infrastructure components shall be capable of accepting a packet with a DSCP value between 0 and 63 on an ingress port and reassign that packet to any new DSCP value (0-63). Current DSCP values are provided in Section 5.3.3.3.2. This requirement was met per the vendor's LoC.

(c) The ASLAN infrastructure components must be able to support the prioritization of aggregate service classes with queuing according to Section 5.3.1.3.6. Using an IP traffic generator, the SUT prioritized the following traffic for queuing from lowest to highest with distinct IPv6 service class values. The IP load included 100 percent of the total aggregate uplink bandwidth with 50 percent each of IPv4 and IPv6 traffic. The test included 24.9 percent each of best effort data, OAM, and video traffic; 20.9 percent voice, and 2 percent each of network management and voice/video signaling. The IP traffic generator tool recorded that the SUT properly queued the higher-prioritized traffic above the lower-prioritized best effort traffic.

(d) The ASLAN infrastructure components may support the 3-bit user priority field of the IEEE 802.1Q ,2-byte Tag Control Information (TCI) field. Default values are provided in Table 5.3.1-4. If provided, the following Class of Service (CoS) requirements apply. The ASLAN infrastructure components shall be capable of accepting any frame with a user priority value (0-7) on an ingress port and assign that frame to a QoS behavior listed in Section 5.3.1.3.6. The ASLAN infrastructure components shall be capable of accepting any frame with a user priority value (0-7) on an ingress port and reassign that frame to any new user priority value (0-7). This requirement was met per the vendor's LoC.

(6) The *UCR 2008, Change 2,* paragraph 5.3.1.3.4, states that the ASLAN infrastructure components shall be capable of supporting the Virtual LAN (VLAN)

capabilities in accordance with IEEE 802.1Q. Using the IP traffic generator tool, the SUT was configured with a preset VLAN ID tag. The load was captured at both the egress and ingress points to ensure that the SUT assigned the VLAN ID in the proper VLAN. The data was not modified or misplaced, and the assigned VLAN traffic was not lost. In addition, the SUT has the capability to assign any VLAN ID any value from 1 through 4094 per the vendor's LoC.

(7) The *UCR 2008, Change 2,* paragraph 5.3.1.3.5, states that the ASLAN infrastructure components shall meet the Department of Defense Information Technology Standards Registry (DISR) protocol requirements for IPv4 and IPv6. Using an IP traffic generator, the SUT prioritized the following traffic for queuing from lowest to highest with distinct IPv4 DSCP values and IPv6 service class values. The SUT was tested using 100 percent of the total aggregate uplink bandwidth with 50 percent each of IPv4 and IPv6 traffic. The test included 24.9 percent each of effort data, OAM, and video traffic; 20.9 percent voice, and 2 percent each of network management and voice/video signaling. The IP traffic generator/measurement tool recorded that the SUT properly queued the higher prioritized traffic above the lower-prioritized best effort traffic. The IPv4 and IPv6 DISR RFC protocol requirements were also met by the vendor's LoC.

(8) The *UCR 2008, Change 2,* paragraph 5.3.1.3.6, states that the ASLAN infrastructure components shall be capable of providing the following QoS features:

(a) Provide a minimum of four queues. The SUT has the ability to support up to four queues. The SUT met this requirement through testing.

(b) Assign a DSCP or Traffic Class value to any of the queues. The SUT met this requirement through the vendor's LoC.

(c) Support Differentiated Services (DiffServ) per hop behaviors (PHBs) in accordance with RFCs 2474, 2597, 2598, 3140, and 3246. The SUT met this requirement through testing of the queuing process.

(d) Support, at a minimum, one of the following: Weighted Fair Queuing (WFQ) in accordance with RFC 3662, Priority Queuing (PQ) in accordance with RFC 1046, or Class-Based WFQ in accordance with RFC 3366. The SUT met this requirement with Priority Queuing. Note that RFC 1046 is not a standard.

(9) The *UCR 2008, Change 2*, paragraph 5.3.1.3.7, states that the ASLAN infrastructure components shall be capable of providing the following Network Monitoring features:

(a) Simple Network Management Protocol (SNMP) in accordance with RFCs 1157, 2206, 3410, 3411, 3412, 3413, and 3414. The SUT met the requirements for RFCs 1157, 3411, 3412, 3413, 3414 through the vendor LoC. The RFC 3414 requirement was also met through testing**.** RFC 2206 is not an SNMP standard;

itdefines the Resource Reservation Protocol Management Information Base (RSVP MIB) only. Since RSVP functionality is not supported on the SUT, RFC 2206 is Not Applicable. RFC 3410 is Informational, i.e., “This memo provides information for the Internet community. It does not specify an Internet-standard of any kind.” RFC 3410 is Not Applicable.

(b) SNMP Traps in accordance with RFC 1215. The SUT met this requirement through testing. The SilverCreek Test Suite was used to capture SNMP traps. The speed of an individual port on each switch was changed from 1000 to 100 and back again for the port configuration change test. All of the switches sent a trap, "CISCO-CONFIG-MAN-MIB", but the trap did not specify a port number.

(c) Remote Monitoring (RMON) in accordance with RFC 2819. The SUT met this requirement through the vendor’s LoC.

(d) Coexistence between Version 1, Version 2, and Version 3 of the Internet-standard Network Management Framework in accordance with RFC 3584. Since RFC 3584 is a Best Current Practice and not a standard, RFC 3584 is Not Applicable.

(e) The Advanced Encryption Standard (AES) Cipher Algorithm in the SNMP User-based Security Model in accordance with RFC 3826 is tested by DISA-led Information Assurance test teams, and the results are published in a separate report, Reference (e).

(10) The *UCR 2008, Change 2,* paragraph 5.3.1.3.9, states that all switches must meet Product Requirements in accordance with UCR 2008, Change 2, Table 5.3.1-5. The SUT met these requirements listed in Table 5.3.1-5 by means of testing and/or vendor’s LoC as stipulated throughout this document.

(11) The *UCR 2008, Change 2,* section 5.3.1.4, states that the ASLAN infrastructure components shall be capable of meeting the End-to-End (E2E) performance requirements for voice, video, and data services. End-to-end performance across a LAN is measured from the traffic ingress point to the traffic egress port. The requirements are measured over any five-minute period under congested conditions. “Congested condition” is defined as using 100 percent of the total aggregate uplink bandwidth with 50 percent each of IPv4 and IPv6 traffic. The test included 24.9 percent each of best effort data, OAM, and video traffic; 20.9 percent voice, and 2 percent each of network management and voice/video signaling. The test also included 100 percent of link capacities as defined by baseline traffic engineering, i.e., 25 percent voice/signaling, 25 percent video, 25 percent preferred data, and 25 percent best effort traffic. The E2E requirements are ASLAN requirements. However, all of the E2E voice, video, and data services performance requirements were met by the SUT when included within an ASLAN. Refer to paragraphs 11.b.(2)(b), 11.b.(2)(c), and 11.b.(2)(d).

(12) The *UCR 2008, Change 2*, section 5.3.1.6, states that LAN infrastructure components must meet the requirements in the subparagraphs below. Near Real Time (NRT) is defined as within five seconds of detecting the event, excluding transport time.

(a) Local area networks shall have the ability to perform remote network product configuration/reconfiguration of objects that have existing DoD GIG management capabilities. The NMS shall report configuration change events in NRT, regardless of whether the change was authorized or not. The system shall report the success or failure of authorized configuration change attempts in NRT. The SUT met this requirement through testing.

(b) The LAN infrastructure components must provide metrics to the NMSs to allow them to make decisions on managing the network. Network management systems shall have an automated NM capability to obtain the status of networks and associated assets in NRT 99 percent of the time (with 99.9 percent as an Objective Requirement). Specific metrics are defined in the *UCR 2008, Change 2,* sections 5.3.2.17 and 5.3.2.18. The SUT met this requirement with the vendor's LoC.

(c) The LAN components shall be capable of providing status changes in NRT 99 percent of the time (with 99.9 percent as an Objective Requirement) by means of an automated capability. An NMS will have an automated NM capability to obtain the status of networks and associated assets 99 percent of the time (with 99.9 percent as an Objective Requirement) in NRT. The NMS shall collect statistics and monitor bandwidth utilization, delay, jitter, and packet loss. The SUT met this requirement with the vendor's LoC.

(d) The LAN components shall be capable of providing SNMP alarm indications to an NMS. The NMS will have the NM capability to perform automated fault management of the network, to include problem detection, fault correction, fault isolation and diagnosis, problem tracking until corrective actions are completed, and historical archiving. Alarms will be correlated to eliminate those that are duplicate or false, initiate tests, and perform diagnostics to isolate faults to a replaceable component. Alarms shall be reported as TRAPs via SNMP in NRT. More than 99.95 percent of alarms shall be reported in NRT. The SUT met this requirement with the vendor's LoC.

(e) An NMS will have the NM capability of automatically generating and providing an integrated/ correlated presentation of the network and all associated networks. The SUT fully supports SNMP MIBs that can be used to build visual representations of the network using an NMS.

(13) The *UCR 2008, Change 2*, paragraphs 5.3.1.3.8, 5.3.1.5, 5.3.1.6, state that ASLAN components must meet security requirements. Security is tested by DISA-led Information Assurance test teams, and the results are published in a separate report, Reference (e).

(14) The *UCR 2008 Change 2,* paragraph 5.3.1.7.6 states that ASLAN components must meet an availability of 99.999 percent for Special C2 users and 99.997 percent for C2 users. The SUT provides 99.999 percent availability using Software High Availability features, i.e., Open Shortest Path First (OSPF), Rapid Spanning Tree Protocol (RSTP), etc. Please note that the calculation of actual LAN availability is site-specific. Each site will have a different Mean Time to Repair (MTTR) and LAN architecture, i.e., link redundancy, chassis redundancy, supervisor redundancy, etc.

b. System Interoperability Results. The SUT is certified for joint use within the DSN as a Layer 2 access switch (stackable). It is also certified with any digital switching systems on the UC APL which are certified for use with an ASLAN or non-ASLAN.

12. TEST AND ANALYSIS REPORT. In accordance with the Program Manager's request, no detailed test report was developed. The JITC distributes interoperability information via the JITC Electronic Report Distribution (ERD) system, which uses Unclassified-But-Sensitive Internet Protocol Router Network (NIPRNet) e-mail. More comprehensive interoperability status information is available via the JITC System Tracking Program (STP). The STP is accessible by .mil/gov users on the NIPRNet at https://stp.fhu.disa.mil. Test reports, lessons learned, and related testing documents and references are on the JITC Joint Interoperability Tool (JIT) at http://jit.fhu.disa.mil (NIPRNet). Information related to DSN testing is on the Telecom Switched Services Interoperability (TSSI) website at http://jitc.fhu.disa.mil/tssi. Due to the sensitivity of the information, the Information Assurance Accreditation Package (IAAP) that contains the approved configuration and deployment guide must be requested directly through U.S. Government civilian or uniformed military personnel from the Unified Capabilities Certification Office (UCCO), email: ucco@disa.mil.

This page intentionally left blank.