



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

22 Jun 11

SUBJECT: Special Interoperability Test Certification of the Cisco Catalyst 4500E series Switch with Internetwork Operating System (IOS[®]) 12.2(53) SG3

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

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

2. The Cisco Catalyst 4507R-E Switch with IOS[®] 12.2(53) SG3 is hereinafter referred to as the System Under Test (SUT). The SUT with the WS-X45-SUP6-E processor meets all of its critical interoperability requirements and is certified for joint use within the Defense Information System Network (DISN) as a Layer 2/3 Assured Services Local Area Network (ASLAN) core, distribution, and access switch. The SUT is only certified for use as a Layer 2 access switch with the WS-X45-SUP6L-E processor. 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: 1000/10000BaseSX/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 Catalyst 4503-E, 4506-E, and 4510R-E 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 with the WS-X45-SUP6-E or WS-X45-SUP6L-E processor in the same manner as the SUT.

The SUT is certified to support Assured Services within an ASLAN. 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 C2R 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.

JITC Memo, JTE, Special Interoperability Test Certification of the Cisco Catalyst 4500E series Switch with Internetwork Operating System (IOS®) 12.2(53) SG3

Testing of the SUT did not include video services or data applications; however, simulated preferred data, best effort data, and video traffic was 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 JITC. This certification expires upon changes that could affect interoperability, but no later than three years from the date the DISA Certification and Accreditation (CA) provided a positive Recommendation.

3. This finding is based on interoperability testing conducted by the U.S. 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 DISA CA Recommendation. Interoperability testing was conducted by the USAISEC-TIC and by JITC at the Global Information Grid Network Test Facility, Fort Huachuca, Arizona, from 21 June through 25 October 2010 Fort Huachuca, Arizona. Review of the vendor's LoC was completed on 22 June 2010. DISA adjudication of outstanding TDRs was completed on 18 February 2011. The DISA CA provided a positive Recommendation on 26 May 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 capability and functional requirements are listed in Table 2.

Table 1. SUT Interface Status

Interface	Applicability			CRs/FRs (See note 1.)	Status		
	Co	D	A		Co	D	A
Network Management Interfaces for Core, Distribution, Access Layer Switches							
EIA/TIA-232 (Serial)	R	R	R	EIA/TIA-232	Met ²	Met ²	Met
IEEE 802.3i (10BaseT UTP)	C	C	C	7-18, 25-28, 32-36, 44-46, 55-57, 72-75	Not Tested		
IEEE 802.3u (100BaseT UTP)	C	C	C	7-18, 25-28, 32-36, 44-46, 55-57, 72-75	Met ²	Met ²	Met
IEEE 802.3ab (1000BaseT UTP)	C	C	C	7-18, 25-28, 32-36, 44-46, 55-57, 72-75	Met ²	Met ²	Met
Uplink Interfaces for Core, Distribution Layer Switches							
IEEE 802.3u (100BaseT UTP)	R	R	C ³	7-18, 28, 44-46, 55-57, 72-75	Met ²	Met ²	Met
IEEE 802.3u (100BaseFX)	C	C	C ³	10-18, 28, 44-46, 55-57, 72-75	Not Tested		
IEEE 802.3ab (1000BaseT UTP)	C	C	C ³	7-18, 28, 44-46, 55-57, 72-75	Met ²	Met ²	Met
IEEE 802.3z (1000BaseX Fiber)	R	R	C ³	10-18, 28, 44-46, 55-57, 72-75	Met ²	Met ²	Met
IEEE 802.3ae (10GBaseX)	C	C	C ³	10-18, 28, 44-46, 55-57, 72-75	Met ²	Met ²	Met
Access Interfaces for Core, Distribution, Access Layer Switches							
IEEE 802.3i (10BaseT UTP)	C	C	C ³	7-18, 28, 44-46, 55-57, 72-75	Not Tested		
IEEE 802.3u (100BaseT UTP)	R	R	C ³	7-18, 28, 44-46, 55-57, 72-75	Met ²	Met ²	Met
IEEE 802.3u (100BaseFX)	C	C	C ³	10-18, 28, 44-46, 55-57, 72-75	Not Tested		
IEEE 802.3ab (1000BaseT UTP)	C	C	C ³	7-18, 28, 44-46, 55-57, 72-75	Met ²	Met ²	Met
IEEE 802.3z (1000BaseX Fiber)	R	R	C ³	10-18, 28, 44-46, 55-57, 72-75	Met ²	Met ²	Met
Generic Requirements for all Interfaces							
Generic Requirements not associated with specific interfaces	R	R	R	30-32, 35, 36, 40, 69-71	Met ²	Met ²	Met
DoD IPv6 Profile Requirements	R	R	R	UCR Section 5.3.5.5	Met ²	Met ²	Met
Security	R	R	R	79-82	Met ⁴	Met ⁴	Met ⁴

JITC Memo, JTE, Special Interoperability Test Certification of the Cisco Catalyst 4500E series Switch with Internetwork Operating System (IOS®) 12.2(53) SG3

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 core, distribution, and access layers with the Supervisor 6-E processor: Catalyst 4507R-E , 4510R-E, 4503-E, and 4506E. The JITC tested the devices that are bolded and underlined. The other devices listed that are not bolded or underlined are in the same family series as the SUT were not tested; however, they utilize the same OS software and similar hardware and JITC analysis determined them to be functionally identical for interoperability certification purposes.		
2	The SUT met the core, distribution and access switch requirements with the WS-X45-SUP6-E processor which supports Layer 2/3 functions. The SUT only met the Layer 2 access switch requirements when configured with the WS-X45-SUP6L-E processor.		
3	Access layer switches are required to support only one of the following IEEE interfaces: 802.3i, 802.3j, 802.3u, 802.3ab and 802.3z.		
4	Security testing is accomplished via DISA-led IA test teams and published in a separate report, Reference (e).		
LEGEND:			
802.3ab	1000BaseT Gbps Ethernet over twisted pair at 1 Gbps (125 Mbps)	DoD	Department of Defense
802.3ae	10 Gbps Ethernet	EIA	Electronic Industries Alliance
802.3i	10BaseT Mbps over twisted pair	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
802.3u	Standard for carrier sense multiple access with collision detection at 100 Mbps		
802.3z	Gigabit Ethernet Standard	FRs	Functional Requirements
10BaseT	10 Mbps (Baseband Operation, Twisted Pair) Ethernet	Gbps	Gigabits per second
100BaseT	100 Mbps (Baseband Operation, Twisted Pair) Ethernet	IA	Information Assurance
		ID	Identification
100BaseFX	100 Mbps Ethernet over fiber	ICMP	Internet Control Message Protocol
1000BaseFX	1000 Mbps Ethernet over fiber	IEEE	Institute of Electrical and Electronics Engineers
1000BaseT	1000 Mbps (Baseband Operation, Twisted Pair) Ethernet	IPv6	Internet Protocol version 6
		JITC	Joint Interoperability Test Command
10GBaseX	10000 Mbps Ethernet over Category 5 Twisted Pair Copper	Mbps	Megabits per second
A	Access	NA	Not Applicable
ASLAN	Assured Services Local Area Network	OS	Operating System
C	Conditional	R	Required
Co	Core	SUT	System Under Test
CRs	Capability Requirements	TIA	Telecommunications Industry Association
D	Distribution	UCR	Unified Capabilities Requirements
DISA	Defense Information Systems Agency	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 50% for core and distribution layer switches and 12.5% blocking 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	100 Mbps IAW IEEE 802.3u and 1 Gbps IAW IEEE 802.3z for core and distribution layer components and 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	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) Conditional for Core	
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) Conditional for Core	
14	Multiple Spanning Tree IAW IEEE 802.1s. (R) Conditional for Core	
15	Rapid Reconfiguration of Spanning Tree IAW IEEE 802.1w. (R) Conditional for Core	

JITC Memo, JTE, Special Interoperability Test Certification of the Cisco Catalyst 4500E series Switch with Internetwork Operating System (IOS®) 12.2(53) SG3

Table 2. SUT Capability and Functional Requirements (continued)

ID	Requirement (See note.)		UCR Reference
16	LACP link Failover and Link Aggregation IAW IEEE 802.3ad (uplink ports only) core and distribution switches (C)		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 RFC's 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	MPLS	MPLS May not add measurable Loss or Jitter to system. (C)	5.3.1.8.4.1
45		MPLS Conforms to RFCs in Table 5.3.1-14. (C)	5.3.1.8.4.1
46		MPLS Support L2 and L3 VPNs. (C)	5.3.1.8.4.2.1 /2
The IPv6 requirements (47 through 75) below apply only to Layer 3 LAN switches			
47	IPv6 Product Requirements: Dual Stack for IPv4 and IPv6 IAW RFC 4213 if routing functions are supported. (C)		5.3.5.4
48	IPv6 System Requirements	Support IPv6 IAW RFCs 2460 and 5095 if routing functions are supported. (C)	5.3.5.4
49		Support IPv6 packets over Ethernet IAW RFC2464. (R)	5.3.5.4
50		Support MTU discovery IAW RFC 1981 if routing functions are supported. (R)	5.3.5.4.1
51		Support a minimum MTU of 1280 IAW RFCs 2460 and 5095. (C)	5.3.5.4.1
52		Shall support IPv6 addresses IAW RFC4291. (R)	5.3.5.4.3
53		Shall support IPv6 scoped addresses IAW RFC4007. (R)	5.3.5.4.3
54		if routing functions are supported: If DHCP is supported must be IAW RFC3315, if DHCPv6 is supported it shall be IAW RFC 3313. (C)	5.3.5.4.4

Table 2. SUT Capability and Functional Requirements (continued)

ID	Requirement (See note.)		UCR Reference
55	IPv6 Router Advertisements	If the system supports routing functions, the system 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, and shall prefer routers that are reachable over routers whose reachability is suspect or unknown. (C)	5.3.5.4.5.2
56		If the system supports routing functions, the system shall include the MTU value in the router advertisement message for all links in accordance with RFC 2461 and RFC 4861. (C)	
57		IPv6 Neighbor Discovery: The system shall not set the override flag bit in the neighbor advertisement message for solicited advertisements for anycast addresses or solicited proxy advertisements. (R)	
58	IPv6 Neighbor Discovery	if routing functions are supported: Neighbor discovery IAW RFCs 2461 and 4861. (C)	5.3.5.4.5
59		The system shall not set the override flag bit in the neighbor advertisement message for solicited advertisements for anycast addresses or solicited proxy advertisements. (R)	
60		The system shall set the override flag bit in the neighbor advertisement message to “1” if the message is not an anycast address or a unicast address for which the system is providing proxy service. (R)	
61	IPv6 SLAAC and Manual Address Assignment	If the system supports stateless IP address Auto-configuration, the system shall support IPv6 SLAAC for interfaces supporting UC functions in accordance with RFC 2462 and RFC 4862. (C)	5.3.5.4.6
62		If the product supports IPv6 SLAAC, the product shall have a configurable parameter that allows the function to be enabled and disabled. (C)	
63		If the product supports IPv6 SLAAC, the product shall have a configurable parameter that allows the “managed address configuration” flag and the “other stateful configuration” flag to always be set and not perform stateless auto-configuration. (C)	
64		If the product supports stateless IP address auto-configuration including those provided for the commercial market, the DAD shall be disabled in accordance with RFC 2462 and RFC 4862. (R)	
65		The system shall support manual assignment of IPv6 addresses. (R)	
66	IPv6 ICMP	If the system provides routing functions, the system shall default to using the “managed address configuration” flag and the “other stateful flag” set to TRUE in their router advertisements when stateful auto-configuration is implemented. (C)	5.3.5.4.7
67		The system shall support the ICMPv6 as described in RFC 4443. (R)	
68		The system shall have a configurable rate limiting parameter for rate limiting the forwarding of ICMP messages. (R)	
69		The system shall support the capability to enable or disable the ability of the system to generate a Destination Unreachable message in response to a packet that cannot be delivered to its destination for reasons other than congestion. (R) Required if LS supports routing functions.	
70		The system 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. (R)	
71	IPv6 Routing Functions	The system shall validate ICMPv6 messages, using the information contained in the payload, prior to acting on them. (R)	5.3.5.4.8
72		If the system supports routing functions, the system shall support the OSPF for IPv6 as described in RFC 5340. (C)	
73		If the system supports routing functions, the system shall support securing OSPF with Internet Protocol Security (IPSec) as described for other IPSec instances in UCR 2008, Section 5.4. (C)	
74		If the system supports routing functions, the system shall support OSPF for IPv6 as described in RFC 2740, router to router integrity using IP authentication header with HMAC-SHA1-96 with ESP and AH as described in RFC 2404, shall support OSPFv3 IAW RFC 4552. (C)	
75	Site Requirements	If the system supports routing functions, the system shall support the Multicast Listener Discovery (MLD) process as described in RFC 2710 and extended in RFC 3810. (C)	5.3.1.7.1
76		Engineering Requirements: Physical Media for ASLAN and non-ASLAN. (R) (Site requirement)	
77		Battery Back up two hours for non-ASLAN components and eight hours for ASLAN components. (R) (Site requirement)	
78	IA Security requirements	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
79		Port-Based access Control IAW IEEE 802.1x. (R) Conditional for Core	5.3.1.3.2
80		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
81	IA Security requirements	Security (R)	5.3.1.3.8
82		Must meet IA requirements IAW UCR 2008, Change 2, Section 5.4 for ASLAN and non-ASLAN. (R)	5.3.1.5

NOTE: All requirements are for core, distribution, and access layer components unless otherwise specified.

Table 2. SUT Capability and Functional Requirements (continued)

LEGEND:					
AH	Authentication Header	HTTP	Hypertext Transfer Protocol	ms	millisecond
ASLAN	Assured Services Local Area Network	HTTPS	Hyper Text Transfer Protocol, Secure	MTU	Maximum Transmission Unit
C	Conditional	IA	Information Assurance	OSPF	Open Shortest Path First
C2	Command and Control	IAW	in accordance with	OSPFv3	Open Shortest Path First Version 3
C2(R)	Command and Control ROUTINE only	ICMP	Internet Control Message Protocol	PHB	Per Hop Behavior
CPU	Central Processing Unit	ICMPv6	Internet Control Message Protocol for IPv6	QoS	Quality of Service
DAD	Duplicate Address Detection	ID	Identification	R	Required
DHCP	Dynamic Host Configuration Protocol	IEEE	Institute of Electrical and Electronics Engineers	RFC	Request for Comments
DHCPv6	Dynamic Host Configuration Protocol for IPv6	IPv4	Internet Protocol version 4	SHA	Secure Hash Algorithm
DISR	Department of Defense Information Technology Standards Registry	IPv6	Internet Protocol version 6	SLAAC	Stateless Auto Address Configuration
DSCP	Differentiated Services Code Point	L2	Layer 2	SNMP	Simple Network Management Protocol
E2E	End-to-End	L3	Layer 3	SSH2	Secure Shell Version 2
ESP	Encapsulating Security Payload	LACP	Link Aggregation Control Protocol	SUT	System Under Test
Gbps	Gigabits per second	LAN	Local Area Network	TCI	Tag Control Information
HMAC	Hash-based Message Authentication Code	LS	LAN Switch	UC	Unified Capabilities
		Mbps	Megabits per second	UCR	Unified Capabilities Requirements
		MPLS	Multiprotocol Label Switching	VLAN	Virtual Local Area Network
				VPN	Virtual Private Network

5. In accordance with (IAW) the Program Manager’s request, no detailed test report was developed. 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 through government civilian or uniformed military personnel from the Unified Capabilities Certification Office (UCCO), e-mail: ucco@disa.mil.

JITC Memo, JTE, Special Interoperability Test Certification of the Cisco Catalyst 4500E series Switch with Internetwork Operating System (IOS®) 12.2(53) SG3

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 1002807.

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 MARCORSSYSCOM, 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 Dec 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 4500 Enhanced (E) with sup6L-E/sup6E Internetwork Operating System (IOS) 12.2(53)SG3 (Tracking Number 1002807)," 26 May 2011

CERTIFICATION TESTING SUMMARY

1. SYSTEM TITLE. Cisco Catalyst 4500E series Switch with Internetwork Operating System (IOS[®]) 12.2(53) SG3; hereinafter, referred to as the System Under Test (SUT).

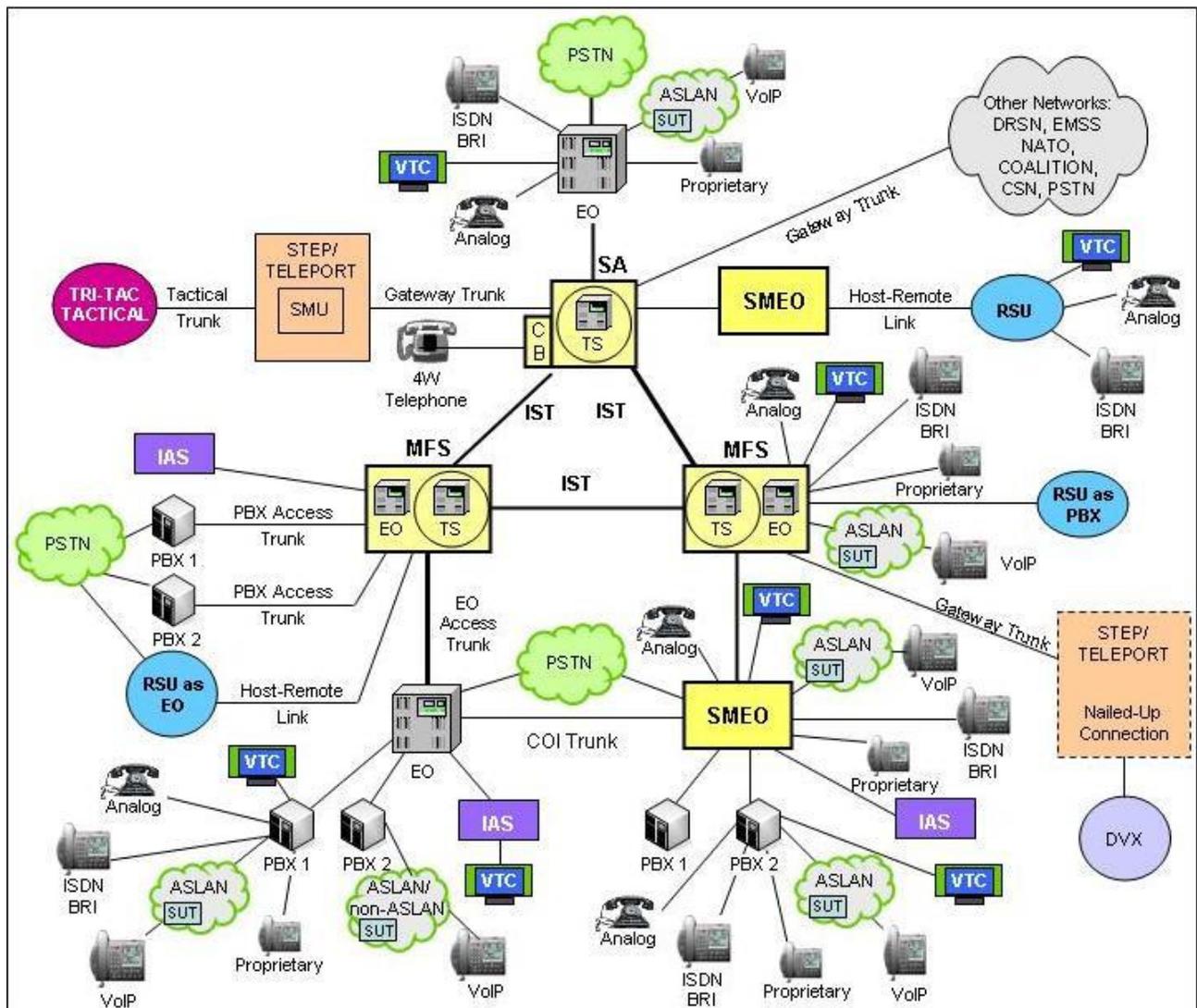
2. PROPONENT. Headquarters, U.S. Army Information Systems Engineering Command (HQ USAISEC).

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

4. TESTER. U.S. Army Information Systems Engineering Command, Technology Integration Center (USAISEC-TIC) and Joint Interoperability Test Command, both at Fort Huachuca, Arizona.

5. SYSTEM 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 with the WS-X45-WS-X45-SUP6-E processor is certified as a Layer 2/3 core, distribution, and access switch, and as a Layer 2 access switch with the WS-X45-SUP6L-E processor. The SUT is interoperable for joint use with other Assured Services Local Area Network (ASLAN) components listed on the Unified Capabilities (UC) Approved Products List (APL) with the following interfaces: 1000/10000 Base SX/LX, 100BaseFX and 10/100/1000 BaseT. The Cisco Catalyst 4507R-E was the system tested; however, the Cisco Catalyst 4503R-E, 4510R-E, and 4506R-E 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 with the WS-X45-SUP6-E or WS-X45-SUP6L-E processor in the same manner as the SUT.

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 is depicted in Figure 2-1, which depicts the relationship of the ASLAN and non-ASLAN to the DSN switch types.



LEGEND:

- | | | | |
|-------|-------------------------------------|---------|---|
| 4W | 4-Wire | NATO | North Atlantic Treaty Organization |
| ASLAN | Assured Services Local Area Network | PBX | Private Branch Exchange |
| BRI | Basic Rate Interface | PBX 1 | Private Branch Exchange 1 |
| CB | Channel Bank | PBX 2 | Private Branch Exchange 2 |
| COI | Community of Interest | PC | Personal Computer |
| CSN | Canadian Switch Network | PSTN | Public Switched Telephone Network |
| DRSN | Defense Red Switch Network | RSU | Remote Switching Unit |
| DSN | Defense Switched Network | SMEO | Small End Office |
| DVX | Deployable Voice Exchange | SMU | Switched Multiplex Unit |
| EMSS | Enhanced Mobile Satellite System | STEP | Standardized Tactical Entry Point |
| EO | End Office | TDM/P | Time Division Multiplex/Packetized |
| IAS | Integrated Access Switch | Tri-Tac | Tri-Service Tactical Communications Program |
| IP | Internet Protocol | TS | Tandem Switch |
| ISDN | Integrated Services Digital Network | VoIP | Voice over Internet Protocol |
| IST | Interswitch Trunk | VTC | Video Teleconferencing |
| MFS | Multifunction Switch | SUT | 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 UCR 2008, Change 2, and verified through JITC testing and review of the vendor’s Letters of Compliance (LoC).

Table 2-1. 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 50% for core and distribution layer switches and 12.5% blocking 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	100 Mbps IAW IEEE 802.3u and 1 Gbps IAW IEEE 802.3z for core and distribution layer components and 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) Conditional for Core	
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) Conditional for Core	
14		Multiple Spanning Tree IAW IEEE 802.1s. (R) Conditional for Core	
15	Rapid Reconfiguration of Spanning Tree IAW IEEE 802.1w. (R) Conditional for Core		
16	LACP link Failover and Link Aggregation IAW IEEE 802.3ad (uplink ports only) core and distribution switches (C)		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 RFC's 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 (See note.)		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	MPLS	MPLS May not add measurable Loss or Jitter to system. (C)	5.3.1.8.4.1
45		MPLS Conforms to RFCs in Table 5.3.1-14. (C)	5.3.1.8.4.1
46		MPLS Support L2 and L3 VPNs. (C)	5.3.1.8.4.2.1 /2
The IPv6 requirements (47 through 75) below apply only to Layer 3 LAN switches			
47	IPv6 Product Requirements: Dual Stack for IPv4 and IPv6 IAW RFC 4213 if routing functions are supported. (C)		5.3.5.4
48	IPv6 System Requirements	Support IPv6 IAW RFCs 2460 and 5095 if routing functions are supported. (C)	5.3.5.4
49		Support IPv6 packets over Ethernet IAW RFC2464. (R)	5.3.5.4
50		Support MTU discovery IAW RFC 1981 if routing functions are supported. (R)	5.3.5.4.1
51		Support a minimum MTU of 1280 IAW RFCs 2460 and 5095. (C)	5.3.5.4.1
52		Shall support IPv6 addresses IAW RFC4291. (R)	5.3.5.4.3
53		Shall support IPv6 scoped addresses IAW RFC4007. (R)	5.3.5.4.3
54		if routing functions are supported: If DHCP is supported must be IAW RFC3315, if DHCPv6 is supported it shall be IAW RFC 3313. (C)	5.3.5.4.4
55	IPv6 Router Advertisements	If the system supports routing functions, the system 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, and shall prefer routers that are reachable over routers whose reachability is suspect or unknown. (C)	5.3.5.4.5.2
56		If the system supports routing functions, the system shall include the MTU value in the router advertisement message for all links in accordance with RFC 2461 and RFC 4861. (C)	
57		IPv6 Neighbor Discovery: The system shall not set the override flag bit in the neighbor advertisement message for solicited advertisements for anycast addresses or solicited proxy advertisements. (R)	
58	IPv6 Neighbor Discovery	if routing functions are supported: Neighbor discovery IAW RFCs 2461 and 4861. (C)	5.3.5.4.5
59		The system shall not set the override flag bit in the neighbor advertisement message for solicited advertisements for anycast addresses or solicited proxy advertisements. (R)	
60		The system shall set the override flag bit in the neighbor advertisement message to "1" if the message is not an anycast address or a unicast address for which the system is providing proxy service. (R)	
61	IPv6 SLAAC and Manual Address Assignment	If the system supports stateless IP address Auto-configuration, the system shall support IPv6 SLAAC for interfaces supporting UC functions in accordance with RFC 2462 and RFC 4862. (C)	5.3.5.4.6
62		If the product supports IPv6 SLAAC, the product shall have a configurable parameter that allows the function to be enabled and disabled. (C)	
63		If the product supports IPv6 SLAAC, the product shall have a configurable parameter that allows the "managed address configuration" flag and the "other stateful configuration" flag to always be set and not perform stateless auto-configuration. (C)	
64		If the product supports stateless IP address auto-configuration including those provided for the commercial market, the DAD shall be disabled in accordance with RFC 2462 and RFC 4862. (R)	
65		The system shall support manual assignment of IPv6 addresses. (R)	
66		If the system provides routing functions, the system shall default to using the "managed address configuration" flag and the "other stateful flag" set to TRUE in their router advertisements when stateful auto-configuration is implemented. (C)	

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

ID	Requirement (See note.)		UCR Reference																																																																																																												
67	IPv6 ICMP	The system shall support the ICMPv6 as described in RFC 4443. (R)	5.3.5.4.7																																																																																																												
68		The system shall have a configurable rate limiting parameter for rate limiting the forwarding of ICMP messages. (R)																																																																																																													
69		The system shall support the capability to enable or disable the ability of the system to generate a Destination Unreachable message in response to a packet that cannot be delivered to its destination for reasons other than congestion. (R) Required if LS supports routing functions.																																																																																																													
70		The system 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. (R)																																																																																																													
71		The system shall validate ICMPv6 messages, using the information contained in the payload, prior to acting on them. (R)																																																																																																													
72	IPv6 Routing Functions	If the system supports routing functions, the system shall support the OSPF for IPv6 as described in RFC 5340. (C)	5.3.5.4.8																																																																																																												
73		If the system supports routing functions, the system shall support securing OSPF with Internet Protocol Security (IPSec) as described for other IPSec instances in UCR 2008, Section 5.4. (C)																																																																																																													
74		If the system supports routing functions, the system shall support OSPF for IPv6 as described in RFC 2740, router to router integrity using IP authentication header with HMAC-SHA1-96 with ESP and AH as described in RFC 2404, shall support OSPFv3 IAW RFC 4552. (C)																																																																																																													
75		If the system supports routing functions, the system shall support the Multicast Listener Discovery (MLD) process as described in RFC 2710 and extended in RFC 3810. (C)																																																																																																													
76	Site Requirements	Engineering Requirements: Physical Media for ASLAN and non-ASLAN. (R) (Site requirement)	5.3.1.7.1																																																																																																												
77		Battery Back up two hours for non-ASLAN components and eight hours for ASLAN components. (R) (Site requirement)	5.3.1.7.5																																																																																																												
78		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																																																																																																												
79	IA Security requirements	Port-Based access Control IAW IEEE 802.1x. (R) Conditional for Core	5.3.1.3.2																																																																																																												
80		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																																																																																																												
81		Security (R)	5.3.1.3.8																																																																																																												
82		Must meet IA requirements IAW UCR 2008, Change 2, Section 5.4 for ASLAN and non-ASLAN. (R)	5.3.1.5																																																																																																												
<p>NOTE: All requirements are for core, distribution, and access layer components unless otherwise specified.</p> <p>LEGEND:</p> <table border="0"> <tr> <td>AH</td> <td>Authentication Header</td> <td>HTTP</td> <td>Hypertext Transfer Protocol</td> <td>ms</td> <td>millisecond</td> </tr> <tr> <td>ASLAN</td> <td>Assured Services Local Area Network</td> <td>HTTPS</td> <td>Hyper Text Transfer Protocol, Secure</td> <td>MTU</td> <td>Maximum Transmission Unit</td> </tr> <tr> <td>C</td> <td>Conditional</td> <td>IA</td> <td>Information Assurance</td> <td>OSPF</td> <td>Open Shortest Path First</td> </tr> <tr> <td>C2</td> <td>Command and Control</td> <td>IAW</td> <td>in accordance with</td> <td>OSPFv3</td> <td>Open Shortest Path First Version 3</td> </tr> <tr> <td>C2(R)</td> <td>Command and Control ROUTINE only</td> <td>ICMP</td> <td>Internet Control Message Protocol</td> <td>PHB</td> <td>Per Hop Behavior</td> </tr> <tr> <td>CPU</td> <td>Central Processing Unit</td> <td>ICMPv6</td> <td>Internet Control Message Protocol for IPv6</td> <td>QoS</td> <td>Quality of Service</td> </tr> <tr> <td>DAD</td> <td>Duplicate Address Detection</td> <td>ID</td> <td>Identification</td> <td>R</td> <td>Required</td> </tr> <tr> <td>DHCP</td> <td>Dynamic Host Configuration Protocol</td> <td>IEEE</td> <td>Institute of Electrical and Electronics Engineers</td> <td>RFC</td> <td>Request for Comments</td> </tr> <tr> <td>DHCPv6</td> <td>Dynamic Host Configuration Protocol for IPv6</td> <td>IPV4</td> <td>Internet Protocol version 4</td> <td>SHA</td> <td>Secure Hash Algorithm</td> </tr> <tr> <td>DISR</td> <td>Department of Defense Information Technology Standards Registry</td> <td>IPV6</td> <td>Internet Protocol version 6</td> <td>SLAAC</td> <td>Stateless Auto Address Configuration</td> </tr> <tr> <td>DSCP</td> <td>Differentiated Services Code Point</td> <td>L2</td> <td>Layer 2</td> <td>SNMP</td> <td>Simple Network Management Protocol</td> </tr> <tr> <td>E2E</td> <td>End-to-End</td> <td>L3</td> <td>Layer 3</td> <td>SSH2</td> <td>Secure Shell Version 2</td> </tr> <tr> <td>ESP</td> <td>Encapsulating Security Payload</td> <td>LACP</td> <td>Link Aggregation Control Protocol</td> <td>SUT</td> <td>System Under Test</td> </tr> <tr> <td>Gbps</td> <td>Gigabits per second</td> <td>LAN</td> <td>Local Area Network</td> <td>TCI</td> <td>Tag Control Information</td> </tr> <tr> <td>HMAC</td> <td>Hash-based Message Authentication Code</td> <td>LS</td> <td>LAN Switch</td> <td>UC</td> <td>Unified Capabilities</td> </tr> <tr> <td></td> <td></td> <td>Mbps</td> <td>Megabits per second</td> <td>UCR</td> <td>Unified Capabilities Requirements</td> </tr> <tr> <td></td> <td></td> <td>MPLS</td> <td>Multiprotocol Label Switching</td> <td>VLAN</td> <td>Virtual Local Area Network</td> </tr> <tr> <td></td> <td></td> <td></td> <td></td> <td>VPN</td> <td>Virtual Private Network</td> </tr> </table>				AH	Authentication Header	HTTP	Hypertext Transfer Protocol	ms	millisecond	ASLAN	Assured Services Local Area Network	HTTPS	Hyper Text Transfer Protocol, Secure	MTU	Maximum Transmission Unit	C	Conditional	IA	Information Assurance	OSPF	Open Shortest Path First	C2	Command and Control	IAW	in accordance with	OSPFv3	Open Shortest Path First Version 3	C2(R)	Command and Control ROUTINE only	ICMP	Internet Control Message Protocol	PHB	Per Hop Behavior	CPU	Central Processing Unit	ICMPv6	Internet Control Message Protocol for IPv6	QoS	Quality of Service	DAD	Duplicate Address Detection	ID	Identification	R	Required	DHCP	Dynamic Host Configuration Protocol	IEEE	Institute of Electrical and Electronics Engineers	RFC	Request for Comments	DHCPv6	Dynamic Host Configuration Protocol for IPv6	IPV4	Internet Protocol version 4	SHA	Secure Hash Algorithm	DISR	Department of Defense Information Technology Standards Registry	IPV6	Internet Protocol version 6	SLAAC	Stateless Auto Address Configuration	DSCP	Differentiated Services Code Point	L2	Layer 2	SNMP	Simple Network Management Protocol	E2E	End-to-End	L3	Layer 3	SSH2	Secure Shell Version 2	ESP	Encapsulating Security Payload	LACP	Link Aggregation Control Protocol	SUT	System Under Test	Gbps	Gigabits per second	LAN	Local Area Network	TCI	Tag Control Information	HMAC	Hash-based Message Authentication Code	LS	LAN Switch	UC	Unified Capabilities			Mbps	Megabits per second	UCR	Unified Capabilities Requirements			MPLS	Multiprotocol Label Switching	VLAN	Virtual Local Area Network					VPN	Virtual Private Network
AH	Authentication Header	HTTP	Hypertext Transfer Protocol	ms	millisecond																																																																																																										
ASLAN	Assured Services Local Area Network	HTTPS	Hyper Text Transfer Protocol, Secure	MTU	Maximum Transmission Unit																																																																																																										
C	Conditional	IA	Information Assurance	OSPF	Open Shortest Path First																																																																																																										
C2	Command and Control	IAW	in accordance with	OSPFv3	Open Shortest Path First Version 3																																																																																																										
C2(R)	Command and Control ROUTINE only	ICMP	Internet Control Message Protocol	PHB	Per Hop Behavior																																																																																																										
CPU	Central Processing Unit	ICMPv6	Internet Control Message Protocol for IPv6	QoS	Quality of Service																																																																																																										
DAD	Duplicate Address Detection	ID	Identification	R	Required																																																																																																										
DHCP	Dynamic Host Configuration Protocol	IEEE	Institute of Electrical and Electronics Engineers	RFC	Request for Comments																																																																																																										
DHCPv6	Dynamic Host Configuration Protocol for IPv6	IPV4	Internet Protocol version 4	SHA	Secure Hash Algorithm																																																																																																										
DISR	Department of Defense Information Technology Standards Registry	IPV6	Internet Protocol version 6	SLAAC	Stateless Auto Address Configuration																																																																																																										
DSCP	Differentiated Services Code Point	L2	Layer 2	SNMP	Simple Network Management Protocol																																																																																																										
E2E	End-to-End	L3	Layer 3	SSH2	Secure Shell Version 2																																																																																																										
ESP	Encapsulating Security Payload	LACP	Link Aggregation Control Protocol	SUT	System Under Test																																																																																																										
Gbps	Gigabits per second	LAN	Local Area Network	TCI	Tag Control Information																																																																																																										
HMAC	Hash-based Message Authentication Code	LS	LAN Switch	UC	Unified Capabilities																																																																																																										
		Mbps	Megabits per second	UCR	Unified Capabilities Requirements																																																																																																										
		MPLS	Multiprotocol Label Switching	VLAN	Virtual Local Area Network																																																																																																										
				VPN	Virtual Private Network																																																																																																										

8. TEST NETWORK DESCRIPTION. The SUT was tested at the USAISEC-TIC and JITC, which are DoD Component Test Labs. The SUT was tested in a manner and configuration similar to that 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 with WS-X45-SUP6-E processor is depicted in Figure 2-5. The ASLAN test configuration used to test the SUT in a heterogeneous with WS-X45-SUP6-E processor configurations are depicted in Figures 2-6 and 2-7. The ASLAN test configuration used to test the SUT in a homogeneous network with WS-X45-SUP6L-E processor is depicted in Figure 2-8. The ASLAN test configuration used to test the SUT in a heterogeneous with WS-X45-SUP6-E processor configurations is depicted in Figure 2-9.

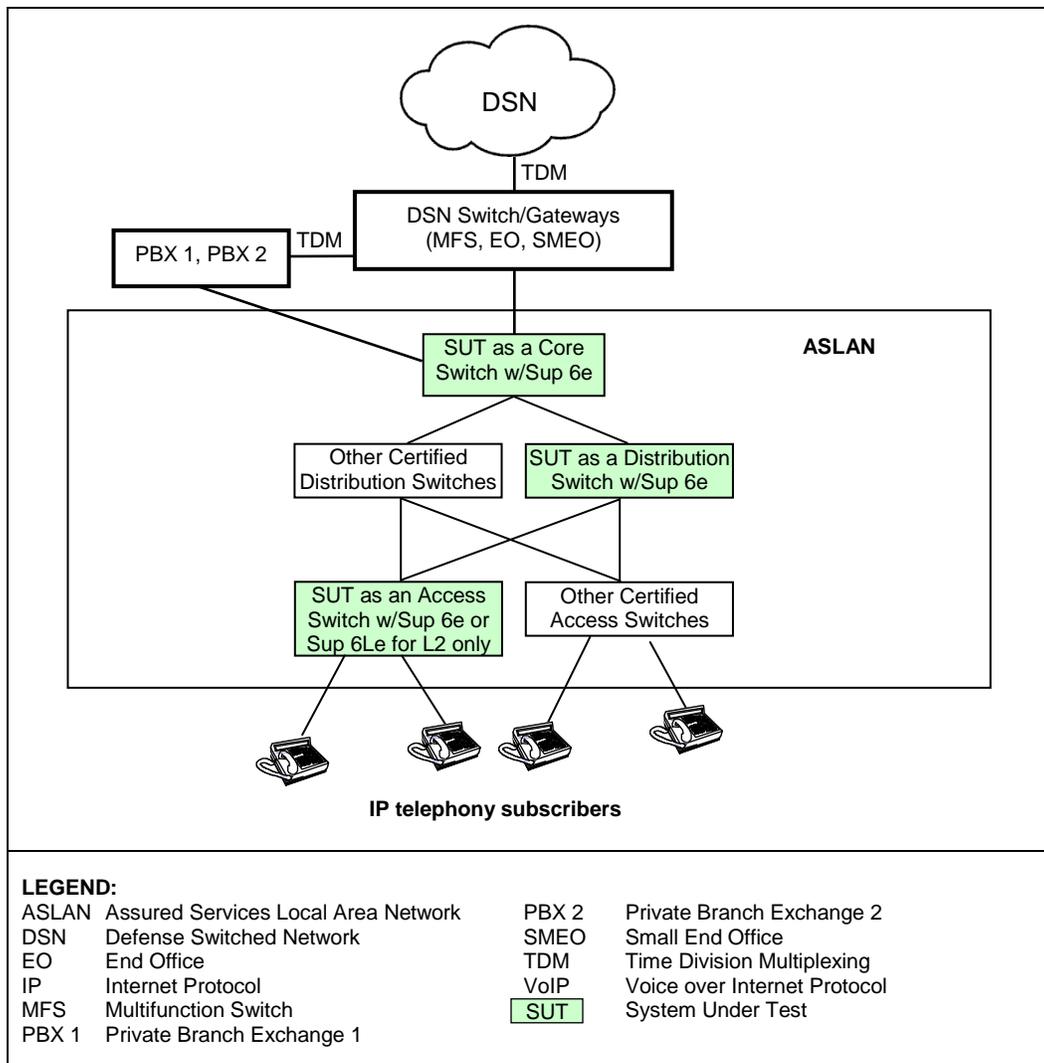


Figure 2-2. SUT Notional ASLAN VoIP Architecture

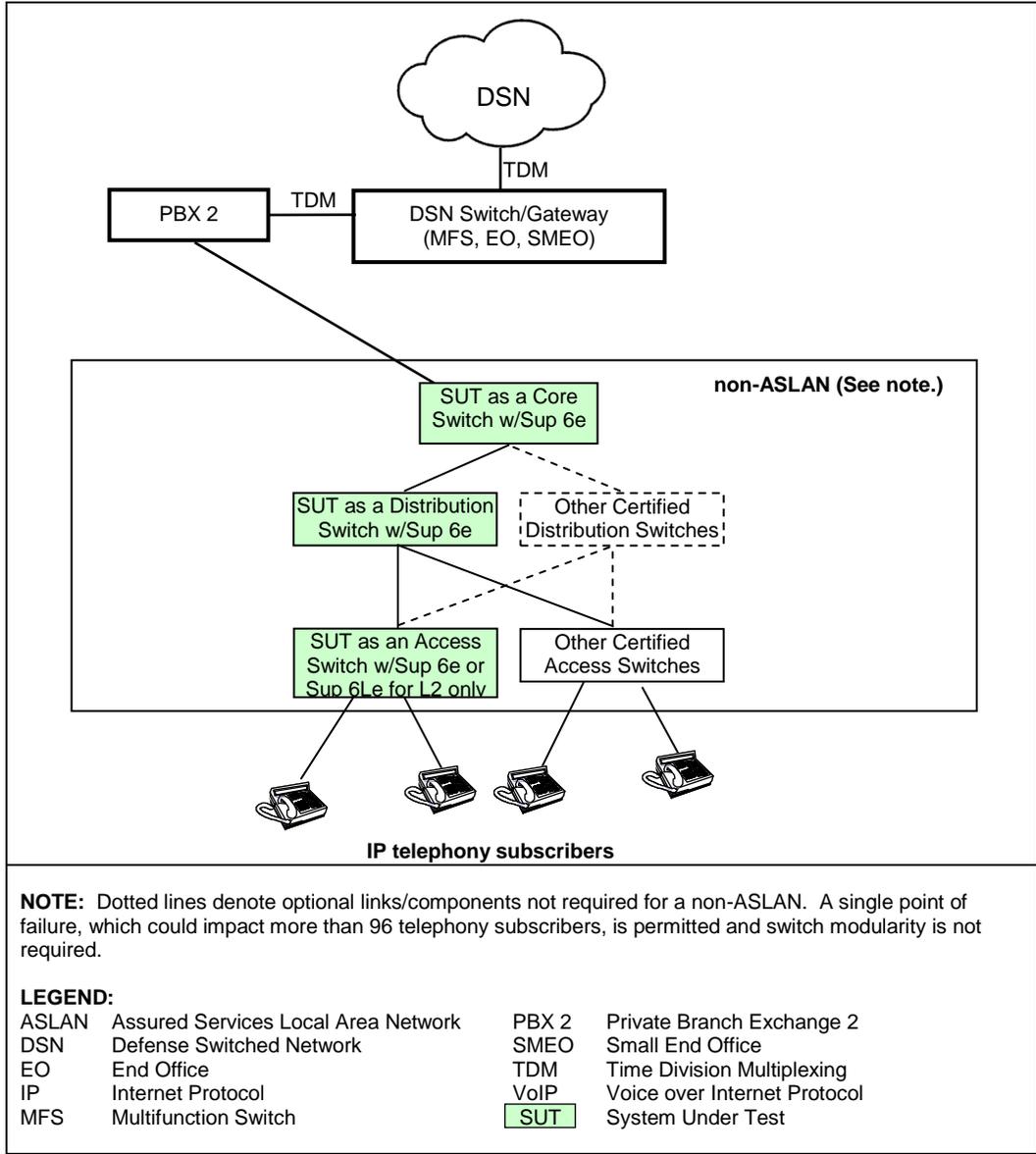


Figure 2-3. SUT Notional Non-ASLAN VoIP Architecture

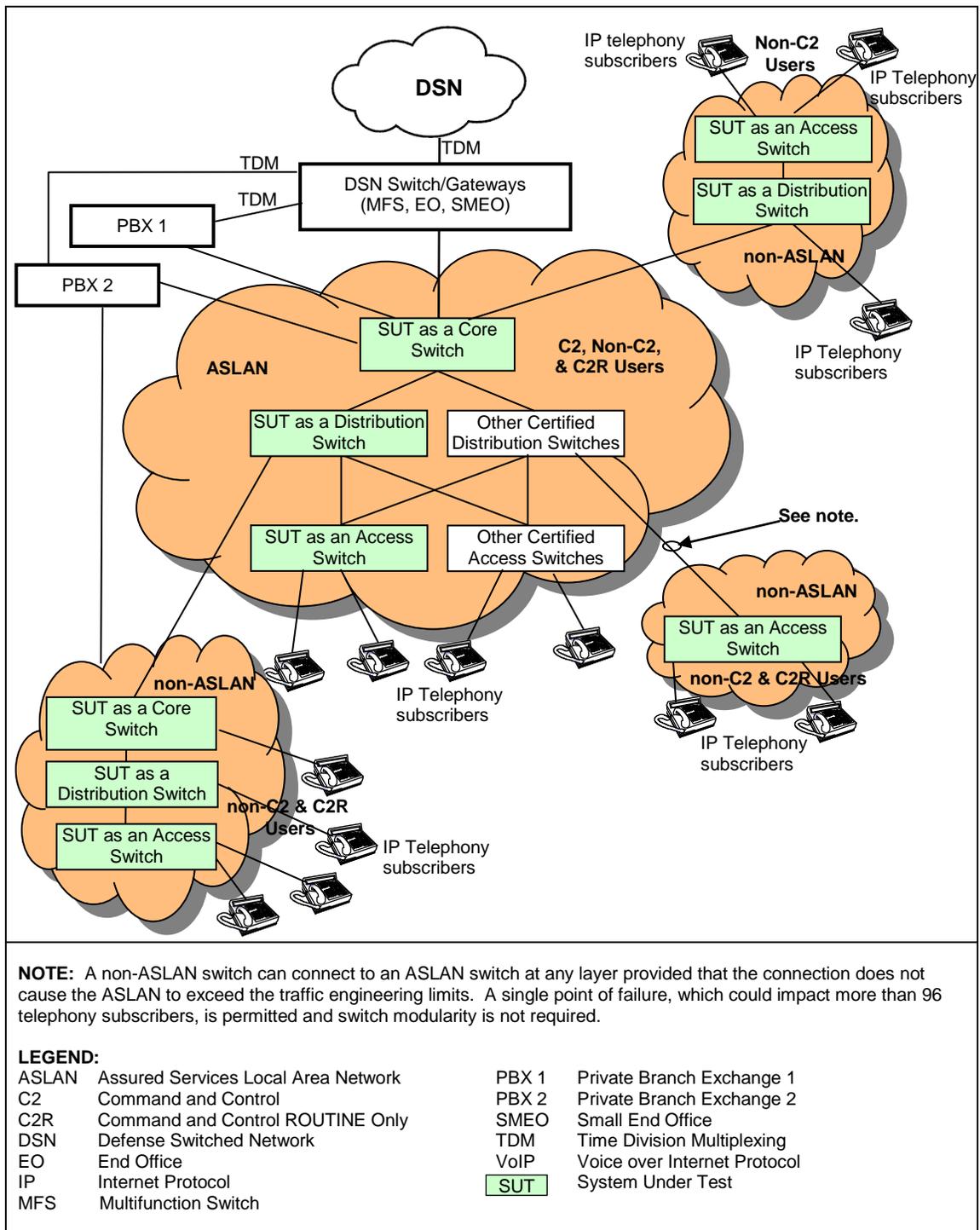


Figure 2-4. SUT Notional ASLAN and non-ASLAN Combined VoIP Architecture

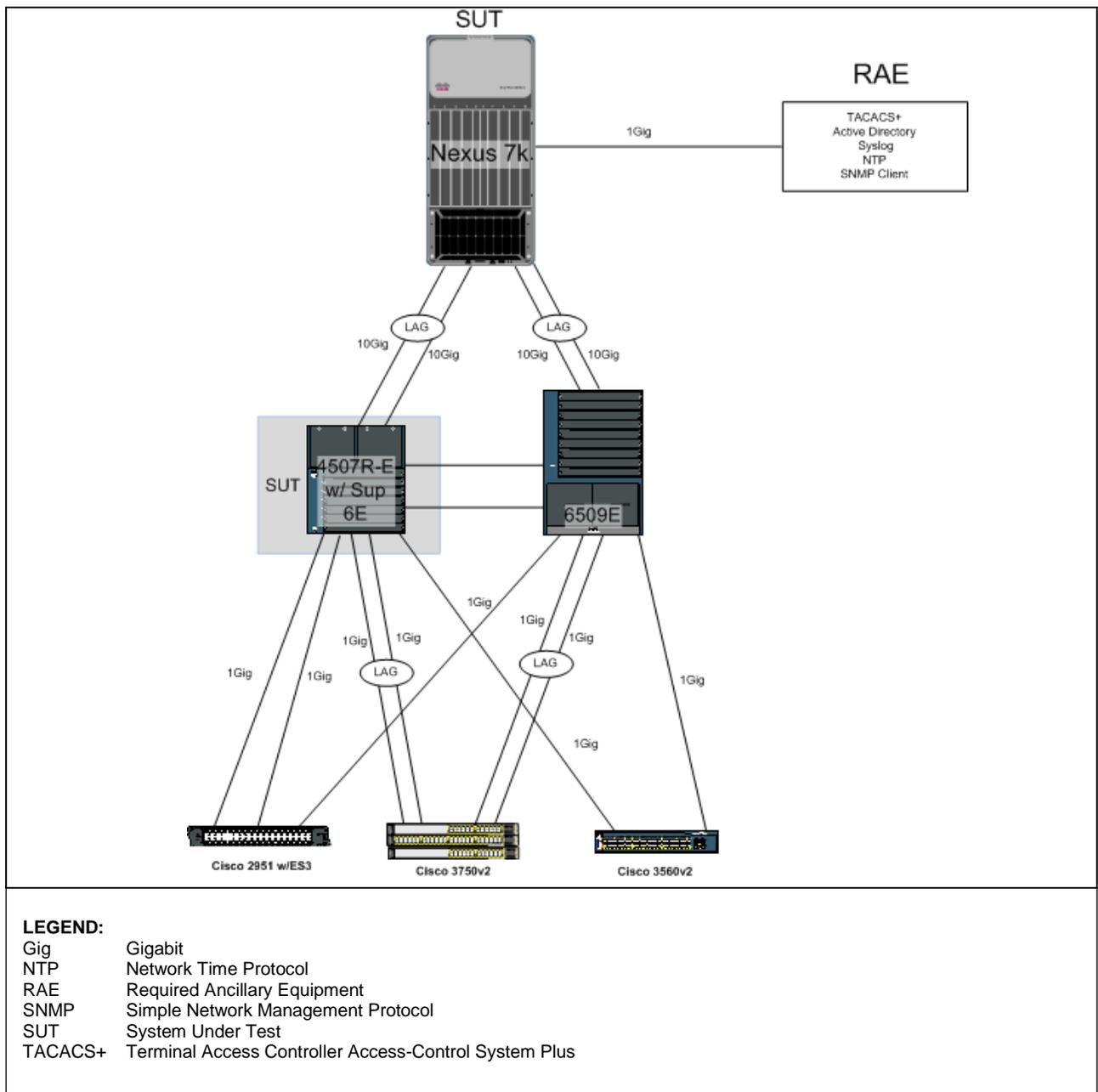
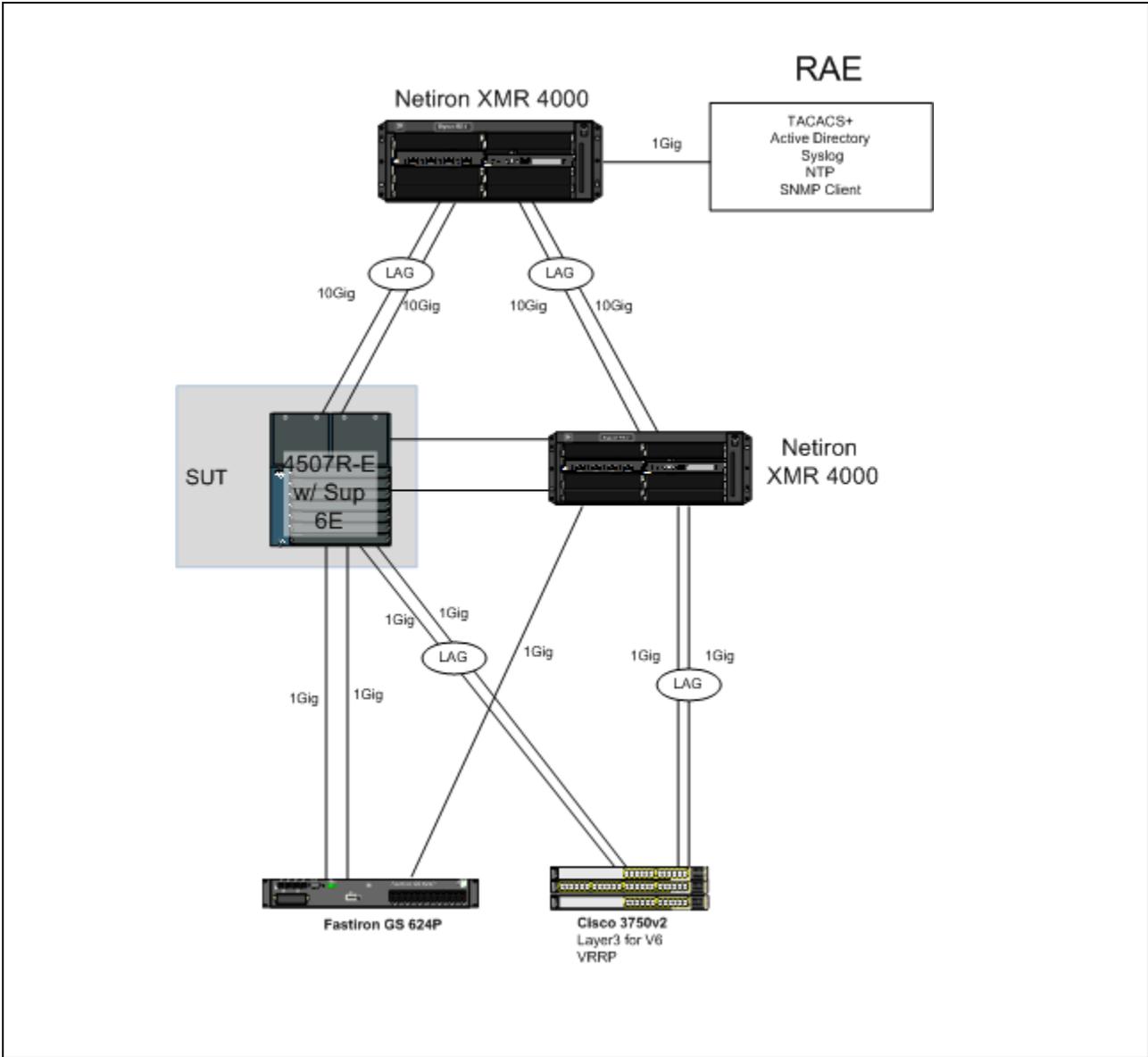


Figure 2-5. SUT with WS-X45-SUP6-E processor Homogenous Test Configuration



- LEGEND:**
- Gig Gigabit
 - 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. SUT with WS-X45-SUP6-E processor Heterogeneous Test Configuration with Brocade

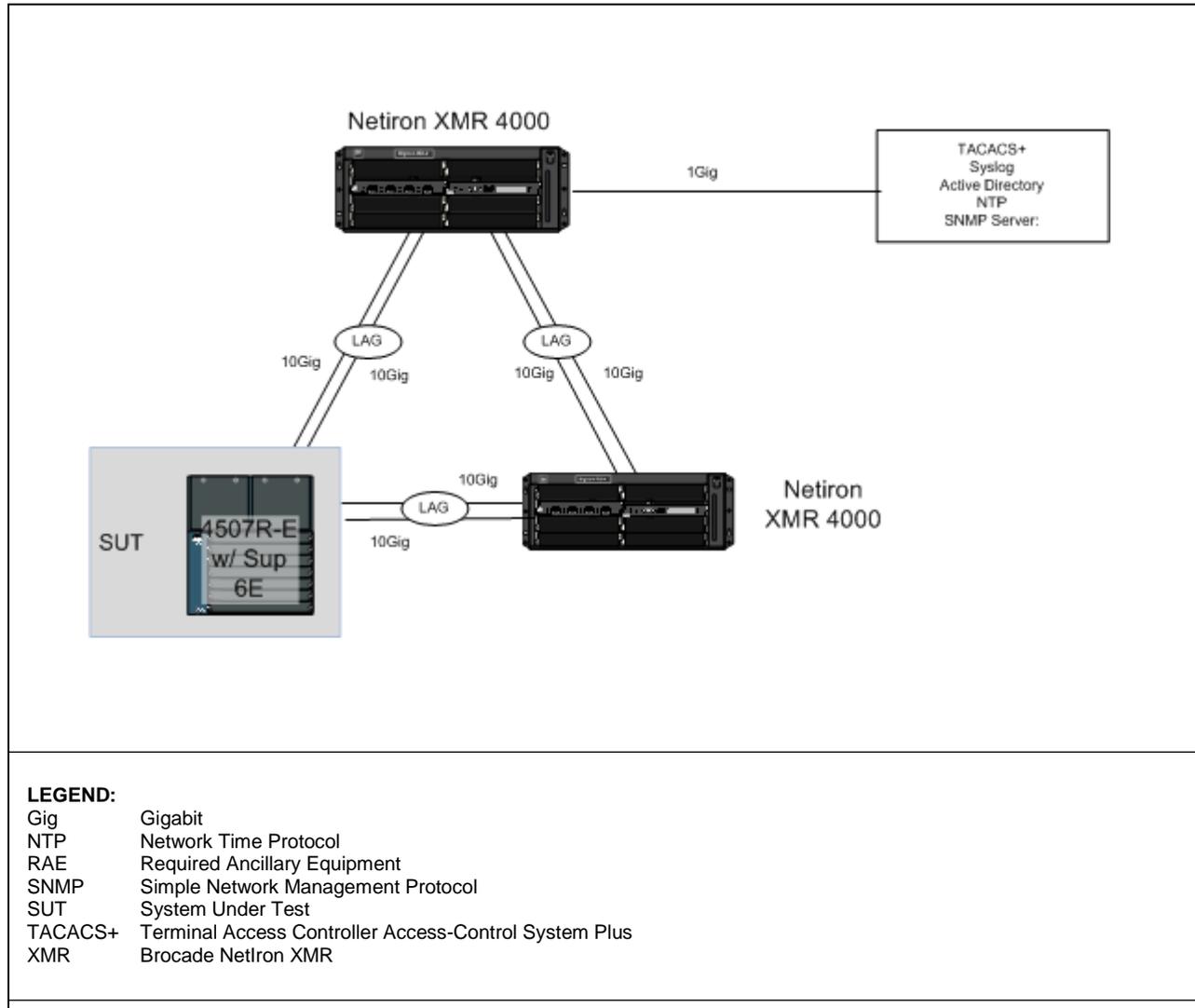
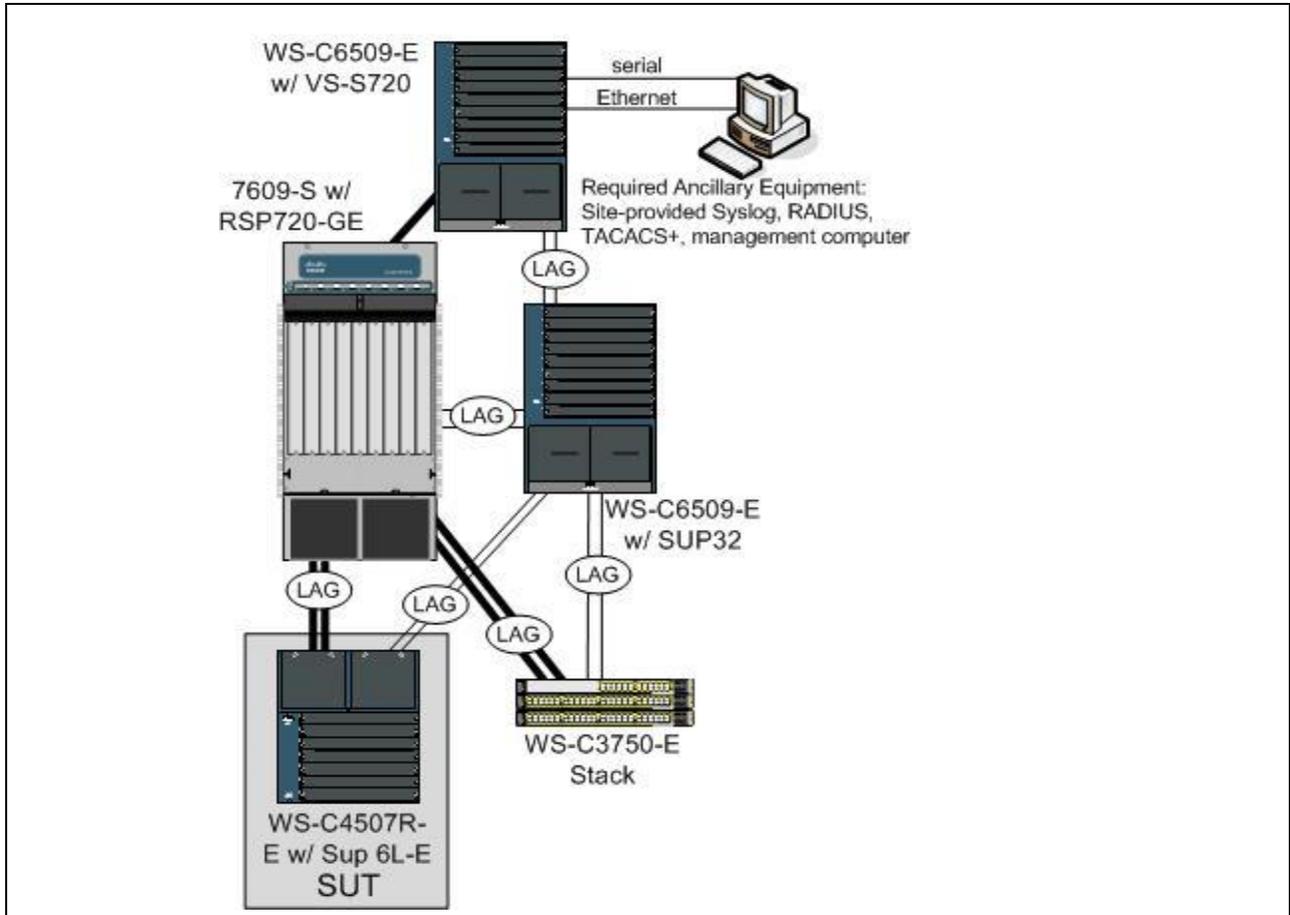
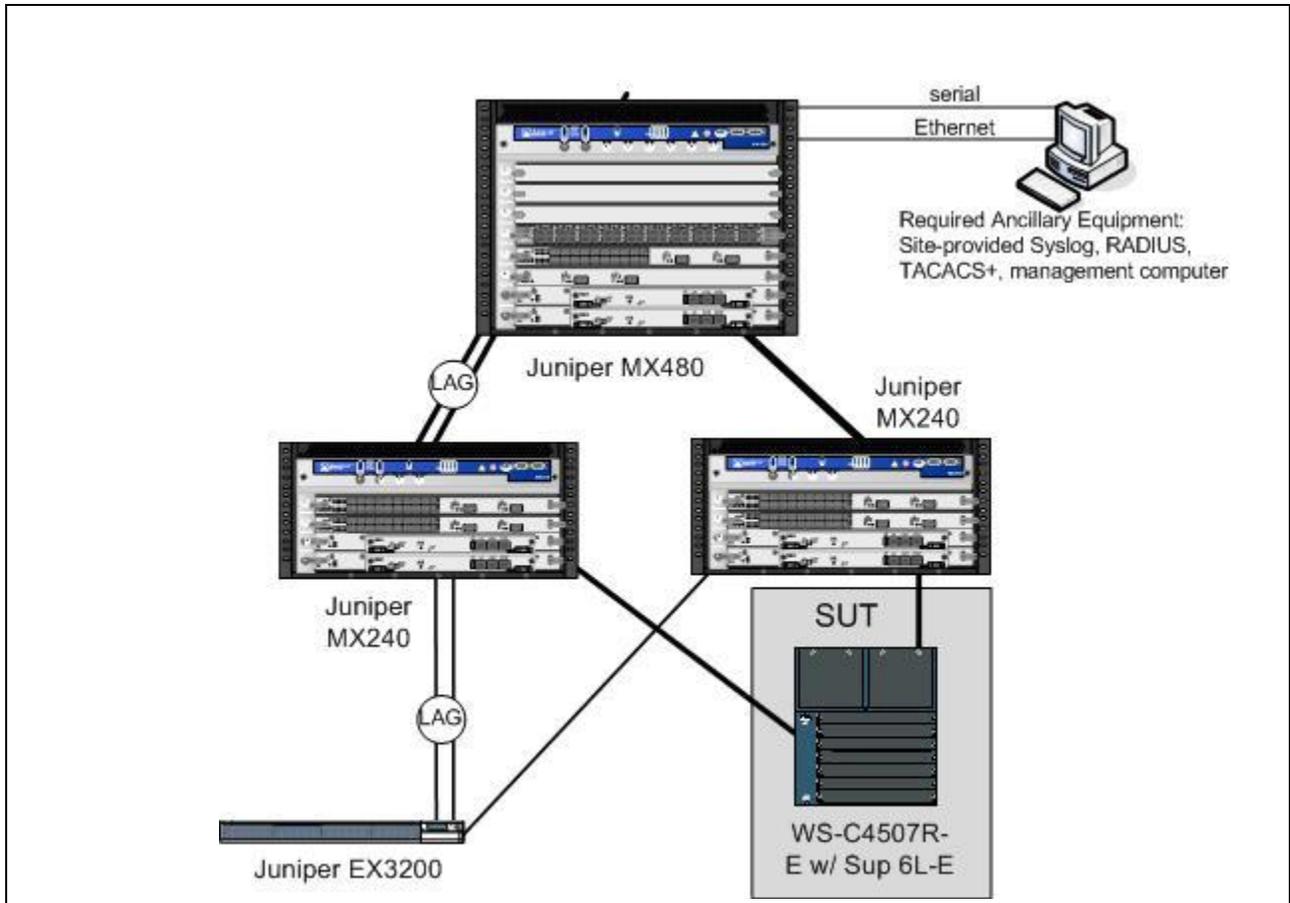


Figure 2-7. SUT with WS-X45-SUP6-E processor Heterogeneous Test Configuration with Brocade



- LEGEND:**
- Gig Gigabit
 - 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 2-8. SUT with WS-X45-SUP6L-E processor Homogenous Test Configuration



- LEGEND:**
- Gig Gigabit
 - 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 2-9. SUT with WS-X45-SUP6-E processor heterogeneous Juniper Test Configuration

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 Nexus 7000		5.0(2a)																		
Cisco Catalyst 6509E		12.2(33)SX14																		
Cisco Catalyst 3750v2		12.2(55)SE																		
Cisco Catalyst 3560v2		12.2(53)SG2																		
Cisco 2951 ISR		15.1(1)T																		
Brocade NetIron XMR-4000		FI 4.0.0f																		
Brocade FastIron GS 624P		FI 4.3.02a																		
SUT (See note.)	Release	Function	Sub-component (See note.)	Description																
Cisco Catalyst 4500E																				
<u>WS-C4507R-E</u> WS-C4510R-E WS-4503-E WS-4506-E	12.2(53) SG3	Core, Distribution, Access	<u>WS-X45-SUP6-E</u>	<u>Catalyst 4500 E-Series Sup 6-E, 2x10GE(X2) w/ Twin Gig</u>																
			<u>WS-X45-Sup6L-E</u>	<u>Catalyst 4500 E-Series Sup 6-E Lite, 2x10GE(X2) w/ Twin Gig</u>																
			<u>WS-X4306-GB</u>	<u>Catalyst 4500 Gigabit Ethernet Module, 6-Ports(GBIC)</u>																
			WS-X4506-GB-T	Catalyst 4500 6-Port 10/100/1000 PoE or SFP																
			<u>WS-X4148-RJ45V</u>	<u>Catalyst 4500 prestandard PoE 10/100, 48-Ports (RJ45)</u>																
			WS-X4148-RJ	Catalyst 4500 10/100 Auto Module, 48-Ports																
			<u>WS-X4248-FE-SFP</u>	<u>Catalyst 4500 48-Port 100BASE-X</u>																
			WS-X4148-FX-MT	Catalyst 4500 FE Switching Module, 48-100FX MMF(MTRJ)																
			<u>WS-X4248-RJ45V</u>	<u>Catalyst 4500 PoE 802.3af 10/100, 48-Ports</u>																
			<u>WS-X4548-RJ45V+</u>	<u>Catalyst 4500 PoE+ Ready 10/100/1000, 48-Port (RJ45)</u>																
			WS-X4548-GB-RJ45V	Catalyst 4500 PoE 802.3af 10/100/1000, 48-Ports (RJ45)																
			WS-X4548-GB-RJ45	Catalyst 4500 Enhanced 48-Port 10/100/1000 Base-T (RJ-45)																
			<u>WS-X4606-X2-E</u>	<u>Catalyst 4500 E-Series 6-Port 10GbE (X2)</u>																
			<u>WS-X4648-RJ45V+E</u>	<u>Catalyst 4500 E-Series 48-Port PoE+ Ready 10/100/1000(RJ45)</u>																
<u>WS-X4624-SFP-E</u>	<u>Catalyst 4500 E-Series 24-Port GE (SFP)</u>																			
<u>WS-X4448-GB-SFP</u>	<u>Catalyst 4500 48-Port 1000Base-X</u>																			
<p>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 them to be functionally identical for interoperability certification purposes and certified for joint use.</p> <p>LEGEND:</p> <table> <tr> <td>ISR</td> <td>Integrated Services Router</td> <td>SUT</td> <td>System Under Test</td> </tr> <tr> <td>JITC</td> <td>Joint Interoperability Test Command</td> <td>USAISEC-TIC</td> <td>U.S. Army Information Systems Engineering Command, Technology Integration Center</td> </tr> <tr> <td>PoE</td> <td>Power over Ethernet</td> <td>XMR</td> <td>Brocade NetIron XMR</td> </tr> <tr> <td>SFP</td> <td>Small Form Factor Pluggable</td> <td></td> <td></td> </tr> </table>					ISR	Integrated Services Router	SUT	System Under Test	JITC	Joint Interoperability Test Command	USAISEC-TIC	U.S. Army Information Systems Engineering Command, Technology Integration Center	PoE	Power over Ethernet	XMR	Brocade NetIron XMR	SFP	Small Form Factor Pluggable		
ISR	Integrated Services Router	SUT	System Under Test																	
JITC	Joint Interoperability Test Command	USAISEC-TIC	U.S. Army Information Systems Engineering Command, Technology Integration Center																	
PoE	Power over Ethernet	XMR	Brocade NetIron XMR																	
SFP	Small Form Factor Pluggable																			

10. TESTING LIMITATIONS. None.

11. TEST RESULTS

a. Test Conduct. The SUT with WS-X45-SUP6-E processor was tested as a Layer 2/3 core, distribution, and access switch in both homogeneous and heterogeneous ASLAN configurations and met all of the requirements with testing and/or the vendor's LoC as outlined in the subparagraphs below. The SUT with the WS-X45-SUP6L-E processor met all requirements as a Layer 2 access switch unless otherwise specified.

(1) The UCR 2008, Change 2, paragraphs 5.3.1.2.1, 5.3.1.7.7, 5.3.1.7.7.1, and 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 product itself provides redundancy internally or a secondary product is added to the ASLAN to provide redundancy to the primary product. Single-product redundancy may be met with a modular chassis that at a minimum provides the following: dual power supplies, dual processors, termination sparing, redundancy protocol, no single point of failure, and switch fabric or backplane redundancy. 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 5 seconds, 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 more than 96 users and was equipped with redundant power supplies and processor units. A standard load of 100 percent of the total bandwidth was used, with 50 percent each of Internet Protocol version 4 (IPv4) and Internet Protocol version 6 (IPv6) traffic. The following test results are for the SUT with the WS-X45-SUP6-E and WS-X45-SUP6L-E processors: Non-Link Aggregation Control Protocol (LACP) link failover was measured between 0.96 and 2.63 seconds. CPU failover was 5.44 seconds for IPv6 traffic, and 4.96 ms for IPv4 traffic. This IPv6 discrepancy was adjudicated by DISA as having a minor operational impact.

(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 IPv4 and IPv6 traffic. The test included 24.9 percent each of best effort data; Operations, Administration, and Maintenance (OA&M); video traffic, 20.9 percent voice; and 2 percent each of network management and voice/video signaling.

(a) The core and distribution products shall be non-blocking for a minimum of 50 percent and access products 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 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 millisecond (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 5-minute period measured from ingress ports to egress ports under congested conditions. The SUT with the WS-X45-SUP6-E processor met this requirement with a measured jitter of .0014 ms for video and .0016 ms for voice. The WS-X45-SUP6L-E processor met this requirement with a measured jitter between .011 and .015 ms.

(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 5-minute period measured from ingress ports to egress ports under congested conditions. The SUT with the WS-X45-SUP6-E processor met this requirement with a measured packet loss of 0.00 percent for all traffic types. The WS-X45-SUP6L-E processor met this requirement with a measured packet loss of 0.00 percent.

(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 5-minute period measured from ingress ports to egress ports under congested conditions. The SUT with the WS-X45-SUP6-E processor met this requirement with a measured latency of 0.043 ms or less for all traffic types using the 10 Gigabit (Gb) interface. The WS-X45-SUP6L-E processor met this requirement with a measured latency between .074 and .096 ms.

(3) The UCR 2008, Change 2, paragraph 5.3.1.3.1, states that, at a minimum, core and distribution products shall provide the following interface rates and other rates may be provided as conditional interfaces: 100 Mbps in accordance with (IAW) IEEE 802.3u and 1 Gbps IAW IEEE 802.3z. At a minimum, access products shall provide one of the following interface rates and other rates may be provided as conditional interfaces: 10 Megabits per second (Mbps) IAW Institute of Electrical and Electronics Engineers (IEEE) 802.3i, 100 Mbps IAW IEEE 802.3u, 1000 Mbps IAW IEEE 802.3ab, and IEEE 802.3z. 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		
	Co	D	A		Co	D	A
Network Management Interfaces for Core, Distribution Layer Switches							
EIA/TIA-232 (Serial)	R	R	R	EIA/TIA-232	Met ²	Met ²	Met
IEEE 802.3i (10BaseT UTP)	C	C	C	7-18, 25-28, 32-36, 44-46, 55-57, 72-75	Not Tested		
IEEE 802.3u (100BaseT UTP)	C	C	C	7-18, 25-28, 32-36, 44-46, 55-57, 72-75	Met ²	Met ²	Met
IEEE 802.3ab (1000BaseT UTP)	C	C	C	7-18, 25-28, 32-36, 44-46, 55-57, 72-75	Met ²	Met ²	Met
Uplink Interfaces for Core, Distribution Layer Switches							
IEEE 802.3u (100BaseT UTP)	R	R	C ³	7-18, 28, 44-46, 55-57, 72-75	Met ²	Met ²	Met
IEEE 802.3u (100BaseFX)	C	C	C ³	10-18, 28, 44-46, 55-57, 72-75	Not Tested.		
IEEE 802.3ab (1000BaseT UTP)	C	C	C ³	7-18, 28, 44-46, 55-57, 72-75	Met ²	Met ²	Met
IEEE 802.3z (1000BaseX Fiber)	R	R	C ³	10-18, 28, 44-46, 55-57, 72-75	Met ²	Met ²	Met
IEEE 802.3ae (10GBaseX)	C	C	C ³	10-18, 28, 44-46, 55-57, 72-75	Met ²	Met ²	Met
Access Interfaces for Core, Distribution, Access Layer Switches							
IEEE 802.3i (10BaseT UTP)	C	C	C ³	7-18, 28, 44-46, 55-57, 72-75	Not Tested		
IEEE 802.3u (100BaseT UTP)	R	R	C ³	7-18, 28, 44-46, 55-57, 72-75	Met ²	Met ²	Met
IEEE 802.3u (100BaseFX)	C	C	C ³	10-18, 28, 44-46, 55-57, 72-75	Not Tested		
IEEE 802.3ab (1000BaseT UTP)	C	C	C ³	7-18, 28, 44-46, 55-57, 72-75	Met ²	Met ²	Met
IEEE 802.3z (1000BaseX Fiber)	R	R	C ³	10-18, 28, 44-46, 55-57, 72-75	Met ²	Met ²	Met
Generic Requirements for all Interfaces							
Generic Requirements not associated with specific interfaces	R	R	R	30-32, 35, 36, 40, 69-71	Met ²	Met ²	Met
DoD IPv6 Profile Requirements	R	R	R	UCR Section 5.3.5.5	Met ²	Met ²	Met
Security	R	R	R	79-82	Met ⁴	Met ⁴	Met ⁴

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 core, distribution, and access layers with the Supervisor 6E processor: **Catalyst 4507R-E**, 4510R-E, 4503-E, and 4506E. The JITC tested the devices that are bolded and underlined. The other devices listed that are not bolded or underlined are in the same family series as the SUT were not tested; however, they utilize the same OS software and similar hardware and JITC analysis determined them to be functionally identical for interoperability certification purposes.
- 2 The SUT met the core, distribution and access switch requirements with the WS-X45-SUP6-E processor which supports Layer 2/3 functions. The SUT only met the Layer 2 access switch requirements when configured with the WS-X45-SUP6L-E processor.
- 3 Access layer switches are required to support only one of the following IEEE interfaces: 802.3i, 802.3j, 802.3u, 802.3ab and 802.3z.
- 4 Security testing is accomplished via DISA-led IA test teams and published in a separate report, Reference (e).

Table 2-3. SUT Interface Status (continued)

LEGEND:	
802.3ab	1000BaseT Gbps Ethernet over twisted pair at 1 Gbps (125 Mbps)
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
802.3z	Gigabit Ethernet Standard
10BaseT	10 Mbps (Baseband Operation, Twisted Pair) Ethernet
100BaseT	100 Mbps (Baseband Operation, Twisted Pair) Ethernet
100BaseFX	100 Mbps Ethernet over fiber
1000BaseFX	1000 Mbps Ethernet over fiber
1000BaseT	1000 Mbps (Baseband Operation, Twisted Pair) Ethernet
10GBaseX	10000 Mbps Ethernet over Category 5 Twisted Pair Copper
A	Access
ASLAN	Assured Services Local Area Network
C	Conditional
Co	Core
CRs	Capability Requirements
D	Distribution
DISA	Defense Information Systems Agency
DoD	Department of Defense
EIA	Electronic Industries Alliance
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
FRs	Functional Requirements
Gbps	Gigabits per second
IA	Information Assurance
ID	Identification
ICMP	Internet Control Message Protocol
IEEE	Institute of Electrical and Electronics Engineers
IPv6	Internet Protocol version 6
JITC	Joint Interoperability Test Command
Mbps	Megabits per second
NA	Not Applicable
OS	Operating System
R	Required
SUT	System Under Test
TIA	Telecommunications Industry Association
UCR	Unified Capabilities Requirements
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, spanning tree protocol, multiple spanning tree, rapid reconfiguration of spanning tree, and port-based access control. The SUT was tested with a series of forced port speeds as well as auto-negotiation. Link failover testing was performed, which confirmed spanning tree convergence. These requirements were all met through the vendor's LoC, with the exception of port-based access control. This capability was confirmed through the SUT configuration file.

(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) IAW Request for Comments (RFC) 2474 as stated in the subparagraphs below:

(a) The ASLAN infrastructure components shall be capable of accepting any packet with a DSCP value between 0 and 63 on an ingress port and assign that packet to a QoS behavior listed in Section 5.3.1.3.6. The SUT prioritized the following traffic for queuing from lowest to highest with distinct IPv4 DSCP values using an IP traffic generator. The IP load included 100 percent of the total aggregate uplink bandwidth, with 50 percent each IPv4 and IPv6 traffic. The test included 24.9 percent each of best effort data, OA&M, 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, it was verified that the SUT is capable of assigning a DSCP value from 0-63 for each type of traffic, which met this requirement.

(b) The ASLAN infrastructure components shall be capable of accepting any packet with a DSCP value from 0-63 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. The SUT prioritized the following traffic for queuing from lowest to highest with distinct IPv6 service class values using an IP traffic generator: The IP load included 100 percent of the total aggregate uplink bandwidth, with 50 percent each IPv4 and IPv6 traffic. The test included 24.9 percent each of best effort data, OA&M, 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 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 IPv6 traffic class values from 0-63 for each type of traffic, which met this requirement.

(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 the Virtual Local Area Network (VLAN) capabilities IAW IEEE 802.1q. The SUT was configured with a preset VLAN Identification (ID) tag using the IP loader. The load was captured at the egress and ingress 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, per the vendor's LoC (non-Ipv6) the SUT has the capability to assign any VLAN ID any value from 1 through 3967, 4048 through 4094. VLANs 3968 through 4047 are the default VLANs reserved for internal use.

(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. The SUT prioritized the following traffic for queuing from lowest to highest with distinct IPv4 DSCP values and IPv6 service class values using an IP traffic generator. The SUT was tested using 100 percent of the total aggregate uplink bandwidth, with 50 percent each IPv4 and IPv6 traffic. The test included 24.9 percent each of best effort data, OA&M,

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. The IPv4 DISR protocol requirements were met by the vendor's LoC for both processors. The subset IPv6 DISR protocol requirements were fully met by the SUT with the WS-X45-SUP6L-E processor as a Layer 2 switch only and partially met by the WS-X45-SUP6-E processor per the vendor's LoC. The vendor stated in their LoC they do not meet RFC4760 Multiprotocol Extensions for BGP-4. This was adjudicated by DISA as having a minor operational impact.

(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 was tested and is certified with a four-queue configuration.

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

(c) Support Differentiated Services (DiffServ) Per Hop Behaviors (PHBs) IAW RFCs 2472, 2597, 2598, 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) IAW RFC 3662, Priority Queuing (PQ) IAW RFC 1046, or Class-Based WFQ IAW RFC 3366. The SUT met this requirement with WFQ.

(e) All queues shall be capable of having bandwidth assigned or percentage of traffic. The SUT prioritized the following traffic for queuing from lowest to highest with distinct IPv4 DSCP values and IPv6 service class values using an IP traffic generator. The SUT was tested using 100 percent of the total aggregate uplink bandwidth, with 50 percent each IPv4 and IPv6 traffic. The test included 24.9 percent each of best effort data, OA&M, 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. The IP traffic generator/measurement tool recorded that the higher prioritized traffic was properly queued by the SUT above lower prioritized best effort traffic at the assigned bandwidth per queue. Subsequently, the IP test equipment was reconfigured to increase the video traffic at 35 percent of line rate to ensure the SUT only allowed 25 percent throughput of the video traffic. The captured video throughput measured by the IP traffic generator/measurement tool was 26.106 percent of the line rate for the SUT with the WS-X45-SUP6-E processor and WS-X45-SUP6L-E processor, and was within the allowable window of 25 percent +/- 10 percent.

(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) IAW RFCs 1157, 2206, 3410, 3411, 3412, 3413, and 3414. The SUT met the requirements for RFCs 1157, 3411, 3412, 3413, and 3414 through the vendor's LoC. RFC 3414 was also met through testing. RFC 2206 is not an SNMP standard. RFC 2206 only defines the Resource Reservation Protocol (RSVP) Management Information Base (MIB). Since RSVP functionality is not supported on the SUT, RFC 2206 is not applicable. RFC 3410 is Informational. From RFC 3410, "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 IAW RFC 1215. The SUT met this requirement through testing. SilverCreek 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) IAW RFC 2819. The SUT met this requirement through the vendor's LoC (non-IPv6).

(d) Coexistence between Version 1, Version 2, and Version 3 of the Internet-standard Network Management Framework IAW RFC 3584. RFC 3584 is not a standard; it is a Best Current Practice. RFC 3584 is not applicable.

(e) Advanced Encryption Standard (AES) Cipher Algorithm in the SNMP User-based Security Model IAW RFC 3826. Security is tested by DISA-led Information Assurance (IA) test teams and 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 IAW Table 5.3.1-5. The SUT met these requirements listed in Table 5.3.1-5 as stipulated throughout this document by testing and/or the vendor's LoC.

(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. E2E performance across a Local Area Network (LAN) is measured from the traffic ingress point to the traffic egress port. The requirements are measured over any 5-minute period under congested conditions. Congested condition is defined as using 100 percent of the total aggregate uplink bandwidth, with 50 percent each IPv4 and IPv6 traffic. The test included 24.9 percent each of best effort data, OA&M, video traffic, 20.9 percent voice, and 2 percent each of network management and voice/video signaling; 100 percent of

link capacities (as defined by baseline traffic engineering (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 5 seconds of detecting the event, excluding transport time.

(a) LANs shall have the ability to perform remote network product configuration/reconfiguration of objects that have existing Department of Defense (DoD) Global Information Grid (GIG) management capabilities. The Network Management System (NMS) shall report configuration change events in NRT, whether or not the change was authorized. The system shall report the success or failure of authorized configuration change attempts in NRT. The SUT met this requirement through testing.

(b) LAN infrastructure components must provide metrics to the NMS to allow them to make decisions on managing the network. The NMSs shall have an automated network management 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 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) LAN components shall be capable of providing status changes 99 percent of the time (with 99.9 percent as an Objective Requirement) by means of an automated capability in NRT. An NMS will have an automated network management 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) LAN components shall be capable of providing SNMP alarm indications to an NMS. The NMSs will have the network management 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 test, and perform diagnostics to isolate faults to a replaceable component. Alarms shall be reported as SNMP traps 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 network management capability of automatically generating and providing an integrated/correlated presentation of 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, and 5.3.1.6, state that ASLAN components must meet security requirements. Security is tested by DISA-led IA test teams and 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, 99.997 percent for C2. The SUT can provide 99.999 percent availability using Software High Availability features (i.e., Open Shortest Path First (OSPF), Virtual Router Redundancy Protocol (VRRP), Rapid Spanning Tree Protocol (RSTP), etc.) and hardware redundancy. The SUT supports redundant processors, power supplies, and interface modules to support > 96 users. Distributed EtherChannels can be utilized to spread uplinks across redundant interface cards. Please note that calculating 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 with the WS-X45-SUP6-E processor is certified for joint use within the Defense Information System Network (DISN) as a core, distribution, and access layer 2/3 switch. The SUT with the WS-X45-SUP6L-E processor is only certified for use as a Layer 2 access switch. It is also certified with any digital switching systems listed 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. 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/tssj>. Due to the sensitivity of the information, the Information Assurance Accreditation Package (IAAP) that contains the approved configuration and deployment guide must be requested directly through government civilian or uniformed military personnel from the Unified Capabilities Certification Office (UCCO), e-mail: ucco@disa.mil.