



## 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

**3 Jun 11**

**SUBJECT:** Special Interoperability Test Certification of the Cisco 2900 Series Integrated Services Router (ISR) Release 15.1(1)T with ES3 Series switch module Release 12.2(52)EX1.

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 2951 ISR with Release 15.1(1)T, and SM-ES3G-24-P switch module with Release 12.2(52)EX1 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 Systems Network (DISN) 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: 1000BaseSX/LX, 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 2911 and 2921 ISR routers employ the same software and similar hardware as the 2951 ISR. The Cisco switch modules SM-ES3-24-P, SM-ES3G-16-P, and SM-ES3-16-P employ the same software and similar hardware as the SM-ES3G-24-P. Up to two switch modules may be inserted into the 2951 ISR chassis service module slots. The JITC analysis determined this system to be functionally identical to the SUT for interoperability certification purposes and certified for joint use.

The SUT is certified to support Defense Switched Network (DSN) Assured Services over Internet Protocol (IP). 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.

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 affect interoperability, but no later than three years from the date of Defense Information Assurance (IA)/Security Accreditation Working Group (DSAWG) accreditation.

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 DSAWG accreditation. Interoperability testing was conducted by the USAISEC-TIC, Fort Huachuca, Arizona, from 21 June through 25 October 2010. Review of the vendor's LoC was completed on 22 June 2010. DISA adjudication of outstanding TDRs was completed on 18 February 2011. The FSO provided a positive CA Recommendation on 22 April 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
	Access		Access
<b>Network Management Interfaces for Layer 3 Access Switches</b>			
EIA/TIA (Serial) 232	R	EIA/TIA-232	Met
IEEE 802.3i (10BaseT UTP)	C	1, 6-15, 18-28, 31, 32-36, 48-53, 58-60, 65, 67-71	Not Tested
IEEE 802.3u (100BaseT UTP)	C	1, 6-15, 18-28, 31, 32-36, 48-53, 58-60, 65, 67-71	Met
IEEE 802.3ab (1000BaseT UTP)	C	1, 6-15, 18-28, 31, 32-36, 48-53, 58-60, 65, 67-71	Met
<b>Uplink Interfaces for Layer 3 Access Switches</b>			
IEEE 802.3u (100BaseT UTP)	C	1-15, 16, 18-24, 28-31, 40, 44-53, 55-60, 65-75	Met
IEEE 802.3u (100BaseFX)	C	1-6, 11, 16, 18-24, 28-31, 40-41, 44-53, 55-60, 65-75	Not Supported <sup>2</sup>
IEEE 802.3ab (1000BaseT UTP)	C	1-16, 18-24, 28-31, 40, 44-53, 55-60, 65-75	Met
IEEE 802.3z (1000BaseX Fiber)	C	1-5, 8-16, 18-24, 28-31, 40, 44-53, 55-60, 65-75	Met
IEEE 802.3ae (10GBaseX)	C	1-5, 8-16, 18, 19, 40-41, 44-53, 55-60, 65-75	Not Supported <sup>2</sup>
<b>Access Interfaces for Layer 3 Access Switches</b>			
IEEE 802.3i (10BASET UTP)	C	1-15, 18-24, 28-41, 44-54, 58-71	Not Tested
IEEE 802.3u (100BaseT UTP)	C	1-15, 18-24, 28-41, 44-54, 58-71	Met
IEEE 802.3u (100BaseFX)	C	1-6, 11, 18-24, 28-31, 44-54, 58-71	Not Supported <sup>2</sup>
IEEE 802.3ab (1000BaseT UTP)	C	1-15, 18-24, 28-41, 44-54, 58-71	Met
IEEE 802.3z (1000BaseX Fiber)	C	1-6, 11, 18-24, 28-31, 44-54, 58-71	Met
<b>Generic Requirements for all Interfaces</b>			
Generic Requirements not associated with specific interfaces	R	30-32, 35, 36, 40, 69-71	Met
DoD IPv6 Profile Requirements	R	UCR 2008, Section 5.3.5.5	Met
Security	R	UCR 2008, Sections 5.3.1.3.8, 5.3.1.5, 5.3.1.6, and 5.4	Met <sup>3</sup>

**Table 1. SUT Interface Status (continued)**

<b>NOTES:</b>			
<p>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 modules, all used in conjunction with the Cisco 2900 series router chassis, which are certified in the ASLAN Access layer: <b>SM-ES3G-24-P 24 port</b>, Switch SM-ES3-24-P 24 port, Switch SM-ES3G-16-P 16-Port, and Switch SM-ES3-16-P 16 port. 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 hardware and JITC analysis determined them to be functionally identical for interoperability certification purposes.</p> <p>2 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.</p> <p>3 Security testing is accomplished via DISA-led IA test teams and published in a separate report, Reference (e).</p>			
<b>LEGEND:</b>			
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	FRs	Functional Requirements
802.3i	10BaseT Mbps over twisted pair	Gbps	Gigabits per second
802.3u	Standard for carrier sense multiple access with collision detection at 100 Mbps	IA	Information Assurance
802.3z	Gigabit Ethernet Standard	ICMP	Internet Control Message Protocol
10BaseT	10 Mbps (Baseband Operation, Twisted Pair) Ethernet	ID	Identification
100BaseT	100 Mbps (Baseband Operation, Twisted Pair) Ethernet	IEEE	Institute of Electrical and Electronics Engineers
100BaseFX	100 Mbps Ethernet over fiber	IPv6	Internet Protocol version 6
1000BaseFX	1000 Mbps Ethernet over fiber	JITC	Joint Interoperability Test Command
1000BaseT	1000 Mbps (Baseband Operation, Twisted Pair) Ethernet	Mbps	Megabits per second
10GBaseX	10000 Mbps Ethernet over Category 5 Twisted Pair Copper	NA	Not Applicable
ASLAN	Assured Services Local Area Network	OS	Operating System
C	Conditional	R	Required
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 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, 10 ms for video, and preferred data and best effort data NA for all ASLAN components. (R)	5.3.1.3
4	Maximum of 0.015% packet loss for Voice, .05 % for video and preferred data for all ASLAN components (R)	5.3.1.3
5	Maximum of 2 ms latency for voice, 10 ms for video, 15 ms for preferred data and best effort data NA for all ASLAN components. (R)	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 only 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)	
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) 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

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

ID	Requirement (See note.)	UCR Reference
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)
21		Must be able to assign VLAN tagged packets to a queue. (R)
22		Support DSCP PHBs per RFCs 2474, 2494, 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)
26		SNMP traps IAW RFC 1215. (R)
27		Remote monitoring IAW RFC 1281 and Advanced Encryption Standard (AES) Cipher Algorithm in the SNMP User-based Security Model IAW RFC 3826. (R)
28	Product Requirements Summary IAW UCR2008 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)
		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 congestion. (R)
30	E2E Performance (Video)	No more than 30 ms Latency over any 5-minute period measured under 100%congestion. (R)
		No more than 30 ms Jitter over any 5-minute period measured under 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 congestion (R)
		Packet loss not to exceed engineered (queuing) parameters over any 5-minute period under congestion. (R)
32	LAN Network Management	Configuration Control for ASLAN and non-ASLAN. (R)
33		Operational Controls for ASLAN and non-ASLAN. (R)
34		Performance Monitoring for ASLAN and non-ASLAN. (R)
35		Alarms for ASLAN and non-ASLAN. (R)
36		Reporting for ASLAN and non-ASLAN. (R)
37	Redundancy	Redundant Power Supplies. (Required on standalone redundant products.)
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)
45		MPLS Conforms to RFCs in Table 5.3.1-14. (C)
46		MPLS Support L2 and L3 VPNs. (C)
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)
49		Support IPv6 packets over Ethernet IAW RFC 2464. (R)
50		Support MTU discovery IAW RFC 1981 if routing functions are supported. (R)
51		Support a minimum MTU of 1280 IAW RFCs 2460 and 5095. (C)
52		Shall support IPv6 addresses IAW RFC 4291. (R)
53		Shall support IPv6 scoped addresses IAW RFC 4007. (R)
54		if routing functions are supported: If DHCP is supported must be IAW RFC 3315, if DHCPv6 is supported it shall be IAW RFC 3313. (C)
55		IPv6 Router Advertisements
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)	

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

ID	Requirement (See note.)		UCR Reference
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)		
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 Backup 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 and 802.3x (R)	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, 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)**

<b>LEGEND:</b>					
AH	Authentication Header	HTTP	Hyper Text 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	IP	Internet Protocol	SLAAC	Stateless Auto Address Configuration
DISR	Department of Defense Information Technology Standards Registry	IPv4	Internet Protocol version 4	SNMP	Simple Network Management Protocol
DSCP	Differentiated Services Code Point	IPv6	Internet Protocol version 6	SSH2	Secure Shell Version 2
E2E	End-to-End	LACP	Link Aggregation Control Protocol	SUT	System Under Test
ESP	Encapsulating Security Payload	LAN	Local Area Network	TCI	Tag Control Information
Gbps	Gigabits per second	LS	LAN Switch	UC	Unified Capabilities
HMAC	Hash-based Message Authentication Code	Mbps	Megabits per second	UCR	Unified Capabilities Requirements
		MPLS	Multiprotocol Label Switching	VLAN	Virtual Local Area Network
		NA	Not Applicable	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](mailto: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](mailto: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 1002812.

FOR THE COMMANDER:

2 Enclosures a/s

  
 for BRADLEY A. CLARK  
 Chief  
 Battlespace Communications Portfolio

JITC Memo, JTE, Special Interoperability Test Certification of the Cisco 2900 Series ISR Release 15.0(1)M w/ES3 series switch module Release 12.2(52)EX1

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 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 Cisco 2951 and SM-ES3G-24-P switch module (Tracking Number 1002812)," 22 April 2011

## CERTIFICATION TESTING SUMMARY

**1. SYSTEM TITLE.** Cisco 2900 Series Integrated Services Router (ISR) Release 15.1(1)T and ES3 Series switch module Release 12.2(52)EX1; hereinafter referred to as the System Under Test (SUT).

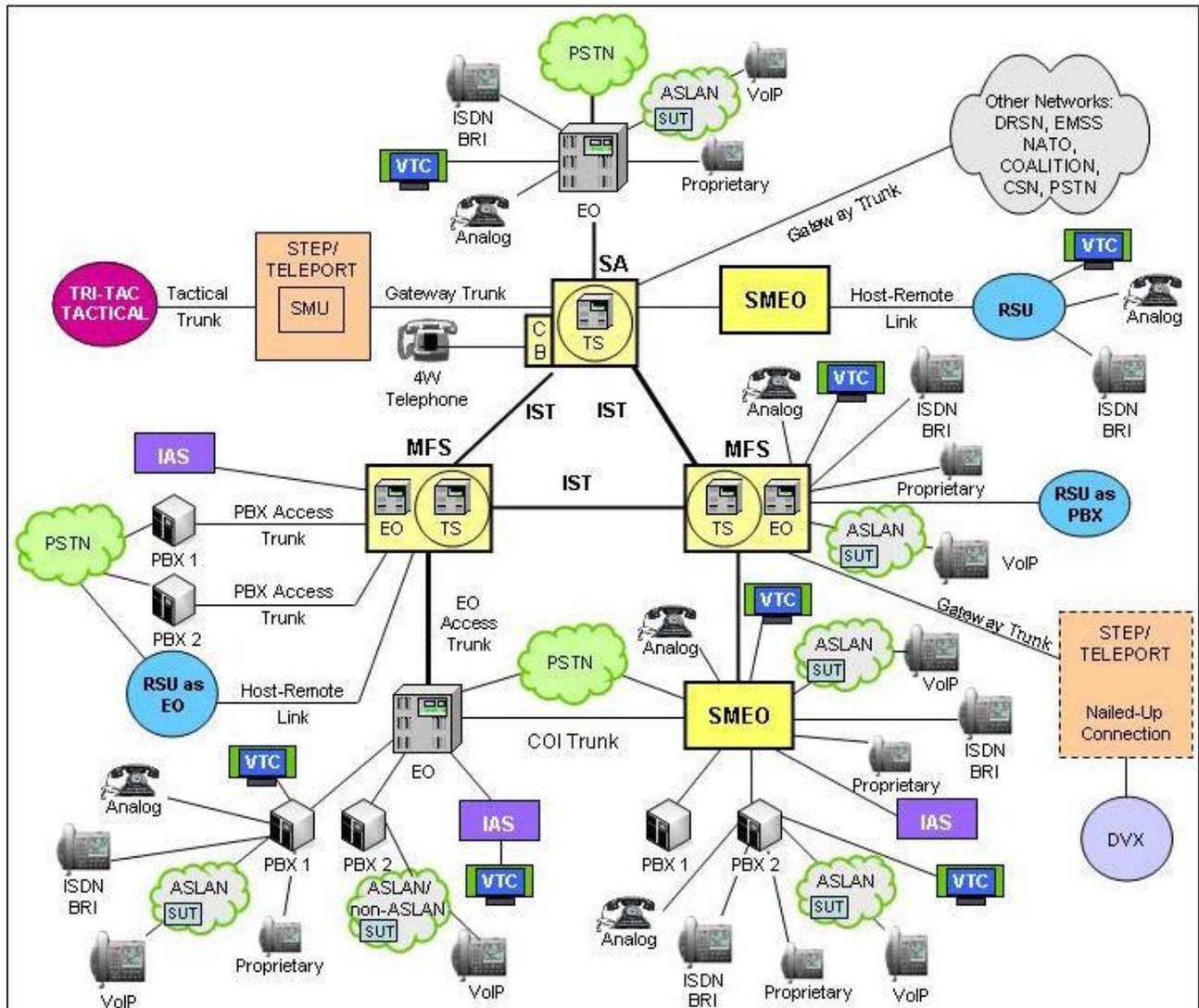
**2. PROPONENT.** Headquarters, U.S. Army Information Systems Engineering Command (HQ USAISEC).

**3. PROGRAM MANAGER.** Mr. Jordan Silk, ELIE-ISE-TI, Building 53302 Arizona Street, Fort Huachuca, 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, AZ.

**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 is certified as a Layer 2 access switch and 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 Base SX/LX and 10/100/1000 BaseT. The Cisco 2951 ISR was the router that was tested, however the 2911 and 2921 ISR models employ the same software and similar hardware as the 2951 ISR. The SM-ES3G-24-P switch module was tested; however, the Cisco SM-ES3-24-P, SM-ES3G-16-P, and SM-ES3-16-P switch modules employ the same software and similar hardware as the SM-ES3G-24-P. Up to two switch modules may be inserted into the 2951 ISR chassis service module slots. The Joint Interoperability Test Command (JITC) analysis determined this system to be functionally identical to the SUT for interoperability certification purposes and certified for joint use.

**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, 10 ms for video, and preferred data and best effort data NA for all ASLAN components. (R)		5.3.1.3
4	Maximum of 0.015% packet loss for Voice, .05 % for video and preferred data for all ASLAN components (R)		5.3.1.3
5	Maximum of 2 ms latency for voice, 10 ms for video, 15 ms for preferred data and best effort data NA for all ASLAN components. (R)		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 only 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) 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, 2494, 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 RFC 1215. (R)	
27		Remote monitoring IAW RFC 1281 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, 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 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 congestion. (R)	
		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
31	E2E Performance (Data)	No more than 45 ms Latency over any 5-minute period measured under congestion (R) Packet loss not to exceed engineered (queuing) parameters over any 5-minute period under congestion. (R)	5.3.1.4.3
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
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 RFC 2464. (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 RFC 4291. (R)	5.3.5.4.3
53		Shall support IPv6 scoped addresses IAW RFC 4007. (R)	5.3.5.4.3
54		If routing functions are supported: If DHCP is supported must be IAW RFC 3315, 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).
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)**

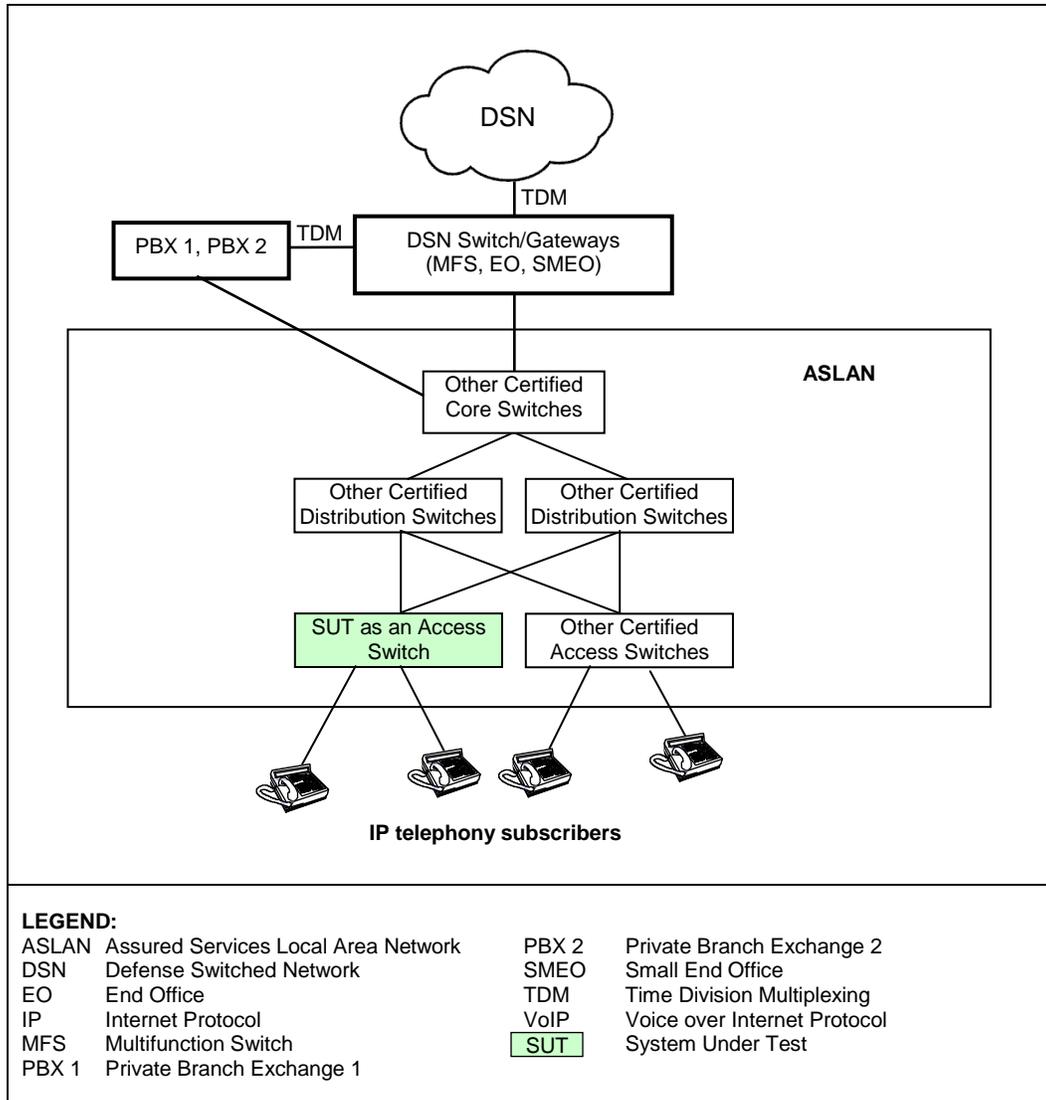
ID	Requirement (See note.)	UCR Reference
67	The system shall support the ICMPv6 as described in RFC 4443. (R)	5.3.5.4.7
68	The system shall have a configurable rate limiting parameter for rate limiting the forwarding of ICMP messages. (R)	
69	The system shall support the capability to enable or disable 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	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	Engineering Requirements: Physical Media for ASLAN and non-ASLAN. (R) (Site requirement)	5.3.1.7.1
77	Battery Backup 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	Port-Based access Control IAW IEEE 802.1x and 802.3x (R)	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, 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.

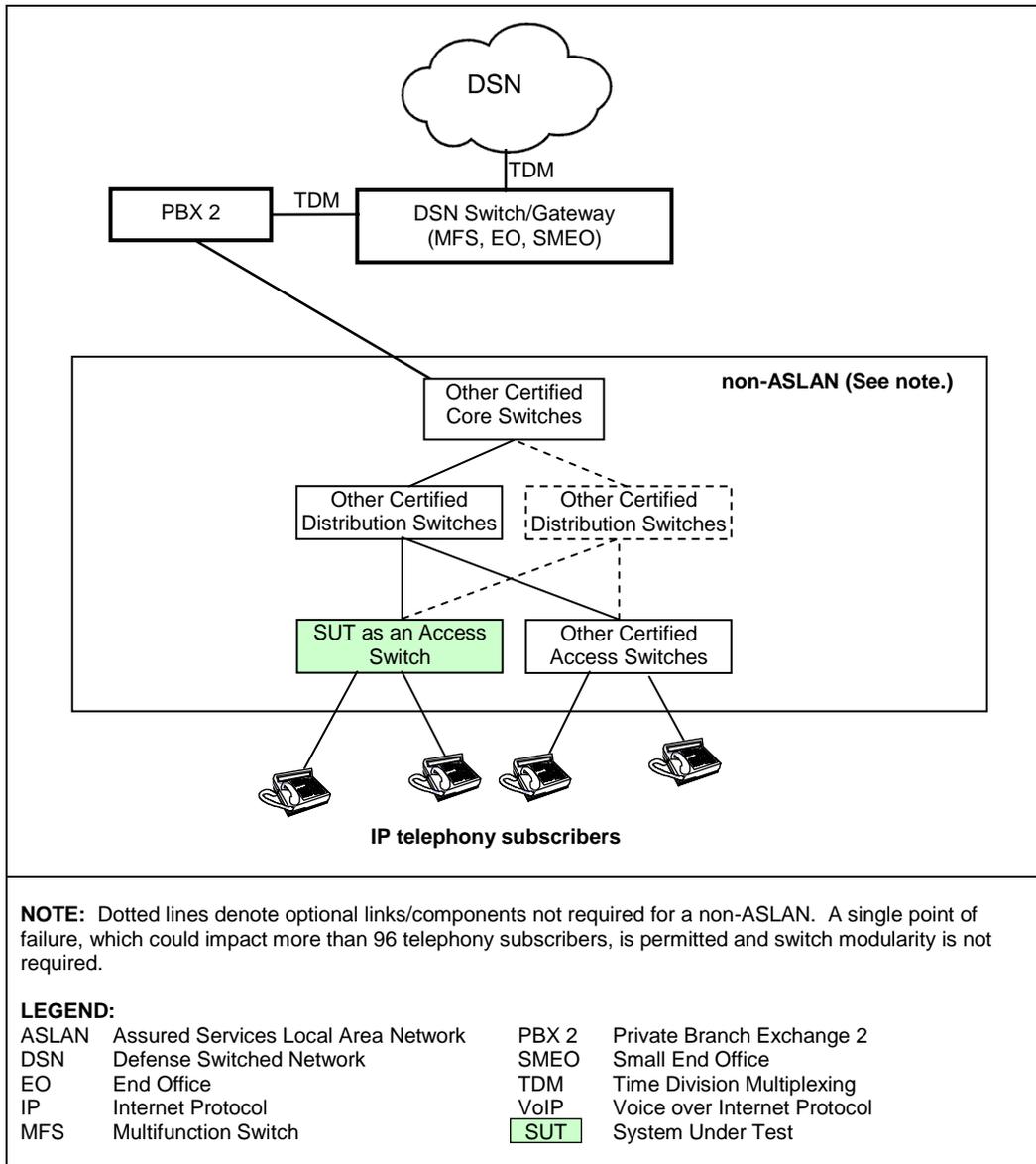
**LEGEND:**

AH	Authentication Header	HMAC	Hash-based Message Authentication Code	MPLS	Multiprotocol Label Switching
ASLAN	Assured Services Local Area Network	HTTP	Hyper Text Transfer Protocol	ms	millisecond
C	Conditional	HTTPS	Hyper Text Transfer Protocol, Secure	MTU	Maximum Transmission Unit
C2	Command and Control	IA	Information Assurance	NA	Not Applicable
C2(R)	Command and Control ROUTINE only	IAW	In Accordance With	OSPF	Open Shortest Path First
CPU	Central Processing Unit	ICMP	Internet Control Message Protocol	OSPFv3	Open Shortest Path First Version 3
DAD	Duplicate Address Detection	ICMPv6	Internet Control Message Protocol for IPv6	PHB	Per Hop Behavior
DHCP	Dynamic Host Configuration Protocol	ID	Identification	QoS	Quality of Service
DHCPv6	Dynamic Host Configuration Protocol for IPv6	IEEE	Institute of Electrical and Electronics Engineers	R	Required
DISR	Department of Defense Information Technology Standards Registry	IP	Internet Protocol	RFC	Request for Comments
DSCP	Differentiated Services Code Point	IPv4	Internet Protocol version 4	SLAAC	Stateless Auto Address Configuration
E2E	End-to-End	IPv6	Internet Protocol version 6	SNMP	Simple Network Management Protocol
ESP	Encapsulating Security Payload	LACP	Link Aggregation Control Protocol	SSH2	Secure Shell Version 2
Gbps	Gigabits per second	LAN	Local Area Network	SUT	System Under Test
		LS	LAN Switch	TCI	Tag Control Information
		Mbps	Megabits per second	UC	Unified Capabilities
				UCR	Unified Capabilities Requirements
				VLAN	Virtual Local Area Network
				VPN	Virtual Private Network

**8. TEST NETWORK DESCRIPTION.** The SUT was tested at the USAISEC-TIC, a DoD Component Test Lab 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 is depicted in Figure 2-5, and the heterogeneous test network configuration is depicted in Figure 2-6.



**Figure 2-2. SUT Notional ASLAN VoIP Architecture**



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

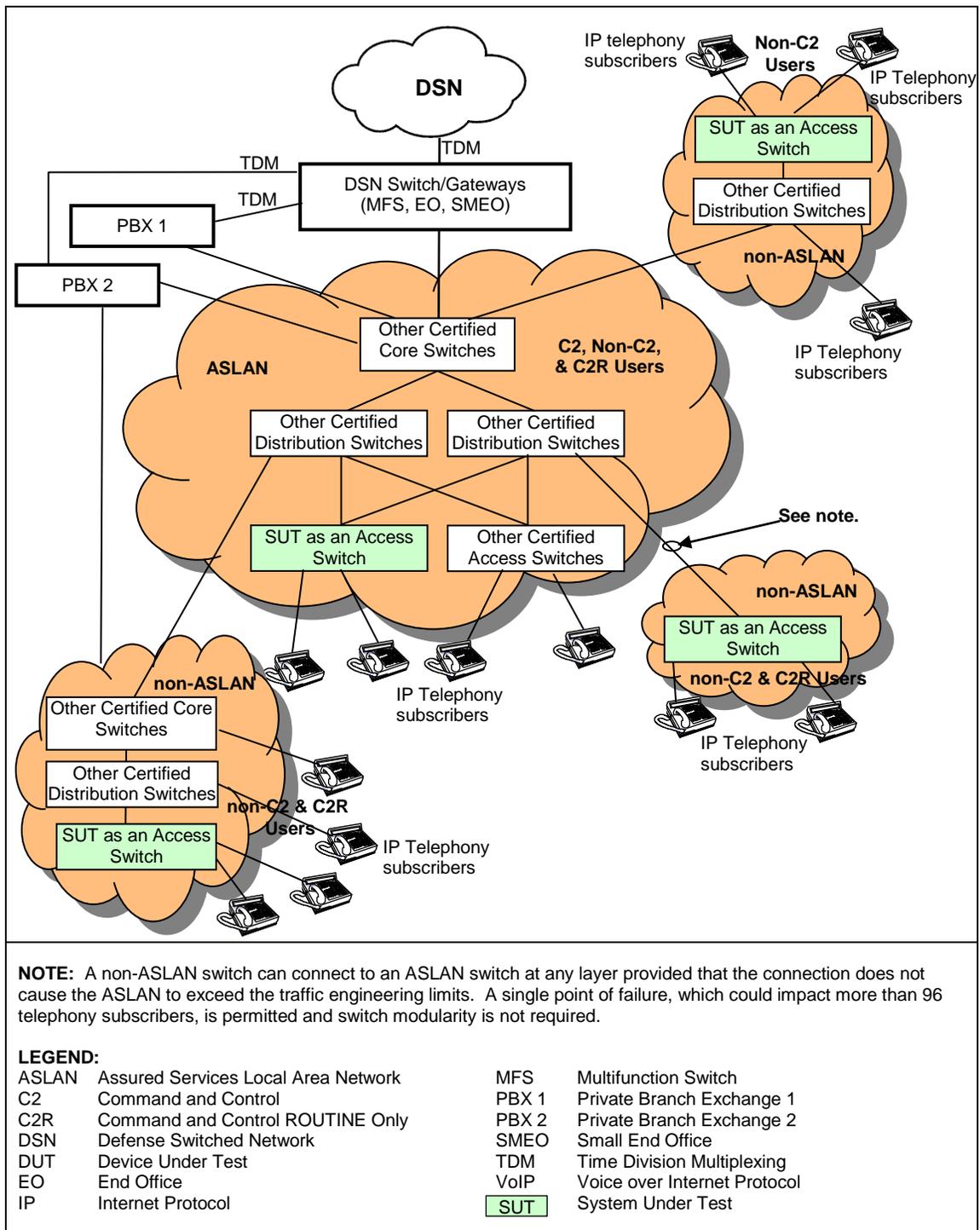
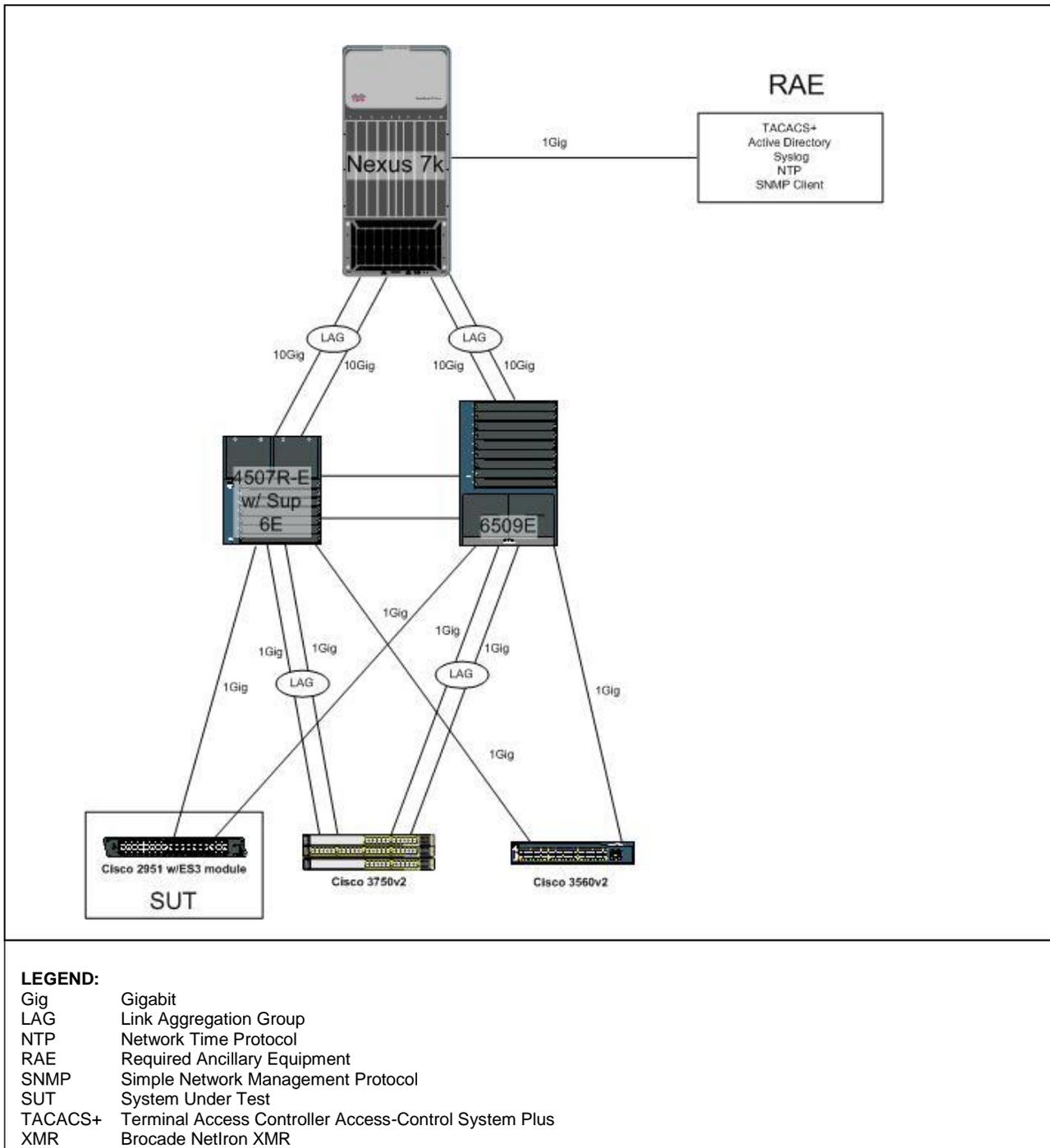
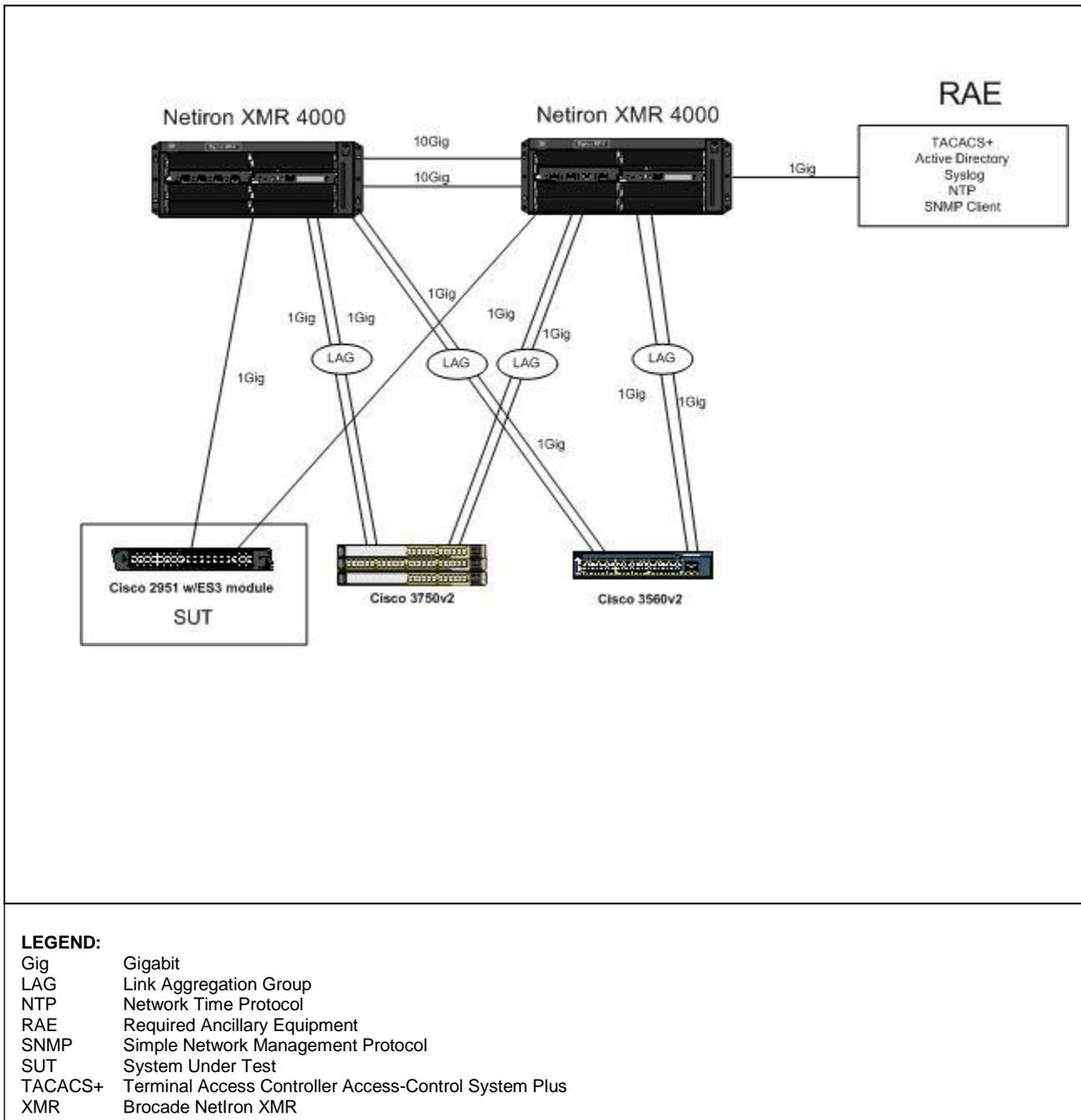


Figure 2-4. SUT Notional ASLAN and non-ASLAN Combined VoIP Architecture



**Figure 2-5. SUT Homogeneous Test Configuration**



**Figure 2-6. Heterogeneous Test Configuration with Brocade**

**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 4507R-E		12.2(53)SG3														
Cisco Catalyst 3750v2		12.2(55)SE														
Cisco Catalyst 3560v2		12.2(53)SE2														
Brocade Netron XMR 4000		FI 4.0.0f														
SUT (See note.)	Release	Function	Sub-component (See note.)	Description												
<b>Cisco 2900 ISR w/ ES3</b>																
<u>2951</u> 2921 2911	15.1(1)T (router)	Access	<b><u>SM-ES3G-24-P</u></b>	<b>Enhanced EtherSwitch SM, Layer 2/3 switching, 24 ports GE, POE capable</b>												
	12.2(52) EX1 (switch module)		SM-ES3G-16-P	Enhanced EtherSwitch SM, Layer 2/3 switching, 16 ports GE, POE capable												
			SM-ES3-24-P	Enhanced EtherSwitch SM, Layer 2/3 switching, 23 ports Fast Ethernet (FE), 1 port GE, POE capable												
			SM-ES3-16-P	Enhanced EtherSwitch SM, Layer 2/3 switching, 15 ports FE, 1 port GE, POE capable												
<p><b>NOTE:</b> 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><b>LEGEND:</b></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 Netron XMR</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 Netron XMR
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 Netron XMR													

**10. TESTING LIMITATIONS.** None.

**11. TEST RESULTS**

**a. Test Conduct.** The SUT was tested as a Layer 2 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.

(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. 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 was equipped with redundant uplinks and can support up to 50 users if multiple ES3 modules are installed in a chassis. 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. Non-Link Aggregation Control Protocol (LACP) link failover was achieved within 3.41 seconds. For a heterogeneous network (tested with Brocade) the average non-LACP link failover time was 3.19 seconds, but some failover times exceeded 5 seconds. This was likely caused by the Brocade XMR 4000 switches inability to recover IPv6 neighbor discovery in sufficient time.

(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 SUT shall be non-blocking for a minimum of 50 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 met this requirement with a measured jitter of .012 ms for video and .010 ms for 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 5-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 and video packets, and 0.003 percent for 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 5-minute period measured from ingress ports to egress ports under congested conditions. The SUT met this requirement with a measured latency of 0.191 ms or less for all traffic types on the 1 Gigabit (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 Megabits per second (Mbps) IAW Institute of Electrical and Electronics Engineers (IEEE) 802.3i and 100 Mbps IAW 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
<b>Network Management Interfaces for Layer 3 Access Switches</b>			
EIA/TIA (Serial) 232	R	EIA/TIA-232	Met
IEEE 802.3i (10BaseT UTP)	C	1, 6-15, 18-28, 31, 32-36, 48-53, 58-60, 65, 67-71	Not Tested
IEEE 802.3u (100BaseT UTP)	C	1, 6-15, 18-28, 31, 32-36, 48-53, 58-60, 65, 67-71	Met
IEEE 802.3ab (1000BaseT UTP)	C	1, 6-15, 18-28, 31, 32-36, 48-53, 58-60, 65, 67-71	Met
<b>Uplink Interfaces for Layer 3 Access Switches</b>			
IEEE 802.3u (100BaseT UTP)	C	1-15, 16, 18-24, 28-31, 40, 44-53, 55-60, 65-75	Met
IEEE 802.3u (100BaseFX)	C	1-6, 11, 16, 18-24, 28-31, 40-41, 44-53, 55-60, 65-75	Not Supported <sup>2</sup>
IEEE 802.3ab (1000BaseT UTP)	C	1-16, 18-24, 28-31, 40, 44-53, 55-60, 65-75	Met
IEEE 802.3z (1000BaseX Fiber)	C	1-5, 8-16, 18-24, 28-31, 40, 44-53, 55-60, 65-75	Met
IEEE 802.3ae (10GBaseX)	C	1-5, 8-16, 18, 19, 40-41, 44-53, 55-60, 65-75	Not Supported <sup>2</sup>
IEEE 802.3i (10BASET UTP)	C	1-15, 18-24, 28-41, 44-54, 58-71	Not Tested
IEEE 802.3u (100BaseT UTP)	C	1-15, 18-24, 28-41, 44-54, 58-71	Met

**Table 2-3. SUT Interface Status (continued)**

<b>Access Interfaces for Layer 3 Access Switches</b>			
IEEE 802.3u (100BaseFX)	C	1-6, 11, 18-24, 28-31, 44-54, 58-71	Not Supported <sup>2</sup>
IEEE 802.3ab (1000BaseT UTP)	C	1-15, 18-24, 28-41, 44-54, 58-71	Met
IEEE 802.3z (1000BaseX Fiber)	C	1-6, 11, 18-24, 28-31, 44-54, 58-71	Met
Interface	Applicability	CRs/FRs (See note 1.)	Status
	Access		Access
<b>Generic Requirements for all Interfaces</b>			
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	UCR, Sections 5.3.1.3.8, 5.3.1.5, 5.3.1.6, and 5.4	Met <sup>3</sup>
<b>NOTES:</b>			
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 modules, which are certified in the ASLAN Access Layer 2: <b>SM-ES3G-24-P</b> , SM-ES3-24P, SM-ES3G-16-P, and SM-ES3-16-P. 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 hardware 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, and 802.3z.			
3 Security testing is accomplished via DISA-led IA test teams and published in a separate report, Reference (e).			
<b>LEGEND:</b>			
802.3ab	1000BaseT Gbps Ethernet over twisted pair at 1 Gbps (125 Mbps)	EIA	Electronic Industries Alliance
802.3ae	10 Gbps Ethernet	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
802.3i	10BaseT Mbps over twisted pair		
802.3u	Standard for carrier sense multiple access with collision detection at 100 Mbps	FRs	Functional Requirements
802.3z	Gigabit Ethernet Standard	Gbps	Gigabits per second
10BaseT	10 Mbps (Baseband Operation, Twisted Pair) Ethernet	IA	Information Assurance
100BaseT	100 Mbps (Baseband Operation, Twisted Pair) Ethernet	ICMP	Internet Control Message Protocol
100BaseFX	100 Mbps Ethernet over fiber	ID	Identification
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
10GBaseX	10000 Mbps Ethernet over Category 5 Twisted Pair Copper	JITC	Joint Interoperability Test Command
ASLAN	Assured Services Local Area Network	Mbps	Megabits per second
C	Conditional	NA	Not Applicable
CRs	Capability Requirements	OS	Operating System
DISA	Defense Information Systems Agency	R	Required
DoD	Department of Defense	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. 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 (0-63) 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, per the vendor's LoC, 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, the SUT has the capability to assign any VLAN ID any value from 0 through 4096, 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. 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.

(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) IAW RFCs 2472, 2494, 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.

(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. As outlined in 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. 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 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. The 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 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 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 is certified for joint use within the DSN as an access layer 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. The SUT is certified to support DSN Assured Services over IP as an ASLAN IAW the requirements set forth in the UCR 2008.

**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/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](mailto:ucco@disa.mil).