DEFENSE INFORMATION SYSTEMS AGENCY
JOINT INTEROPERABILITY TEST COMMAND
P.O. BOX 12798
FORT HUACHUCA, ARIZONA 85670-2798

IN REPLY
REFER TO: Networks and Transport Division (JTE) 22 May 2006

MEMORANDUM FOR DISTRIBUTION

SUBJECT: Special Interoperability Test Certification of Cisco Assured Services Voice Application Local Area Network (ASVALAN) with Specified Software Releases

References: (a) DoD Directive 4630.5, "Interoperability and Supportability of Information Technology (IT) and National Security Systems (NSS)," 5 May 2004
(b) CJCSI 6212.01C, "Interoperability and Supportability of Information Technology and National Security Systems," 20 November 2003

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. Additional references are provided in enclosure 1.

2. The Cisco ASVALAN with specified software releases, hereinafter referred to as the system under test (SUT), meets all of its critical interoperability requirements and is certified as interoperable for joint use within the Defense Switched Network (DSN). The ASVALAN, formerly known as a Command and Control Voice Grade Local Area Network (C2VGLAN), is certified to support DSN assured services over Internet Protocol. Components found in the tables throughout this certification letter, which are bolded and underlined, were tested by JITC. Components not underlined and bolded are in the family and were not tested. However, they utilize the same IOS software and hardware and JITC analysis determined them to be functionally identical for interoperability certification purposes and they are also certified for joint use. Testing the SUT did not include converged voice, video, and data services via a single port, and, therefore is not covered under this certification. This certification expires upon changes that could affect interoperability, but no later than three years from the date of this memorandum.

3. This finding is based on interoperability testing conducted by JITC and a review of the vendor's Letters of Compliance (LoC). Testing was conducted at JITC's Global Information Grid Network Test Facility at Fort Huachuca, Arizona, from 26 September 2005 through 31 October 2005. Review of the vendor's LoC was completed on 12 May 2006. Enclosure 2 documents the test results and describes the tested network. System interoperability should be verified before deployment in an operational environment that varies significantly from the test environment.

4. The overall interoperability status of the SUT is indicated in table 1. The SUT system requirements are listed in table 2. In addition to system level requirements, components that comprise the SUT must meet specific criteria to be certified for use as core, distribution, or access

components. The interoperability status of the SUT components is listed in table 3. The requirements used to certify the components are listed in table 4. This interoperability test status is based on the SUT's ability to meet:

a. Local Area Network (LAN) system requirements specified in reference (c) verified through JITC testing and/or vendor submission of LoC.

b. Assured services as defined in reference (d).

c. The overall system interoperability performance derived from test procedures listed in reference (e).

Table 1. SUT ASVALAN Interoperability Status

System Interoperability Status			
Components (see note 1)	**Release**	**Status**	**Remarks**
Cisco **6509**/6509-NEB/6509-NEB-A/ 6503/6506/6513 Catalyst Switches	Native IOS 12.2 (18) SXD5	Certified	All LAN system requirements depicted in tables 2 and 4 were met when the SUT was configured in accordance with architecture provided in enclosure 2.[4] Additional details about component level certification are provided in table 3.
Cisco **4507R**/4503[2]/4506[2]/4510R Catalyst Switches	IOS 12.2 (25) EWA		
Catalyst 3750PoE24/3750PoE48	IOS 12.2 (25) SEB2		
Catalyst 3550 – Inline Power[3]	IOS 12.2 (25) SEB2		
Catalyst 3560 – PoE 24	IOS 12.2 (25) SEB2		

LEGEND:

ASVALAN	- Assured Services Voice Application Local Area Network	LAN	- Local Area Network
DISA	- Defense Information Systems Agency	NEB	- Network Equipment Building
IA	- Information Assurance	PoE	- Power over Ethernet
IOS	- Internetworking Operating System	SUT	- System Under Test
JITC	- Joint Interoperability Test Command		

NOTES:

1 Components bolded and underlined were tested by JITC. The other components in the family series were not tested; however, they utilize the same IOS software and hardware and JITC analysis determined them to be functionally identical for interoperability certification purposes and they are also certified for joint use.
2 Indicates these switches support one processor and must be configured to fail over to a redundant distribution switch.
3 The vendor has no plan to support IPv6 on the Catalyst 3550. The operational impact is minor.
4 LAN Security is accomplished through DISA-led IA testing and evaluation. Results are published in a separate report.

Table 2. ASVALAN System Requirements

System Requirements			
Requirement	**Criteria**	**Reference**	**Critical**
Delay	One-way packet delay for voice packets of an established call (signaling and media) shall be five ms or less averaged over any five-minute period.	GSCR, Appendix 3, Section A3.3.1.1	Yes
Jitter	For voice media packets, jitter shall be five ms or less averaged over any five-minute period.	GSCR, Appendix 3, Section A3.3.1.2	Yes
Packet Loss	Voice packet loss within the LAN shall not exceed 0.05% averaged over any five-minute period.	GSCR, Appendix 3, Section A3.3.1.3	Yes
Reliability	- LANs shall have a reliability of .99999 - No single point of failure for outage of more than 64 telephony subscribers - Maximum downtime of 35 mins/yr for network links and 12 mins/yr for IP subscribers - Network Path restores within 2 seconds	GSCR, Appendix 3, Section A3.3.4.1	Yes
Security	- DITSCAP/IA (see note)	GSCR, Appendix 3, Section A3.3.4.3	Yes
IPv6	All IP devices shall be IPv6 capable	GSCR, Appendix 3, Section A3.2.8.	Yes

LEGEND:

ASVALAN	- Assured Services Voice Application Local Area Network	IP	- Internet Protocol
DISA	- Defense Information Systems Agency	IPv6	- Internet Protocol version 6
DITSCAP	- Department of Defense Information Technology Security Certification and Accreditation Process	LAN	- Local Area Network
		mins	- minutes
GSCR	- Generic Switching Center Requirements	ms	- milliseconds
IA	- Information Assurance	yr	- year

NOTE: Information assurance testing is accomplished via DISA-led Information Assurance test teams and published in a separate report.

Table 3. SUT Component Interoperability Status

Component Interoperability Status				
Component[1]	**Release**	**Sub-component[1]**	**Status**	**Remarks**
Cisco **6509**/6509-NEB/6509-NEB-A/ 6503/6506/6513 Catalyst Switches	Native IOS 12.2 (18) SXD5	**WS-X6K-SUP2-2GE**[3, 4]	Certified	All Core, Distribution, and Access requirements were met when configured in accordance with the architecture provided in enclosure 2.
		WS-X6K-S2U-MSFC2[3, 4]	Certified	
		WS-X6K-S2-MSFC2[3, 4]	Certified	
		WS-SUP720-3B[4]	Certified	
		WS-SUP720[4]	Certified	
		WS-SUP720-3BXL[4]	Certified	
		WS-C6500-SFM	Certified	
		WS-X6148-RJ45V	Certified	
		WS-X6148-RJ-21	Certified	
		WS-X6148-RJ21V	Certified	
		WS-X6148-RJ-45	Certified	
		WS-X6148V-GE-TX	Certified	
		WS-X6148-GE-TX	Certified	
		WS-X6148-45AF	Certified	
		WS-X6148-21AF	Certified	
		WS-X6348-RJ45V	Certified	
		WS-X6348-RJ21V	Certified	
		WS-X6348-RJ-45	Certified	
		WS-X6516-GBIC	Certified	
		WS-X6516-GE-TX	Certified	
		WS-X6516A-GBIC	Certified	
		WS-X6548-GE-45AF	Certified	
		WS-X6548V-GE-TX	Certified	
		WS-X6548-GE-TX	Certified	
		WS-X6548-RJ-21	Certified	
		WS-X6548-RJ-45	Certified	
		WS-X6748-SFP	Certified	
		WS-X6724-SFP	Certified	
		WS-X6748-GE-TX	Certified	
		WS-X6816-GBIC	Certified	

Table 3. SUT Component Interoperability Status (Continued)

Component Interoperability Status				
Component[1]	**Release**	**Sub-component[1]**	**Status**	**Remarks**
Cisco **4507R**/4503[2] /4506[2]/4510R Catalyst Switches	IOS 12.2 (25) EWA	**WS-X4515-10GE Supervisor Engine V-10GE**[4, 5]	Certified	All Distribution requirements were met when configured in accordance with the architecture provided in enclosure 2.
		WS-X4306-GB	Certified	
		WS-X4302-GB	Certified	
Catalyst **3750G-24PS-E**[6]/ **3750G-48PS-E**[6]/3750-24PS-E[6]/3750G-24TS-E1U[6]/3750-24TS-E1U[6]/ 3750G -24TS-E[6]/3750-24TS-E[6]/3750G-24T-E[6]/ 3750-24T-E[6]/ 3750-48PS-E[6]/ 3750G-48TS-E[6]/ 3750-48TS-E[6]	12.2(25) SEB2		Certified	All Access requirements were met when configured in accordance with the architecture provided in enclosure 2.
Catalyst 3560-24PS-S	12.2(25) SEB2		Certified	All Access requirements were met when configured in accordance with the architecture provided in enclosure 2.
Catalyst 3550-24PWR-EMI	12.2(25) SEB2		Certified	All Access requirements were met when configured in accordance with the architecture provided in enclosure 2. The vendor has no plan to support IPv6 on the Catalyst 3550. The operational impact is minor.

LEGEND:

AF	- IEEE 802.3af complaint	NEB	- Network Equipment Building
EMI	- Enhanced Multilayer Software Image	PoE	- Power Over Ethernet
G	- Gigabit	PWR	- Power
GB	- Gigabit	RJ	- Registered Jack
GBIC	- Gigabit Interface Card	SFM	- Switch Fabric Module
GE	- Gigabit Ethernet	SFP	- Small Form-Factor Pluggable
IEEE	- Institute of Electrical and Electronics Engineers, Inc.	SUT	- System Under Test
IOS	- Internetworking Operating System	SUP	- Supervisor
JITC	- Joint Interoperability Test Command	V	- Voice
MSFC	- Multilayer Switch Feature Card	WS	- Workgroup Station

NOTES:

1 Components bolded and underlined were tested by JITC. The other components in the family series were not tested; however, they utilize the same IOS software and hardware and JITC analysis determined them to be functionally identical for interoperability certification purposes and they are also certified for joint use.
2 Indicates these switches support one processor and must be configured to fail over to a second distribution switch.
3 Memory on this supervisor card must be upgraded to 512 megabits to run the certified IOS.
4 The Gigabit ports are not certified as uplinks.
5 The 10-Gigabit Ethernet ports are not certified as uplinks.
6 The switch is certified as standalone only. Switches are not certified when stacked/daisy-chained together.

Table 4. Component Requirements

Core/Distribution/Access Component Requirements			
Requirement	**Criteria**	**Reference**	**Critical**
CoS Models	LAN components shall support IEEE 802.1p to DSCP mapping and at least one of the following: - IEEE 802.1p/Q tagging - DSCP - ToS	GSCR, Appendix 3, Section A3.3.2.1	Yes
Traffic Prioritization	Traffic within LAN components shall be prioritized so that voice signaling receives highest priority, voice media second highest priority, and data lowest priority.	GSCR, Appendix 3, Section A3.3.2.2	Yes
QoS	LAN components shall support one of the following: - Priority Queuing - Custom Queuing - Weighted Fair Queuing - Class Based Weighted Fair Queuing	GSCR, Appendix 3, Section A3.3.3.1	Yes
Policing	LAN components shall support one of the following: - DSCP PHB - Generic Traffic Shaping - Class-Based Shaping	GSCR, Appendix 3, Section A3.3.3.2	Yes
VLANs	LAN components shall support: - Port based VLANs - MAC address based VLANs - Protocol based VLANs	GSCR, Appendix 3, Section A3.3.3.3	Yes
IEEE Conformance	LAN components shall support: - IEEE 802.1d – Bridging - IEEE 802.1p/Q – VLAN tagging - IEEE 802.1s – Per-VLAN Group Spanning Tree - IEEE 802.1v – VLAN Classification by port and protocol - IEEE 802.1w –Rapid Reconfiguration of Spanning Tree - IEEE 802.1x – Port Based Network Access Control - IEEE 802.3ad – Link Aggregation Protocol	GSCR, Appendix 3, Section A3.3.4	Yes
Reliability	LAN components shall support[1]: - Dual power supplies and dual processors (more than 64 users) - N+1 sparing for access (more than 64 users) - Redundancy protocol[2] - 2 second path restoral	GSCR, Appendix 3, Section A3.3.4.1	Yes
Network Management	LAN components shall support: - In-band or out-of-band management - SNMP - Measurements	GSCR, Appendix 3, Section A3.3.4.2	Yes
Security	LAN components shall employ the Network Infrastructure and VoIP STIGs.[3]	GSCR, Appendix 3, Section A3.3.4.3	Yes
IPv6	All IP devices shall be IPv6 capable	GSCR, Appendix 3, Section A3.2.8	Yes
TE	- LAN components shall be engineered for a maximum of 25% voice traffic per link.[4] - For more than 64 users, link pairs (redundant links) must be used.	GSCR, Appendix 3, Section A3.3.4.4	Yes
LAN Architectures	- Access - Distribution - Core	GSCR, Appendix 3, Section A3.3.4.5	No

LEGEND:

CoS	- Class of Service	N	- total VoIP users / 64
DISA	- Defense Information Systems Agency	PHB	- Per Hop Behaviors
DSCP	- Differentiated Services Code Point	QoS	- Quality of Service
GSCR	- Generic Switching Center Requirements	SNMP	- Simple Network Management Protocol
IEEE	- Institute of Electrical and Electronics Engineers, Inc.	STIGs	- Security Technical Implementation Guide
IP	- Internet Protocol	TE	- Traffic Engineering
IPv6	- Internet Protocol version 6	ToS	- Type of Service
LAN	- Local Area Network	VLANs	- Virtual LANs
MAC	- Media Access Control	VoIP	- Voice over Internet Protocol
Mbps	- Megabits per second		

NOTES:

1 Core and distribution components may use redundant (duplicated) components instead of dual modules (processor and power) to provide failover capability.

2 For core, distribution, and access components, redundancy protocol shall be Enhanced Interior Gateway Routing Protocol.

3 Verified using the Information Assurance Test Plan. Results of the security testing are reported in a separate test report generated by the DISA Information Assurance test personnel.

4 Instruments connected to an access device must provide a minimum of a 10 Mbps full duplex link. For core and distribution connections, the minimum link capacity is 100 Mbps full duplex.

5. No detailed test report was developed in accordance with the Program Manager's request. JITC distributes interoperability information via the JITC Electronic Report Distribution (ERD) system, which uses Unclassified-But-Sensitive Internet Protocol Router Network (NIPRNet) e-mail. More comprehensive interoperability status information is available via the JITC System Tracking Program (STP). The STP is accessible by .mil/gov users on the NIPRNet at https://stp.fhu.disa.mil. Test reports, lessons learned, and related testing documents and references are on the JITC Joint Interoperability Tool (JIT) at http://jit.fhu.disa.mil (NIPRNet), or http://199.208.204.125 (SIPRNet). Information related to DSN testing is on the Telecom Switched Services Interoperability (TSSI) website at http://jitc.fhu.disa.mil/tssi.

6. The JITC point of contact is Capt. Michel Roy, DSN 821-8575, commercial (520) 533-8575, FAX DSN 879-4347, or e-mail to Michel.Roy.ca@disa.mil. The VCAO tracking numbers for the SUT are 50222/51641.

FOR THE COMMANDER:

2 Enclosures a/s

RICHARD A. MEADOR
Chief
Networks and Transport Division

JITC Memo, JTE, Special Interoperability Test Certification of Cisco Assured Services Voice Application Local Area Network (LAN) with Specified Software Releases

Distribution:
Joint Staff J6I, Room 1E596, Pentagon, Washington, DC 20318-6000
Joint Interoperability Test Command, Liaison, ATTN: TED/JT1, 2W24-8C, P.O. Box 4502, Falls Church, VA 22204-4502
Defense Information Systems Agency, Net-Centricity Requirements and Assessment Branch, ATTN: GE333, Room 244, P.O. Box 4502, Falls Church, VA 22204-4502
Office of Chief of Naval Operations (N71CC2), CNO N6/N7, 2000 Navy Pentagon, Washington, DC 20350
Headquarters U.S. Air Force, AF/XICF, 1800 Pentagon, Washington, DC 20330-1800
Department of the Army, Office of the Secretary of the Army, CIO/G6, ATTN: SAIS-IOQ, 107 Army Pentagon, Washington, DC 20310-0107
U.S. Marine Corps (C4ISR), MARCORSYSCOM, 2200 Lester St., Quantico, VA 22134-5010
DOT&E, Net-Centric Systems and Naval Warfare, 1700 Defense Pentagon, Washington, DC 20301-1700
U.S. Coast Guard, CG-64, 2100 2nd St. SW, Washington, DC 20593
Defense Intelligence Agency, 2000 MacDill Blvd., Bldg 6000, Bolling AFB, Washington, DC 20340-3342
National Security Agency, ATTN: DT, Suite 6496, 9800 Savage Road, Fort Meade, MD 20755-6496
Director, Defense Information Systems Agency , ATTN: GS235, Room 5W24-8A, P.O. Box 4502, Falls Church, VA 22204-4502
Office of Assistant Secretary of Defense (NII)/DOD CIO, Crystal Mall 3, 7th Floor, Suite 7000, 1851 S. Bell St., Arlington, VA 22202
Office of Under Secretary of Defense, AT&L, Room 3E144, 3070 Defense Pentagon, Washington, DC 20301
U.S. Joint Forces Command, J68, Net-Centric Integration, Communications, and Capabilities Division, 1562 Mitscher Ave., Norfolk, VA 23551-2488
Defense Information Systems Agency (DISA), ATTN: GS23 (Mr. Osman), Room 5w23, 5275 Leesburg Pike (RTE 7), Falls Church, VA 22041

ADDITIONAL REFERENCES

(c) Defense Information Systems Agency (DISA), "Defense Switched Network (DSN) Generic Switching Center Requirements (GSCR), Appendix 3, (Incorporated Change 1)," 1 March 2005

(d) Chairman of the Joint Chiefs of Staff Instruction (CJCSI) 6215.01B, "Policy for Department of Defense Voice Services," 23 September 2001

(e) Joint Interoperability Test Command, "Defense Switched Network Generic Switch Test Plan (GSTP), Change 1, Revision 1," 1 June 2005

CERTIFICATION TESTING SUMMARY

1. SYSTEM TITLE. Cisco Assured Services Voice Application Local Area Network (ASVALAN) with specified software releases, hereinafter referred to as the system under test (SUT).

2. PROPONENT. Defense Information Systems Agency (DISA).

3. PROGRAM MANAGER. Mr. Howard Osman, GS23, Room 5W23, 5275 Leesburg Pike, Falls Church, VA 22041, E-mail: Howard.Osman@disa.mil.

4. TESTER. Joint Interoperability Test Command (JITC), Fort Huachuca, Arizona.

5. SYSTEM UNDER TEST DESCRIPTION. The SUT is an ASVALAN. An ASVALAN is used to transport voice signaling and media as part of an overall Voice over Internet Protocol (VoIP) system. The SUT consisted of the following devices:

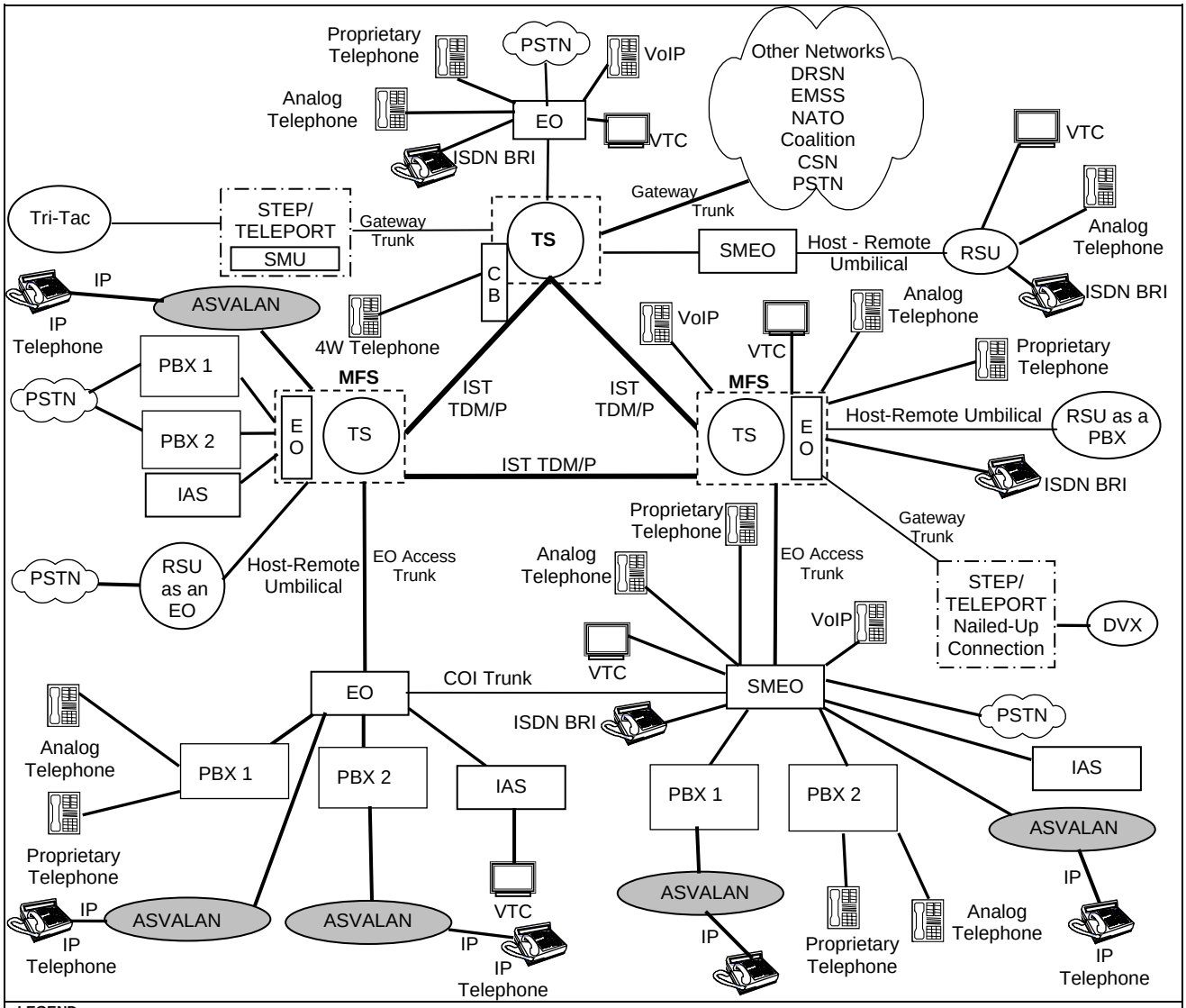
a. Core: The Catalyst 6500 series switches can be used as core, distribution, or access switches. The Catalyst 6509 switch with Native Internetworking Operating System (IOS) 12.2 (18) SXD5, delivers scalable performance and port density across several chassis configurations. The Catalyst 6500 series is available in 3-, 6-, 9-, and 13-slot chassis. The Catalyst 6500 series switches feature a range of integrated services modules, including gigabit fiber cards and 10/100/1000 Megabits per second (Mbps) switchblades used as access points. For data and voice applications, users connect to the Local Area Network (LAN) using the 10/100/1000 Base-T Ethernet interface on the access devices.

b. Distribution: The Cisco Catalyst 4507R with IOS 12.2 (25) EWA is certified in the distribution layer only. The 4500 series switch is available in a multi-slot chassis. This framework allows flexibility in creating a switching platform. This configuration also allows for a highly redundant architecture to ensure no single point of failure for hardware operations. Some slots are reserved for special functions such as supervisor engines. Most slots are flexible and can be configured for specific user needs. One benefit of this system is the ability to add, delete, and change system elements over time. All line card capabilities including bandwidth, throughputs, and routing are dependent on the supervisor engine. With a failure of the supervisor engine, all ports on the 4500 switch will reset, therefore, this switch cannot be used as an access device.

c. Access: The Cisco Catalyst 3750 Ethernet Switch with release 12.2(25) SEB2, the Catalyst 3560 Ethernet Switch with release 12.2(25) SEB2, the Catalyst 3550 with release 12.2(25) SEB2 are certified in the access layer only. The 3550 provide Power over Ethernet (PoE) specifically to Cisco devices. The 3750 and 3560 can provide PoE to Cisco devices, as well as any device, which complies with the Institute of Electrical and Electronics Engineers, Inc. (IEEE) 802.3af standard. All of these standalone switches provide high availability, security, and Quality of Service (QoS) to meet the operational requirements of the network. Security access control lists, QoS, rate-limiting, multicast management, and Internet Protocol (IP) routing can be implemented on the switches. Shared access (i.e., same switch port is shared by PC and IP phone),

was tested with this configuration. IP phones were connected to the 100 Mbps full duplex access switch port and data was connected to the 100 Mbps ethernet port on the back of the phones. In this configuration the Catalyst 3550 showed degradation of voice quality, therefore this system is certified for shared access on all devices except the Catalyst 3550 access switch.

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 IP infrastructures. The Generic Switching Center Requirements (GSCR) operational DSN Architecture is depicted in figure 2-1. The installation VoIP architecture is depicted in figure 2-2. The VoIP architecture depicts the relationship of ASVALAN DSN switch types.



LEGEND:

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

Figure 2-1. DSN Architecture

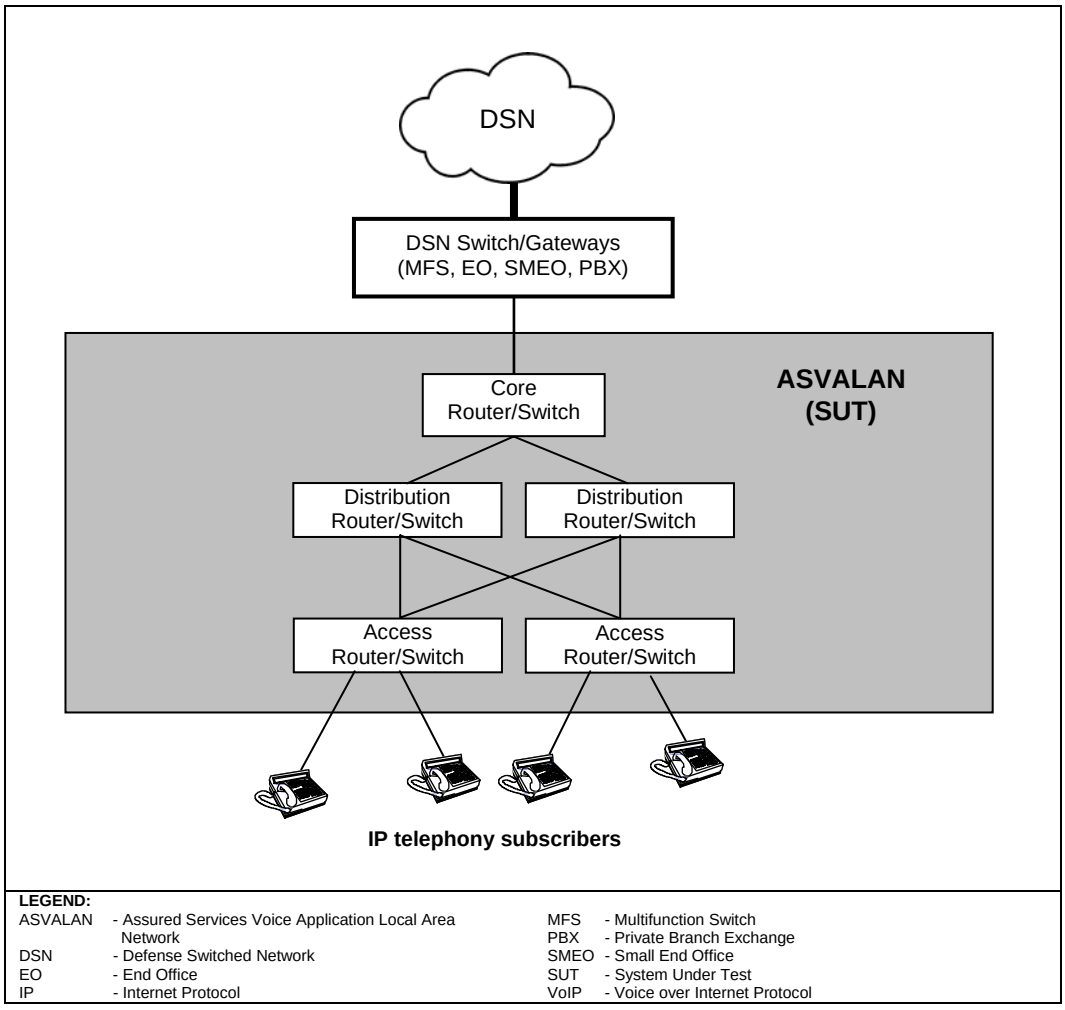


Figure 2-2. VoIP Architecture

7. REQUIRED SYSTEM INTERFACES. Requirements specific to the SUT and its components are listed in table 2-1. The requirements specific to the SUT components are shown in table 2-2. These requirements are derived from:

a. DSN services for Network and Applications specified in Chairman of the Joint Chiefs of Staff Instruction (CJCSI) 6215.01B, "Policy for Department of Defense Voice Services."

b. GSCR, appendix 3: Capability Requirements (CRs) and Feature Requirements (FRs) verified through JITC testing and/or vendor submission of Letters of Compliance (LoC).

Table 2-1. ASVALAN Requirements

System Requirements			
Requirement	**Criteria**	**Reference**	**Critical**
Delay	One-way packet delay for voice packets of an established call (signaling and media) shall be five ms or less averaged over any five-minute period.	GSCR, Appendix 3, Section A3.3.1.1	Yes
Jitter	For voice media packets, jitter shall be five ms or less averaged over any five-minute period.	GSCR, Appendix 3, Section A3.3.1.2	Yes
Packet Loss	Voice packet loss within the LAN shall not exceed 0.05% averaged over any five-minute period.	GSCR, Appendix 3, Section A3.3.1.3	Yes
Reliability	- LANs shall have a reliability of .99999 - No single point of failure for outage of more than 64 telephony subscribers - Maximum downtime of 35 mins/yr for network links and 12 mins/yr for IP subscribers - Network Path restores within 2 seconds	GSCR, Appendix 3, Section A3.3.4.1	Yes
Security	- DITSCAP/IA (see note)	GSCR, Appendix 3, Section A3.3.4.3	Yes
IPv6	All IP devices shall be IPv6 capable	GSCR, Appendix 3, Section A3.2.8.	Yes

LEGEND:

ASVALAN - Assured Services Voice Application Local Area Network
DISA - Defense Information Systems Agency
DITSCAP - Department of Defense Information Technology Security Certification and Accreditation Process
GSCR - Generic Switching Center Requirements
IA - Information Assurance
IP - Internet Protocol
IPv6 - Internet Protocol version 6
LAN - Local Area Network
mins - minutes
ms - milliseconds
yr - year

NOTE: Information assurance testing is accomplished via DISA-led Information Assurance test teams and published in a separate report.

Table 2-2. Component Requirements

Core/Distribution/Access Component Requirements			
Requirement	**Criteria**	**Reference**	**Critical**
CoS Models	LAN components shall support IEEE 802.1p to DSCP mapping and at least one of the following: - IEEE 802.1p/Q tagging - DSCP - ToS	GSCR, Appendix 3, Section A3.3.2.1	Yes
Traffic Prioritization	Traffic within LAN components shall be prioritized so that voice signaling receives highest priority, voice media second highest priority, and data lowest priority.	GSCR, Appendix 3, Section A3.3.2.2	Yes
QoS	LAN components shall support one of the following: - Priority Queuing - Custom Queuing - Weighted Fair Queuing - Class Based Weighted Fair Queuing	GSCR, Appendix 3, Section A3.3.3.1	Yes
Policing	LAN components shall support one of the following: - DSCP PHB - Generic Traffic Shaping - Class-Based Shaping	GSCR, Appendix 3, Section A3.3.3.2	Yes
VLANs	LAN components shall support: - Port based VLANs - MAC address based VLANs - Protocol based VLANs	GSCR, Appendix 3, Section A3.3.3.3	Yes
IEEE Conformance	LAN components shall support: - IEEE 802.1d – Bridging - IEEE 802.1p/Q – VLAN tagging - IEEE 802.1s – Per-VLAN Group Spanning Tree - IEEE 802.1v – VLAN Classification by port and protocol - IEEE 802.1w –Rapid Reconfiguration of Spanning Tree - IEEE 802.1x – Port Based Network Access Control - IEEE 802.3ad – Link Aggregation Protocol	GSCR, Appendix 3, Section A3.3.4	Yes

Table 2-2. Component Requirements (continued)

Core/Distribution/Access Component Requirements			
Requirement	**Criteria**	**Reference**	**Critical**
Reliability	LAN components shall support[1]: - Dual power supplies and dual processors (more than 64 users) - N+1 sparing for access (more than 64 users) - Redundancy protocol[2] - 2 second path restoral	GSCR, Appendix 3, Section A3.3.4.1	Yes
Network Management	LAN components shall support: - In-band or out-of-band management - SNMP - Measurements	GSCR, Appendix 3, Section A3.3.4.2	Yes
Security	LAN components shall employ the Network Infrastructure and VoIP STIGs.[3]	GSCR, Appendix 3, Section A3.3.4.3	Yes
IPv6	All IP devices shall be IPv6 capable	GSCR, Appendix 3, Section A3.2.8	Yes
TE	- LAN components shall be engineered for a maximum of 25% voice traffic per link.[4] - For more than 64 users, link pairs (redundant links) must be used.	GSCR, Appendix 3, Section A3.3.4.4	Yes
LAN Architectures	- Access - Distribution - Core	GSCR, Appendix 3, Section A3.3.4.5	No

LEGEND:

CoS	- Class of Service	N	- total VoIP users / 64
DISA	- Defense Information Systems Agency	PHB	- Per Hop Behaviors
DSCP	- Differentiated Services Code Point	QoS	- Quality of Service
GSCR	- Generic Switching Center Requirements	SNMP	- Simple Network Management Protocol
IEEE	- Institute of Electrical and Electronics Engineers, Inc.	STIGs	- Security Technical Implementation Guide
IPv6	- Internet Protocol version 6	TE	- Traffic Engineering
LAN	- Local Area Network	ToS	- Type of Service
MAC	- Media Access Control	VLANs	- Virtual LANs
Mbps	- Megabits per second	VoIP	- Voice over Internet Protocol

NOTES:

1 Core and distribution components may use redundant (duplicated) components instead of dual modules (processor and power) to provide failover capability.

2 For core, distribution, and access components, redundancy protocol shall be Enhanced Interior Gateway Routing Protocol.

3 Verified using the Information Assurance Test Plan. Results of the security testing are reported in a separate test report generated by the DISA Information Assurance test personnel.

4 Instruments connected to an access device must provide a minimum of a 10 Mbps full duplex link. For core and distribution connections, the minimum link capacity is 100 Mbps full duplex.

8. TEST NETWORK DESCRIPTION. The SUT was tested at JITC's Global Information Grid Network Test Facility in a manner and configuration similar to that of the DSN operational environment. Testing of the systems required functions and features was conducted using the test configuration depicted in figure 2-3.

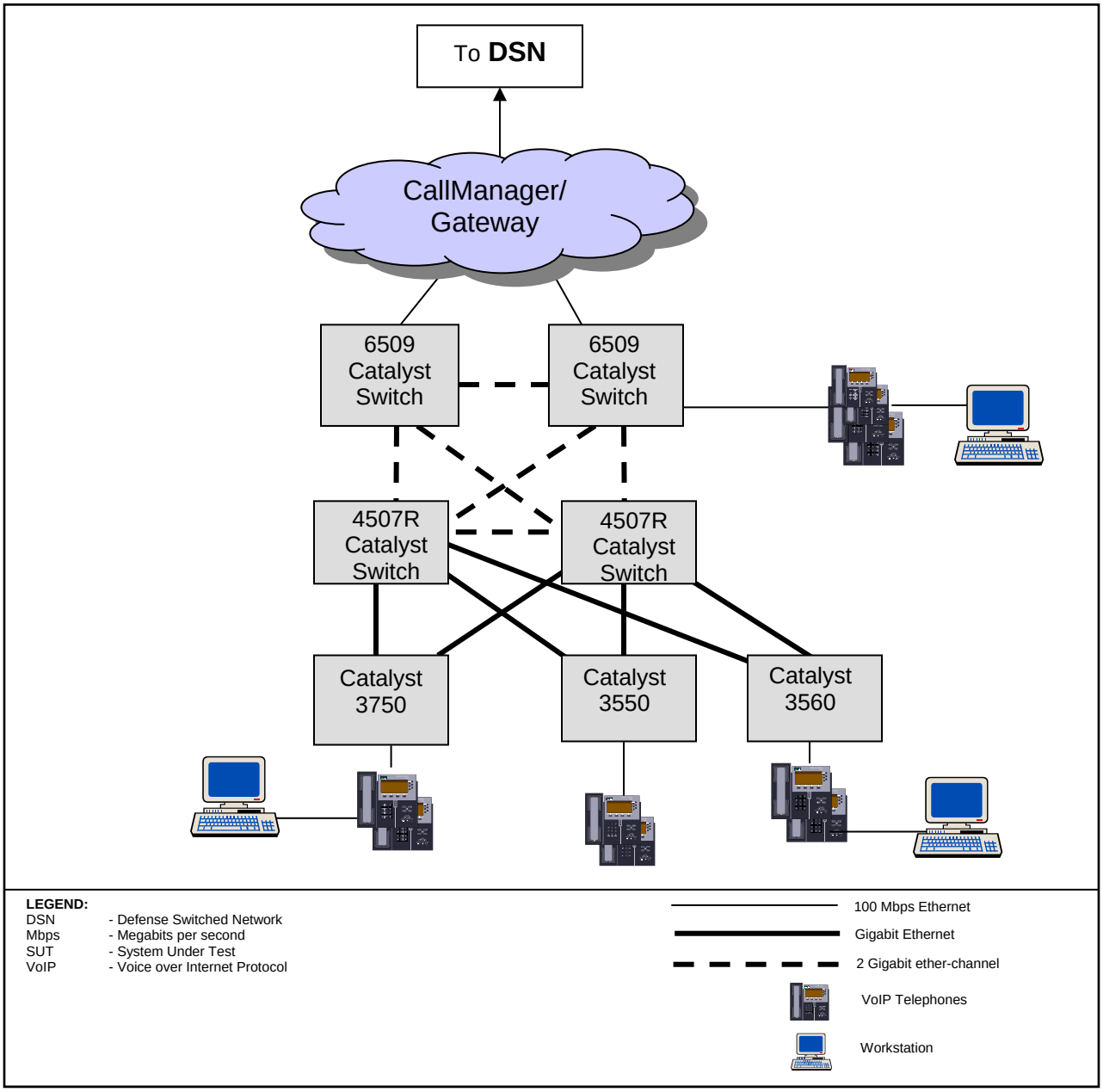


Figure 2-3. SUT Assured Services Voice Application Local Area Network

9. SYSTEM CONFIGURATIONS. Table 2-3 provides the tested system configurations.

Table 2-3. Tested System Configurations

System Under Test ASVALAN and Components			
Component[1]	**Release**	**Sub-component**[1]	**Function**
Cisco **6509**/6509-NEB/ 6509-NEB-A/6503/6506/6513 Catalyst Switches	Native IOS 12.2 (18) SXD5	**WS-X6K-SUP2-2GE**[3, 4]	Core Processor
		WS-X6K-S2U-MSFC2[3, 4]	Core Processor
		WS-X6K-S2-MSFC2[3, 4]	Core Processor
		WS-SUP720-3B[4]	Core Processor
		WS-SUP720[4]	Core Processor
		WS-SUP720-3BXL[4]	Core Processor
		WS-C6500-SFM	Switch Fabric Module
		WS-X6148-RJ45V	48-port Access switch 10/100 Mbps, RJ-45, with Inline Power
		WS-X6148-RJ-21	48-port Access switch 10/100 Mbps, RJ-21
		WS-X6148-RJ-21V	48-port Access switch 10/100 Mbps, RJ-21, with Inline Power
		WS-X6148-RJ45	48-port Access switch 10/100 Mbps, RJ-45
		WS-X6148V-GE-TX	48-port Access switch 10/100/1000 Mbps, RJ-45, with Inline Power
		WS-X6148-GE-TX	48-port Access switch 10/100/1000 Mbps, RJ-45
		WS-X6148-45AF	48-port Access switch 10/100/1000 Mbps, RJ-45, with PoE
		WS-X6148-21AF	48-port Access switch 10/100/1000 Mbps, RJ-21, with PoE
		WS-X6348-RJ45V	48-port Access switch 10/100 Mbps RJ-45, with Inline Power
		WS-X6348-RJ21V	48-port Access switch 10/100 Mbps RJ-21, with Inline Power
		WS-X6348-RJ-45	48-port Access switch 10/100 Mbps RJ-45
		WS-X6516-GBIC	16-port 1000 Mbps (GE) optical interface
		WS-X6516-GE-TX	16-port 1000 Mbps (GE) copper interface
		WS-X6516A-GBIC	16-port 1000 Mbps (GE) optical interface
		WS-X6548-GE-45AF	48-port Access switch 10/100/1000 RJ-45, with PoE
		WS-X6548V-GE-TX	48-port Access switch 10/100/1000 Mbps, with Inline Power
		WS-X6548-GE-TX	48-port Access switch 10/100/1000 Mbps
		WS-X6548-RJ-21	48-port Access switch 10/100 Mbps RJ-21
		WS-X6548-RJ-45	48-port Access switch 10/100 Mbps RJ-45
		WS-X6748-SFP	48-port 1000 Mbps (GE) optical interface
		WS-X6724-SFP	24-port 1000 Mbps (GE) optical interface
		WS-X6748-GE-TX	48-port Access switch 10/100/1000 Mbps RJ-45
		WS-X6816-GBIC	16-port 1000Mbps (GE) optical interface

Table 2-3. Tested System Configurations (Continued)

System Under Test ASVALAN and Components			
Component[1]	**Release**	**Sub-component**[1]	**Function**
Cisco **4507R**/4503[2]/4506[2]/4510R Catalyst Switches	IOS 12.2 (25) EWA	**WS-X4515-10GE Supervisor Engine V-10GE**[4, 5]	Distribution Processor
		WS-X4306-GB	6-port 1000 Mbps (Gig) Interface
		WS-X4302-GB	2-port 1000 Mbps (Gig) Interface
Catalyst **3750G-24PS-E**[6]/**3750G-48PS-E**[6]/3750G-24TS-E1U[6]/ 3750G -24TS-E[6]/3750G-24T-E[6]/ 3750G-48TS-E[6]**/**	12.2(25) SEB2		Access switch 10/100/1000 Mbps
Catalyst 3750-24PS-E[6]/3750-24TS-E1U[6]/3750-24TS-E[6]/3750-24T-E[6]**/**3750-48PS-E[6]/ 3750-48TS-E[6]			Access switch 10/100 Mbps
Catalyst 3560 – PoE 24	12.2(25) SEB2	**WS-3560-24PS-S**	Access switch 10/100 Mbps
Catalyst 3550 – Inline Power	12.2(25) SEB2	**WS-C3550-24PWR-EMI**	Access switch 10/100 Mbps

LEGEND:

ASVALAN	- Assured Service Voice Application Local Area Network	MSFC	- Multilayer Switch Feature Card
EMI	- Enhanced Mulitlayer Software Image	NEB	- Network Equipment Building
G	- Gigabit	PoE	- Power Over Ethernet
GB	- Gigabit	RJ	- Registered Jack
GBIC	- Gigabit Interface Card	SFM	- Switch Fabric Module
GE	- Gigabit Ethernet	SFP	- Small Form-Factor Pluggable
IOS	- Internetworking Operating System	SUP	- Supervisor
JITC	- Joint Interoperability Test Command	V	- Voice
LAN	- Local Area Network	WS	- Workgroup Station
Mbps	- Megabits per second		

NOTES:

1 Components bolded and underlined were tested by JITC. The other components in the family series were not tested; however, they utilize the same IOS software and hardware and JITC analysis determined them to be functionally identical for interoperability certification purposes and they are also certified for joint use as described above.
2 Indicates these switches support one processor and must be configured to fail over to a second distribution switch.
3 Memory on these supervisor cards must be upgraded to 512 megabits to run the certified IOS.
4 Gigabit Ethernet ports not certified as uplinks.
5 10 Gigabit Ethernet ports not certified as uplinks.
6 The switch is certified as standalone only. Switches are not certified when stacked/daisy-chained together.

10. TESTING LIMITATIONS. None.

11. TEST RESULTS

a. Components. The SUT LAN solution as shown in figure 2-3 met the minimum interoperability requirements of the GSCR, appendix 3, for an ASVALAN. The network consisted of three main components: core switches, distribution switches, and access switches. The results for the specific tests carried out are provided below.

(1) Class of Service (CoS). The SUT is required to support CoS. The SUT employed IEEE 802.1p at the Data Link Layer (L2) and Differentiated Services Code Point (DSCP) at the Network Layer (L3).

(2) Traffic Prioritization. Priorities were applied in accordance with the CoS listed above. This ensured voice signaling would get the highest level of priority; voice media stream would be prioritized lower than voice signaling but higher than data, and data traffic would receive the lowest priority. At L2, packets were tagged as: Data traffic = 0, Voice media = 5, and Voice Signaling and Network Management = 3. Trust DSCP and trust CoS statements were applied between all ports.

In addition, flooding parameters were set to prevent broadcast and multicast traffic from overwhelming the ports. Broadcast limits were set to 5% and multicast limits were set to 70%. The configuration changes that were made to ensure proper operation can be found on the Telecom Switched Services Interoperability (TSSI) website at http://jitc.fhu.disa.mil/tssi.

(3) QoS. Packets tagged with a CoS of 3 are queued in the high priority queue. The CoS values 5 and 0 are serviced in separate Weighted Round Robin or Shaped Round Robin queues, with 5 receiving a higher weight value therefore, it will be serviced more frequently then 0. These tags were used to identify and separate traffic as it passed through network connections ensuring voice traffic takes precedence over data traffic. For L3 DSCP, packets tagged 0, 5, and 3 were marked 0, 46, and 48 respectively.

(4) Policing. The SUT implemented Class Based Weighted Fair Queuing that uses DSCP values to defines how traffic is treated at each individual network node. DSCP values are used from the L3 IP header.

(5) Virtual LAN (VLAN). The SUT utilized port-based VLANs. Switches within the topology were configured with multiple VLANs using the IEEE 802.1Q tag to separate data from voice traffic. Media Access Control address and Protocol based VLANs were verified through LoC.

(6) IEEE Conformance. All aspects of IEEE conformance were met through the LoC or through testing. All tested results are discussed under their respective topics.

(7) Reliability. In order to meet the requirement for no single point of failure within the network, the SUT must have redundant links configured between all switches that service more than 64 users. To meet this requirement, all links connected between the cores, core and distribution, and between the distribution switches, as shown in figure 2-3, are configured as Port-Channels. Two Gigabit Port-Channels must be configured on all these links. A Gigabit Port-Channel is an aggregation of two one-gigabit fiber ports to form a single two-gigabit fiber link. The two fiber links must be terminated onto separate fiber cards at each switch.

The processors on the 6500 series switches must be configured for Stateful Switch Over (SSO), which is configured under the redundancy command and Non-stop forwarding (NSF), which must be set within the router under Enhanced Interior Gateway Routing Protocol (EIGRP). NSF with SSO is a supervisor redundancy mechanism on the Supervisor Engine 2. NSF works in conjunction with SSO to ensure Layer 3

integrity following a switchover. It allows a router experiencing the failure of an active supervisor to continue forwarding data packets along known routes while the routing protocol information is recovered and validated. NSF relies on the separation of the control plane and the data plane during supervisor switchover. The data plane continues to forward packets based on pre-switchover Cisco Express Forwarding information. The control plane implements graceful restart routing protocol extensions to signal a supervisor restart to NSF-aware neighbor routers, reform its neighbor adjacencies, and rebuild its routing protocol database following a switchover.

The processors on the 4507 series switches must be configured for Route Processor Redundancy (RPR) mode. In the 4507 series, a standby supervisor engine takes over if the primary supervisor engine fails. The standby supervisor engine runs in RPR mode. The standby engine partially boots and keeps synchronized copies of the active configuration. The time needed to bring up the standby supervisor engine and to start handling traffic is shortened to 30 seconds to finish booting and re-establish links. The current code on the 4507 does not support SSO.

The 3750 series switches' processors were tested for fail over at the distribution level in a stacked configuration. During fail over, the primary processor was failed over to the backup processor. The backup processor rebooted causing all FastEthernet ports to reset in 30 seconds. Therefore, the processors did not meet the GSCR requirement that the path through the network shall be restored in 2 seconds. The 3750 series is not certified at the distribution level. Because the 3750 series switches do not meet the GCSR, appendix 3, section A3.3.4.1 reliability standards for dual processors, the 3750 series must be configured in standalone mode and not stacked.

The SUT access switches and access module blades were tested and are certified with the port configuration for the VoIP phones and switch access ports to be configured for 100 Mbps full duplex. Auto-negotiation is not a perfected technology. If configured for auto-negotiation the VoIP phone ports may fail to negotiate properly and this can cause excessive frame loss within the LAN. In order to meet the frame loss requirement, all ports on the access switches must be configured and hard set to 100 Mbps and full duplex.

(8) Network Management. The GSCR, appendix 3, section A3.3.4.2, requires that the vendor provide a management system to monitor the performance of the LAN portion of the VoIP system. Due to numerous third party systems and applications capable of performing this function, this requirement was verified via LoC.

(9) Security. Security requirements in accordance with the GSCR, appendix 3, section A3.3.4.3, were verified using the Information Assurance Test Plan. Results of the security testing are reported in a separate test report generated by the DISA Information Assurance test personnel.

(10) Internet Protocol version 6 (IPv6). This was met through the vendor submission of an LoC with the following minor exception: The vendor has no plan to support IPv6 on the Catalyst 3550. The operational impact is minor.

(11) Traffic Engineering

(a) Links. Two Gigabit Port-Channels were configured between the core switches, between the core and distribution switches, and between the distribution switches. These were configured to separate fiber cards on each switch to ensure proper redundancy. Gigabit Port-Channel is a high-performance Ethernet technology that provides gigabit per second transmission rates. It provides flexible, scalable bandwidth with resiliency and load sharing across links for switches and router interfaces.

Trunk Protocol Negotiation was changed from its default "Desirable" to "Mode on." Configuring the trunk mode as "on" on both sides of the link will allow the trunk to come up without a Dynamic Trunking Protocol negotiation agreement.

(b) Scalability. The SUT can be scaled to meet any number of IP phone subscribers as long as it's composed of the equipment and software listed in Table 2-3 and is consistent with traffic engineering constraints contained in the GSCR, appendix 3. Table 2-4 outlines the maximum number of subscribers that can be supported by link capacity.

Table 2-4. IP Subscriber Supportability by Link Capacity

Link Type	LAN BW	Users
Non-Converged	10 Mbps	64[1]
	100 Mbps	64[1]
	1 Gbps	64[1]
	10 Gbps	64[1]
	10 Mbps LP	100[2]
	100 Mbps LP	1000[2]
	1 Gbps LP	10000[2]
	10 Gbps LP	100000[2]
Converged	10 Mbps	25[3]
	100 Mbps	64[1]
	1 Gbps	64[1]
	10 Gbps	64[1]
	10 Mbps LP	25[3]
	100 Mbps LP	250[4]
	1 Gbps LP	2500[4]
	10 Gbps LP	25000[4]

Table 2-4. IP Subscriber Supportability by Link Capacity (continued)

LEGEND:

BW	- Bandwidth	LAN	- Local Area Network
Gbps	- Gigabits per second	LP	- Link Pair
IP	- Internet Protocol	Mbps	- Megabits per second
kbps	- kilobits per second		

NOTES:

1 For single links, number of users is limited to a maximum of 64 because of single point of failure requirements.
2 The number of users is calculated as bandwidth (BW) divided by 100 kbps per user.
3 The number of users was limited to 64 users per note 1 or 25 percent of total users per note 2, whichever was less.
4 For the converged network, voice traffic was engineered not to exceed 25 percent of total utilization using an estimated 100 kbps per voice call.

(12) LAN Architectures. As shown if figure 2-3, this architecture consists of dual core switches, two distribution switches, and access devices. VLANs were utilized to separate voice and data traffic throughout the converged architecture. The tested LAN was configured at L3 from the core to the access devices; therefore no L2 protocols were used or tested. QoS and CoS for this architecture were discussed earlier in this document. The architecture meets all requirements set forth by GSCR, appendix 3, section A3.3.4.5. EIGRP was implemented between the two core 6509 switches, the 4507R in the distribution layer and the 3750, 3560, and 3550 switches at the access layer. EIGRP integrates the capabilities of link-state protocols into distance-vector protocols. Additionally, EIGRP contains several important protocols that greatly increase its operational efficiency. One of these protocols is the Diffusing Update Algorithm (DUAL). DUAL enables EIGRP routers to determine whether a path advertised by a neighbor is looped or loop-free and allows a router running EIGRP to find alternate paths without waiting on updates from other routers. EIGRP provides capabilities, which include fast convergence, support for variable-length subnet mask, support for partial updates, and support for multiple network layer protocols. A router running EIGRP stores all its neighbors' routing tables so that it can quickly adapt to alternate routes. If no appropriate route exists, EIGRP queries its neighbors to discover an alternate route. These queries propagate until an alternate route is found. EIGRP support for variable-length subnet masks permits routes to be automatically summarized on a network number boundary. In addition, EIGRP can be configured to summarize on any bit boundary at any interface. EIGRP does not make periodic updates. Instead, it sends partial updates only when the metric for a route changes. Propagation of partial updates is automatically bounded so that only those routers that need the information are updated. As a result of these two capabilities, EIGRP consumes significantly less bandwidth than other routing protocols. EIGRP includes support for IP. The IP implementation redistributes routes learned from Open Shortest Path First (OSPF), Routing Information Protocol, Intermediate System-to-Intermediate System, Exterior Gateway Protocol, or Border Gateway Protocol. Only OSPF redistribution was tested during this certification testing.

(a) Delay. In accordance with the GSCR, appendix 3, section A3.3.1.1, the one-way packet delay, the amount of time a packet takes to traverse the network, will be five milliseconds (ms) or less, as measured over a five-minute period. The average one-way delay over 50 five-minute periods, measured between the access and core devices was 1.96 ms.

(b) Jitter. The SUT utilizes a dynamic jitter buffer in the IP phones, which cannot be adjusted. The egress jitter buffer in all gateways was set for a fixed duration of 20 ms. With a 100 percent bandwidth load, the jitter was measured over a 20 minute period with an average of 0.8 ms. The measured jitter met the 5 ms requirement established by section A3.3.1.2, appendix 3 of the GSCR.

(c) Packet Loss. Network packet loss occurs when packets sent are not received at the final destination. The GSCR, appendix 3, section A3.3.1.3, states that LANs shall be engineered so the measured voice packet loss within the LAN shall not exceed 0.05% averaged over any five-minute period. With 100% bandwidth load, the measured packet loss was 0.00% over a 24-hour period.

b. System Interoperability Results. The SUT is certified for joint use within the DSN as an ASVALAN in accordance with the requirements set forth in the GSCR, appendix 3. The system interoperability test summary is shown in table 2-5 and the detailed component interoperability test status is shown table 2-6.

Table 2-5. System Interoperability Test Summary

Device Requirement	Reference	Test Results	Remarks
Delay measured at 5 ms or less	GSCR, Appendix 3, A3.3.1.1	Met	
Jitter measured at less than 5 ms	GSCR, Appendix 3, A3.3.1.2	Met	
Packet Loss less than 0.05%	GSCR, Appendix 3, A3.3.1.3	Met	
Reliability	GSCR, Appendix 3, Section A.3.3.4.1	Met	
IPv6	GSCR, Appendix 3, Section A3.2.8	See note 1.	
Security	GSCR, Appendix 3, A3.2.4	See note 2.	

LEGEND:

DISA	- Defense Information Systems Agency	GSCR	- Generic Switching Center Requirements
DITSCAP	- DoD Information Technology Security Certification and Accreditation Process	IPv6	- Internet Protocol version 6
		ms	- millisecond
DoD	- Department of Defense	SUT	- System Under Test
DSN	- Defense Switched Network		

NOTES:
1 The vendor has no plan to support IPv6 on the Catalyst 3550. The operational impact is minor.
2 Information assurance testing is accomplished via DISA-led Information Assurance test teams and published in a separate report.

12. TEST AND ANALYSIS REPORT. No detailed test report was developed in accordance with the Program Manager's request. JITC distributes interoperability information via the JITC Electronic Report Distribution (ERD) system, which uses Unclassified-But-Sensitive Internet Protocol Router Network (NIPRNet) e-mail. More comprehensive interoperability status information is available via the JITC System Tracking Program (STP). The STP is accessible by .mil/gov users on the NIPRNet at https://stp.fhu.disa.mil. Test reports, lessons learned, and related testing documents and references are on the JITC Joint Interoperability Tool (JIT) at http://jit.fhu.disa.mil (NIPRNet), or http://199.208.204.125 (SIPRNet). Information related to DSN testing is on the TSSI website at http://jitc.fhu.disa.mil/tssi.

Table 2-6. Component Interoperability Test Summary

DSN Line Interfaces					
Interface	**Component[1]**	**Status**	**Device Requirement**	**Test Results**	**Reference**
1000Base FX 100BaseT	Cisco **6509**/6509-NEB/ 6509-NEB-A/6503/6506/ 6513 Catalyst Switches	Certified as: Core Distribution Access	CoS Models	Met	GSCR, Appendix 3, A3.3.2.1
			Traffic Prioritization	Met	GSCR, Appendix 3, A3.3.2.2
			QoS	Met	GSCR, Appendix 3, A3.3.3
			Policing	Met	GSCR, Appendix 3, A3.3.3.2
			VLANs	Met	GSCR, Appendix 3, A3.3.3.3
			IEEE Conformance	Met	GSCR, Appendix 3, A3.3.4
			Reliability	Met	GSCR, Appendix 3, A3.3.4.1
			Network Management	Met	GSCR, Appendix 3, A3.3.4.2
			Security	Met	GSCR, Appendix 3, A3.3.4.3
			IPv6	Met	GSCR, Appendix 3, A3.2.8
			TE	Met	GSCR, Appendix 3, A3.3.4.4
			LAN Architectures	Met	GSCR, Appendix 3, A3.3.4.5
1000Base FX	Cisco **4507R**/4503[2]/4506[2] /4510R Catalyst Switches	Certified as: Distribution	CoS Models	Met	GSCR, Appendix 3, A3.3.2.1
			Traffic Prioritization	Met	GSCR, Appendix 3, A3.3.2.2
			QoS	Met	GSCR, Appendix 3, A3.3.3
			Policing	Met	GSCR, Appendix 3, A3.3.3.2
			VLANs	Met	GSCR, Appendix 3, A3.3.3.3
			IEEE Conformance	Met	GSCR, Appendix 3, A3.3.4
			Reliability	Met[3]	GSCR, Appendix 3, A3.3.4.1
			Network Management	Met	GSCR, Appendix 3, A3.3.4.2
			Security	Met	GSCR, Appendix 3, A3.3.4.3
			IPv6	Met	GSCR, Appendix 3, A3.2.8
			TE	Met	GSCR, Appendix 3, A3.3.4.4
			LAN Architectures	Met	GSCR, Appendix 3, A3.3.4.5

Table 2-6. Component Interoperability Test Summary (continued)

DSN Line Interfaces					
Interface	**Component[1]**	**Status**	**Device Requirement**	**Test Results**	**Reference**
1000Base FX 100BaseT	**Catalyst 3750PoE24/ 3750PoE48** **Catalyst 3560** – PoE 24 **Catalyst 3550** – Inline Power	Certified as: Access	CoS Models	Met	GSCR, Appendix 3, A3.3.2.1
			Traffic Prioritization	Met	GSCR, Appendix 3, A3.3.2.2
			QoS	Met	GSCR, Appendix 3, A3.3.3
			Policing	Met	GSCR, Appendix 3, A3.3.3.2
			VLANs	Met	GSCR, Appendix 3, A3.3.3.3
			IEEE Conformance	Met	GSCR, Appendix 3, A3.3.4
			Reliability	Met	GSCR, Appendix 3, A3.3.4.1
			Network Management	Met	GSCR, Appendix 3, A3.3.4.2
			Security	Met	GSCR, Appendix 3, A3.3.4.3
			IPv6	Met[4]	GSCR, Appendix 3, A3.2.8
			TE	Met	GSCR, Appendix 3, A3.3.4.4
			LAN Architectures	Met	GSCR, Appendix 3, A3.3.4.5

LEGEND:

100BaseT	- IEEE 802.3 100 Mbps Ethernet with Twisted Para Copper
1000BaseFX	- IEEE 802.3 1000 Mbps Ethernet with Fiber Optic Interface
CoS	- Class of Service
DSN	- Defense Switched Network
GSCR	- Generic Switching Center Requirements
IEEE	- Institute of Electrical and Electronics Engineers, Inc.
IOS	- Internetworking Operating System
IPv6	- Internet Protocol version 6
JITC	- Joint Interoperability Test Command
LAN	- Local Area Network
NEB	- Network Equipment Building
PoE	- Power Over Ethernet
QoS	- Quality of Service
TE	- Traffic Engineering
VLAN	- Virtual Local Area Network

NOTES:

1 Components bolded and underlined were tested by JITC. The other components in the family series were not tested; however, they utilize the same IOS software and hardware and JITC analysis determined them to be functionally identical for interoperability certification purposes and they are also certified for joint use.

2 Indicates these switches support one processor and must be configured to fail over to a second distribution switch.

3 This item was not tested and was met through Letter of Compliance.

4 The vendor has no plan to support IPv6 on the Catalyst 3550. The operational impact is minor.