



DEFENSE INFORMATION SYSTEMS AGENCY

P. O. BOX 4502
ARLINGTON, VIRGINIA 22204-4502

IN REPLY REFER TO: Battlespace Communications Portfolio (JTE)

27 Jun 08

MEMORANDUM FOR DISTRIBUTION

SUBJECT: Special Interoperability Test Certification of Cisco 3845 Integrated Services Router Running Internetworking Operating System (IOS) Version 12.4(11)T bundled with the 7600 Family of Routers Running IOS Version 12.2(33)SRB1 System for Internet Protocol Version 6 (IPv6) Capability

References: (a) DoDD 4630.5, "Interoperability and Supportability of Information Technology (IT) and National Security Systems (NSS)," 5 May 2004
(b) CJCSI 6212.01D, "Interoperability and Supportability of Information Technology and National Security Systems," 8 March 2006
(c) through (h), see enclosure 1

1. References (a) and (b) establish the Joint Interoperability Test Command (JITC), as the responsible organization for interoperability test certification.
2. The Cisco 3845 Integrated Services Router (ISR) Running Internetworking Operating System (IOS) Version 12.4(11)T bundled with the 7609 Router Running IOS Version 12.2(33)SRB1 (3845/7609 System) met the Internet Protocol (IP) Version 6 (IPv6) Capable interoperability requirements of an exterior router as described in the Department of Defense (DoD) Information Technology Standards Registry, "DoD IPv6 Standard Profiles for IPv6 Capable Products Version 2.0," 1 August 2007, reference (c). The Cisco 7609 router is architecturally equivalent to other routers within the family (7603-S, 7604, 7606, 7606-S, 7609-S, and 7613) and utilizes the same IOS. Therefore, this certification applies to the Cisco 3845 ISR running IOS Version 12.4(11)T bundled with any router in the Cisco 7600 family running IOS Version 12.2(33)SRB1. The Cisco 3845/7609 System has successfully completed the related IPv6 Interoperability portions of the DoD IPv6 Generic Test Plan (GTP) Version 3, August 2007, reference (d), and is certified for listing on the Unified Capabilities (UC) Approved Products List (APL) as an IPv6 Capable system. This certification expires upon changes that could affect interoperability, but no later than 3 years from the date of this memorandum.

JITC Memo, JTE, Special Interoperability Test Certification of Cisco 3845 Integrated Services Router Running Internetworking Operating System (IOS) Version 12.4(11)T bundled with the 7600 Family of Routers Running IOS Version 12.2(33)SRB1 System for Internet Protocol Version 6 (IPv6) Capability

3. This special certification is based on IPv6 Capable Interoperability testing conducted by JITC at Fort Huachuca, Arizona, and the vendor's Letters of Conformance (LoC) dated 15 November 2007 and 5 June 2008. Interoperability testing commenced on 3 October and went through 2 November 2007 at JITC's Advanced IP Technology Capability. Conformance testing was confirmed by Cisco Systems and was verified in the LoCs Cisco provided. Enclosure 2 documents the summary test results and describes the systems. Users should verify interoperability before deploying the systems in an environment that varies significantly from that described.

4. The system's interoperability status summary is in table 1 and table 2 is the equipment list.

Table 1. Cisco Router System Interoperability Status Summary

Cisco 3845/7609 System		
Functional Category	Requirement	Verified
Base IPv6	M	Yes
IPSec	M	Yes
Transition Mechanisms	M	Yes
Quality of Service	M	Yes
Mobility	CM/CS+	No
Bandwidth Limited Networks	O	No
Network Management	M	Yes
Routing	M	Yes

LEGEND:
 CM Conditional Must IPv6 Internet Protocol Version 6
 CS+ Conditional Should + M Must
 IPSec Internet Protocol Security O Optional
NOTE: The terms Must, Conditional Must, Conditional Should+, and Optional are used to reference specific required Request for Comments from the Internet Engineering Task Force, the Department of Defense Information Technology Standards Registry, and the Department of Defense Internet Protocol Version 6 Generic Test Plan.

Table 2. Cisco Router Equipment Listing

Cisco 3845/7609 System		
Component	Firmware/Software	Interface
Cisco 3845	Cisco IOS Version 12.4(11)T	RJ45 10/100/1000 Mbps Ethernet
Cisco 7609	Cisco IOS Version 12.2(33)SRB1	RJ45 10/100/1000 Mbps Ethernet

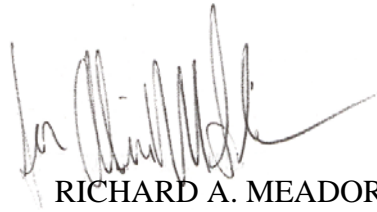
LEGEND:
 IOS Internetworking Operating System RJ Registered Jack
 Mbps Megabits Per Second T New Technology

JITC Memo, JTE, Special Interoperability Test Certification of Cisco 3845 Integrated Services Router Running Internetworking Operating System (IOS) Version 12.4(11)T bundled with the 7600 Family of Routers Running IOS Version 12.2(33)SRB1 System for Internet Protocol Version 6 (IPv6) Capability

5. No detailed test report was written in accordance with the DoD IPv6 Transition Office. 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 IPv6 Capable Interoperability testing is on the UC APL at http://jitc.fhu.disa.mil/adv_ip/register/register.html.

6. The JITC point of contact is Donald L. Hann, DSN 879-0154, commercial (520) 538-5130, or e-mail don.hann@disa.mil.

FOR THE COMMANDER:



RICHARD A. MEADOR

Chief

Battlespace Communications Portfolio

2 Enclosures a/s

JITC Memo, JTE, Special Interoperability Test Certification of Cisco 3845 Integrated Services Router Running Internetworking Operating System (IOS) Version 12.4(11)T bundled with the 7600 Family of Routers Running IOS Version 12.2(33)SRB1 System for Internet Protocol Version 6 (IPv6) Capability

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), MARCORSSYSCOM, 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

DITO, Defense Information Systems Agency (DISA), Attn: GE36, P.O. Box 4502, Arlington, VA 22204-4502

ADDITIONAL REFERENCES

- (c) Department of Defense (DoD) Information Technology Standards Registry (DISR), "DoD Internet Protocol Version 6 (IPv6) Standard Profiles for IPv6 Capable Products Version 2.0," 1 August 2007
- (d) JITC, "DoD IPv6 Generic Test Plan Version 3," August 2007
- (e) DoD IPv6 Transition Office, "DoD IPv6 Master Test Plan, Version 2," September 2006
- (f) DoD Chief Information Officer (CIO) Memorandum, "IPv6," 9 June 2003
- (g) DoD CIO Memorandum, "IPv6 Interim Transition Guidance," 29 September 2003
- (h) DoD, "Defense Information Systems Network (DISN) Global Information Grid (GIG) Convergence Master Plan (GCMP), Version 5.25," 29 March 2006
- (i) NSA, "Evaluation and Implementation of DISA IPv6 Information Assurance Guidance for Milestone Objective 2 Version 2," 30 September 2007

INTERNET PROTOCOL VERSION 6 CAPABLE TESTING SUMMARY

- 1. SYSTEM TITLE.** Cisco 3845 Integrated Services Router (ISR) bundled with 7609 router (3845/7609 System).
- 2. PROPONENT.** Department of Defense (DoD) Internet Protocol (IP) Version 6 (IPv6) Transition Office (DITO).
- 3. PROGRAM MANAGER/USER POC.** DITO, Defense Information Systems Agency (DISA), Attn: GE36 Mark Dugroo, P.O. Box 4502, Arlington, VA 22204-4502, (703) 882-0241, e-mail: mark.dugroo@disa.mil.
- 4. TESTER.** Donald L. Hann, Joint Interoperability Test Command (JITC), P.O. Box 12798, Fort Huachuca, AZ 85670-2798, DSN: 879-5130, commercial: (520) 538-5130, e-mail: don.hann@disa.mil.
- 5. SYSTEM UNDER TEST DESCRIPTION.** The system under test was the Cisco 3845 ISR running Internetworking Operating System (IOS) Version 12.4(11)T bundled with the 7609 router running IOS Version 12.2(33)SRB1 (3845/7609 System) providing IPv6 capability, firewall, IP Security (IPSec) and authentication. The basic function of a router is to direct IP traffic and forward packets from one network to another based on internal routing tables. Routers read each incoming packet and determine how to forward those packets.
- 6. OPERATIONAL ARCHITECTURE.** The operational architecture was the JITC simulated Defense Information Systems Network (DISN) IP Core Network as depicted in figure 2-1.

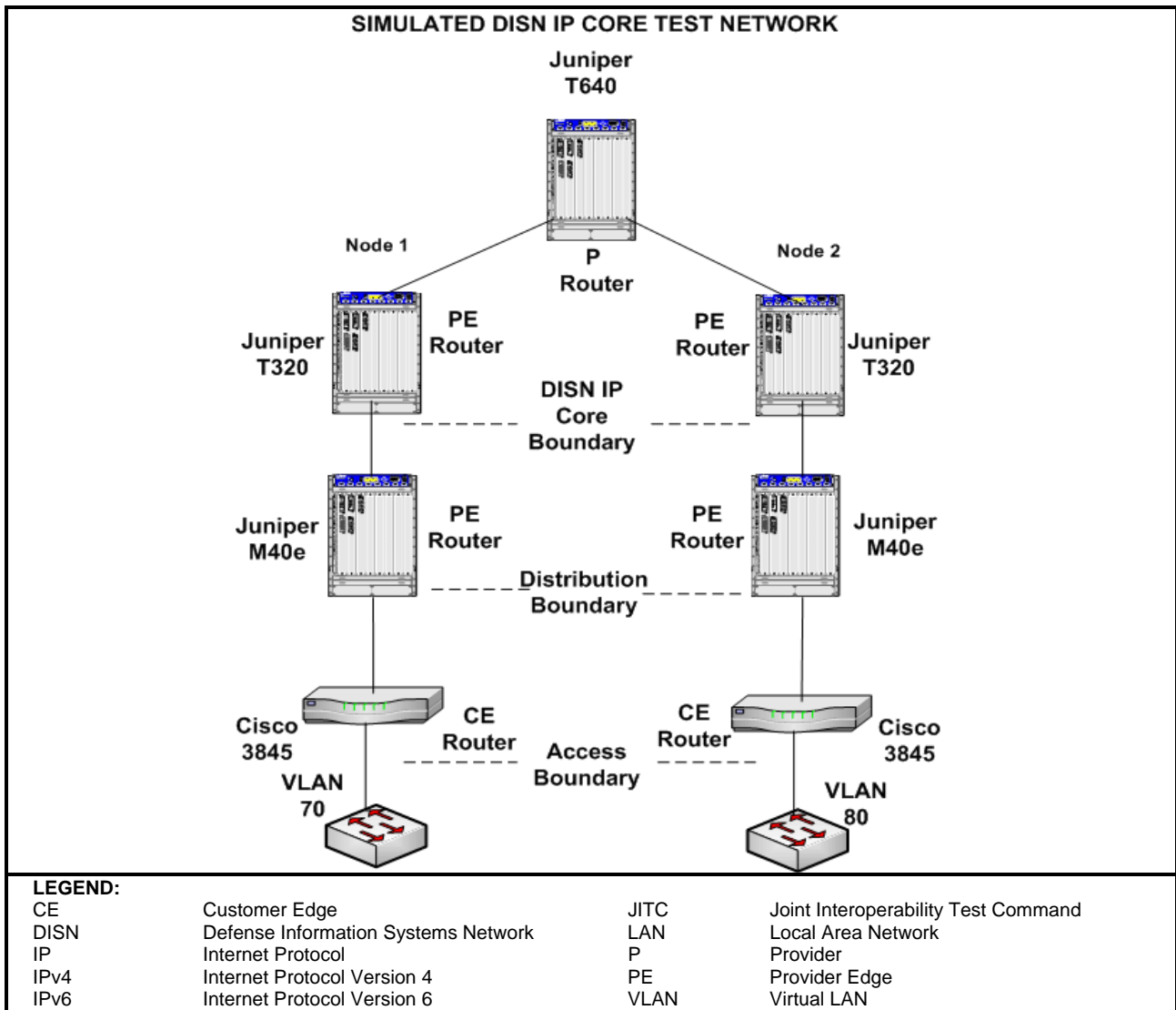


Figure 2-1. JITC Simulated DISN IP Core Network

7. REQUIRED DEVICE INTERFACES. All IPv6-capable products to be included on the Unified Capabilities Approved Products List must meet the requirements of the DoD Information Technology Standards Registry (DISR), “DoD IPv6 Standard Profiles for IPv6 Capable Products Version 2.0,” 1 August 2007. Product testing conducted against these requirements is in accordance with the “DoD IPv6 Generic Test Plan (GTP) Version 3,” August 2007. The IPv6 router profile requirements for conformance and interoperability are in table 2-1.

Table 2-1. IPv6 Capability Requirements and Status

Cisco 3845/7609 System							
RFC	RFC Title	Testing Completed		Router		Implemented	Comments
		Conformance	Interoperability	Requirement	Met/Not Met		
IPv6 Base							
2460	Internet Protocol version 6 (IPv6) Specification	Stated in LoC	Yes	M	Met	Yes	
4443	Internet Control Message Protocol (ICMPv6) for the Internet Protocol Version 6 (IPv6) Specification	Stated in LoC	Yes	M	Met	Yes	
2461	Neighbor Discovery for IP version 6 (IPv6)	Stated in LoC	Yes	M	Met	Yes	
1981	Path Maximum Transmission Unit Discovery for IPv6	Stated in LoC	Yes	M	Met	Yes	
2462	IPv6 Stateless Address Auto configuration	Stated in LoC	Yes	M	Met	Yes	Note 1
3315	DHCPv6 (Client)	Stated in LoC	Yes	M	Met	Yes	Note 1
4291	IPv6 Addressing Architecture	Stated in LoC	Yes	M	Met	Yes	
4007	IPv6 Scoped Address Architecture	Stated in LoC	Yes	M	Met	Yes	
4193	Unique Local IPv6 Unicast Addresses	Stated in LoC	Yes	M	Met	Yes	
2710	Multicast Listener Discovery (MLD)	Stated in LoC	Yes	M	Met	Yes	
3810	Multicast Listener Discovery Version 2 (MLDv2) for IPv6	Stated in LoC	Yes	M	Met	Yes	
2464	Transmission of IPv6 Packets over Ethernet Networks	Stated in LoC	Yes	CM	Met	Yes	
IPSec							
2401	Security Architecture for the Internet Protocol	Stated in LoC	Yes	M	Met	Yes	
2402	IP Authentication Header	Stated in LoC	Yes	M	Met	Yes	
2406	IP Encapsulating Security Payload (ESP)	Stated in LoC	Yes	M	Met	Yes	
2407	Internet Key Exchange Version 1 (IKEv1) protocol	Stated in LoC	Yes	M	Met	Yes	
2408	Internet Security Association and Key Management Protocol (ISAKMP)	Stated in LoC	Yes	M	Met	Yes	
2409	The Internet Key Exchange (IKE)	Stated in LoC	Yes	M	Met	Yes	
4109	Algorithms for Internet Key Exchange Version 1	Stated in LoC	Yes	M	Met	Yes	
4301	Security Architecture for the Internet Protocol	Not Stated	Not Tested	M	Not Tested	No	Note 2
4302	IP Authentication Header	Stated in LoC	Yes	M	Met	Yes	
4303	IP Encapsulating Security Payload (ESP)	Not Stated	Not Tested	M	Not Tested	No	Note 2

Table 2-1. IPv6 Capability Requirements and Status (continued)

Cisco 3845/7609 System							
RFC	RFC Title	Testing Completed		Router		Implemented	Comments
		Conformance	Interoperability	Requirement	Met/Not Met		
4304	Extended Sequence Number (ESN) Addendum to IPsec Domain of Interpretation (DOI) for Internet Security Association and Key Management Protocol (ISAKMP)	Not Stated	Not Tested	S	Not Tested	No	
4305	Cryptographic Algorithm Implementation Requirements for Encapsulating Security Payload (ESP) and Authentication Header (AH)	Stated in LoC	Yes	M	Met	Yes	Note 2
4869	Suite B Cryptographic Suites for IPsec	Not Stated	Not Tested	S+	Not Tested	No	
4309	Using Advanced Encryption Standard (AES) CCM Mode with IPsec Encapsulating Security Payload (ESP)	Not Stated	Not Tested	CS	Not Tested	No	
3971	Secure Neighbor Discovery	Not Stated	Not Tested	S	Not Tested	No	
3972	Cryptographically Generated Addresses	Not Stated	Not Tested	S	Not Tested	No	
3041	Privacy Extensions for Stateless Address Auto configuration in IPv6	Stated in LoC	Yes	S+/CM	Met	Yes	
4306	Internet Key Exchange (IKEv2) Protocol	Not Stated	Not Tested	M	Not Tested	No	Note 2
4307	Cryptographic Algorithms for Internet Key Exchange Version 2 (IKEv2)	Not Stated	Not Tested	M	Not Tested	No	Note 2
4308	Cryptographic Suites for IPsec	Stated in LoC	Yes	M	Met	Yes	
Transition Mechanisms							
4213	Transition Mechanisms for IPv6 Host and Routers	Stated in LoC	Yes	M	Met	Yes	
2766	Network Address Translation – Protocol Translation (NAT-PT)	Not Stated	Not Tested	SN	Not Tested	No	
3053	IPv6 Tunnel Broker	Not Stated	Not Tested	CS	Not Tested	No	
QoS							
2474	Definition of the Differentiated Services Field (DS Field) in the IPv4 and IPv6 Headers	Stated in LoC	Yes	M	Met	Yes	
2205	Resource ReSerVation Protocol (RSVP) – Version 1 Functional Specification	Not Stated	Not Tested	S+	Not Tested	No	
2207	RSVP Extensions for IPSEC Data Flows	Not Stated	Not Tested	S+	Not Tested	No	
2210	The Use of RSVP with IETF Integrated Services	Not Stated	Not Tested	S+	Not Tested	No	
2750	RSVP Extensions for Policy Control	Not Stated	Not Tested	S+	Not Tested	No	
3175	Aggregation of RSVP for IPv4 and IPv6 Reservations	Not Stated	Not Tested	O	Not Tested	No	

Table 2-1. IPv6 Capability Requirements and Status (continued)

Cisco 3845/7609 System							
RFC	RFC Title	Testing Completed		Router		Implemented	Comments
		Conformance	Interoperability	Requirement	Met/Not Met		
Mobility							
3775	Mobility Support in IPv6	Not Stated	Not Tested	CM	Not Tested	No	
3776	Using IPsec to Protect Mobile IPv6 Signaling Between Mobile Nodes and Home Agents	Not Stated	Not Tested	CS+	Not Tested	No	
4282	The Network Access Identifier	Not Stated	Not Tested	CM	Not Tested	No	
4283	Mobile Node Identifier Option for Mobile IPv6 (MIPv6)	Not Stated	Not Tested	CS+	Not Tested	No	
3963	Network Mobility (NEMO) Basic Support Protocol	Not Stated	Not Tested	CM	Not Tested	No	
Bandwidth Limited Networks							
3095	Robust Header Compression (RoHC)	Not Stated	Not Tested	O	Not Tested	No	
3241	RoHC over PPP	Not Stated	Not Tested	O	Not Tested	No	
3843	RoHC: A Compression Profile for IP	Not Stated	Not Tested	O	Not Tested	No	
4362	RoHC: A Link-Layer Assisted Profile for IP/UDP/RTP	Not Stated	Not Tested	O	Not Tested	No	
2507	IP Header Compression	Not Stated	Not Tested	O	Not Tested	No	
2508	Compressing IP/UDP/RTP Headers for Low-Speed Serial Links	Not Stated	Not Tested	O	Not Tested	No	
Network Management							
3411	An Architecture for Describing Simple Network Management Protocol Version 3 (SNMPv3)	Stated in LoC	Yes	M	Met	Yes	
3412	Message Processing and Dispatching for the SNMP	Stated in LoC	Yes	M	Met	Yes	
3413	SNMP Applications	Stated in LoC	Yes	M	Met	Yes	
3595	Textual Conventions for IPv6 Flow Label	Stated in LoC	Not Tested	M	Not Tested	Yes	Note 3
4022	Management Information Base for the Transmission Control Protocol	Stated in LoC	Not Tested	M	Not Tested	Yes	Note 3
4113	Management Information Base for the User Datagram Protocol	Stated in LoC	Not Tested	M	Not Tested	Yes	Note 3
4087	IP Tunnel MIB	Stated in LoC	Not Tested	M	Not Tested	Yes	Note 3
4293	Management Information Base (MIB) for IP	Stated in LoC	Not Tested	M	Not Tested	Yes	Note 3
4295	Mobile IP Management MIB	Not Stated	Not Tested	CM	Not Tested	No	Note 3
4807	IPsec Security Policy Database Configuration	Not Stated	Not Tested	CM	Not Tested	No	Note 3
4292	IP Forwarding Table MIB	Stated in LoC	Not Tested	M	Not Tested	Yes	Note 3

Table 2-1. IPv6 Capability Requirements and Status (continued)

Cisco 3845/7609 System							
RFC	RFC Title	Testing Completed		Router		Implemented	Comments
		Conformance	Interoperability	Requirement	Met/Not Met		
Routing							
2784	Generic Routing Encapsulation (GRE)	Stated in LoC	Yes	M	Met	Yes	
2473	Generic Packet Tunneling in IPv6 Specification	Stated in LoC	Yes	M	Met	Yes	
4601	Protocol Independent Multicast - Sparse Mode (PIM-SM): Protocol Specification (Revised)	Not Stated	Not Tested	CS+	Not Met	No	
3973	Protocol Independent Multicast - Dense Mode (PIM-DM): Protocol Specification (Revised)	Not Stated	Not Tested	CS+	Not Met	No	
2740	OSPF for IPv6 (OSPFv3)	Stated in LoC	Yes	CM	Met	Yes	
4552	Authentication/Confidentiality for OSPFv3	Not Stated	Not Tested	CS+	Not Met	No	
4271	A Border Gateway Protocol 4 (BGP-4)	Stated in LoC	Yes	CM	Met	Yes	
1772	Application of the Border Gateway Protocol in the Internet	Stated in LoC	Yes	CM	Met	Yes	
2545	Border Gateway Protocol Extensions for IPv6 Interdomain Routing	Stated in LoC	Yes	CM	Met	Yes	
2858	Multiprotocol Extensions for BGP-4	Stated in LoC	Yes	CM	Met	Yes	
LEGEND:							
CBC	Cipher Block Chaining		MAC	Message Authentication Code			
CCM	CBC MAC Mode		MIB	Management Information Base			
CM	Conditional Must		NAT	Network Address Translation			
CS	Conditional Should		O	Optional (May)			
CS+	Conditional Should+		OSPF	Open Shortest Path First			
DHCPv6	Dynamic Host Configuration Protocol Version 6		PPP	Point-to-Point Protocol			
DNS	Domain Name Service		QoS	Quality of Service			
DoD	Department of Defense		RFC	Request for Comment			
FTP	File Transfer Protocol		RoHC	Robust Header Compression			
IETF	Internet Engineering Task Force		RSVP	Resource ReSerVation Protocol			
IKEv2	Internet Key Exchange Version 2		RTP	Real-Time Transport Protocol			
IP	Internet Protocol		S	Should			
IPSec	Internet Protocol Security		SLAAC	Stateless Address Auto-configuration			
IPv4	Internet Protocol Version 4		SN	Should Not			
IPv6	Internet Protocol Version 6		S+	Should+			
LoC	Letter of Conformance		UDP	User Datagram Protocol			
M	Must						
NOTES:							
1. All Products must support a method of autonomous configuration, either SLAAC or DHCPv6.							
2. These devices were granted a waiver for IKEv2; therefore, they are not required to support IKEv2 and the 4301 architecture.							
3. Interoperability was not tested due to the lack of network management implementations for IPv6.							
4. The terms Must, Conditional Must, Should, Should+, Conditional Should, Conditional Should +, Should Not, and Optional are used to reference specific required RFCs from the IETF, the DoD Information Technology Standards Registry, and the DoD IPv6 Generic Test Plan.							

8. TEST NETWORK DESCRIPTION. The 3845/7609 System was tested as part of the JITC simulated DISN IP Core Network test architecture incorporating DoD Master Test Plan Milestone Objective 2 (MO2) dual stack test enclave architecture managed by the Advanced IP Technology Capability. Figure 2-2 shows the 3845/7600 System configuration that was inserted into the JITC simulated DISN IP Core Network. Primary APL testing was conducted via the DISN IP Core Network architecture, while functional testing of the Cisco ISR firewall capabilities was achieved through monitoring communications across the MO2 enclave test segment in accordance with National Security Agency (NSA), "Evaluation and Implementation of DISA IPv6 Information Assurance Guidance for Milestone Objective 2 Version 2," 30 September 2007.

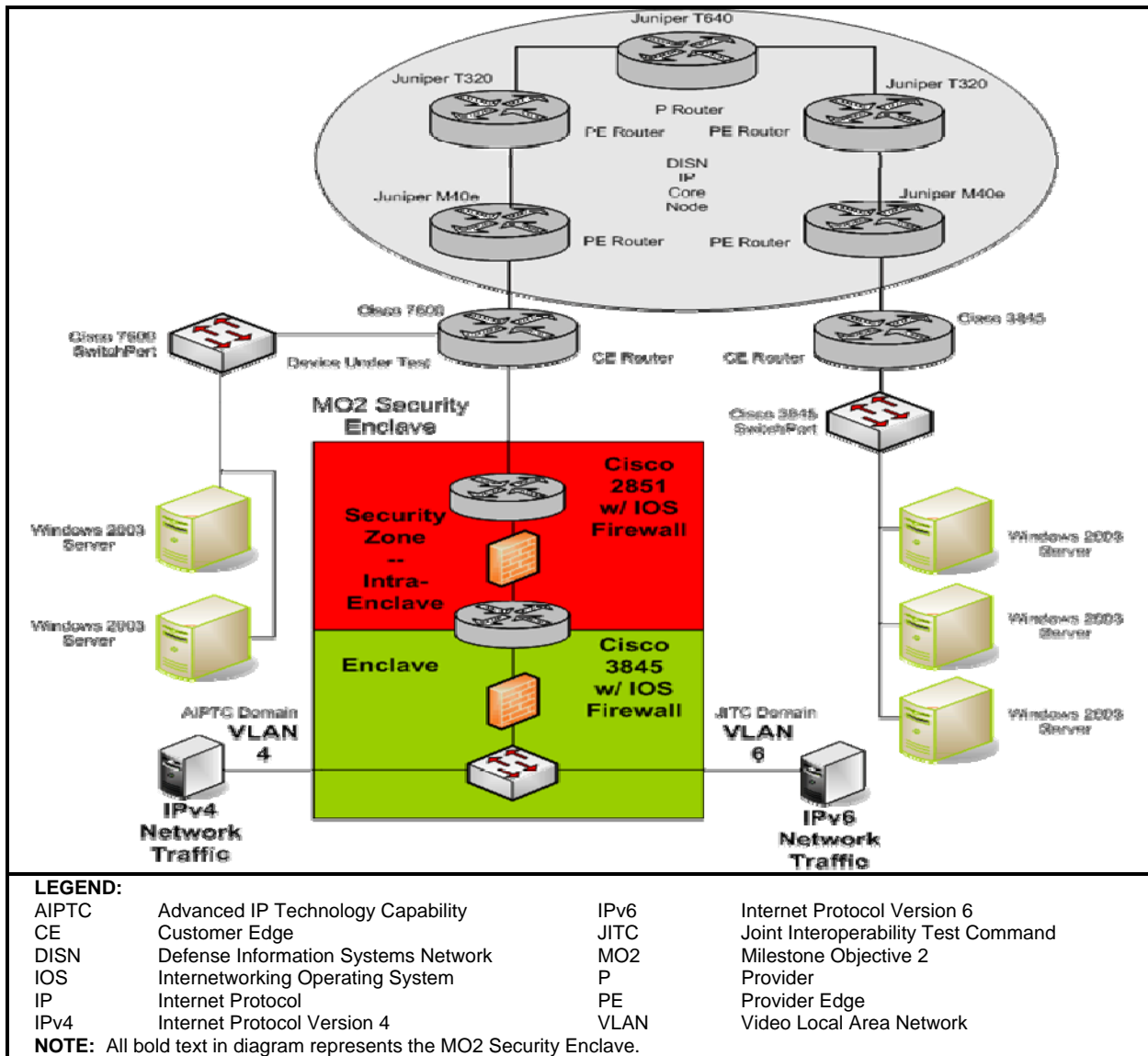


Figure 2-2. 3845/7609 System Test Network

9. DEVICE CONFIGURATIONS. Table 2-2 provides hardware and software components used in the test network.

Table 2-2. Test Configuration Hardware and Software

Equipment Name	Model Number	IOS/OS/Version(s)
Hardware		
3845/7600 System	Cisco 3845 ISR	12.4(11)T
	Cisco 7609	12.2(33)SRB1
Cisco Router	Cisco 3845 ISR	12.4(11)T
Cisco Router	Cisco 2851	12.4(11)T
Juniper Router	Juniper M40e	V 7.6R3.6
Juniper Router	Juniper M40e	V 7.6R3.6
Juniper Router	Juniper T320	V 7.5R4.4
Juniper Router	Juniper T320	V 7.5R4.4
Juniper Router	Juniper T640	V 7.5R4.4
5 Dell Power Edge Servers	2850	MS 2003 Server
2 Gateway Notebooks	450ROG	Windows XP Professional
Gateway Workstation	E Series	Windows XP Professional
Software		
Windows XP Professional	N/A	Build 5.1.2600 SP2
Windows Server 2003	N/A	Build 5.2.3790 SP1
SimpleTesterPro	N/A	V11.0.1
VLC Media Player	N/A	V0.8.6b
Wireshark	N/A	V.0.99.2
LEGEND:		
IOS	Internetworking Operating System	R Release
ISR	Integrated Services Router	SP Service Pack
LAN	Local Area Network	T New Technology
MS	Microsoft	V Version
N/A	Not Applicable	VLC VideoLAN Client
OS	Operating System	

10. TEST LIMITATIONS. A discrepancy was noted in the DoD IPv6 Standard Profiles for IPv6 Capable Products Version 2.0,” 1 August 2007. The lack of firewall specific requirements caused the JITC to develop its own functionality based test case in accordance with the NSA document.

11. TEST RESULTS.

a. IPv6 Base.

Test Case C.1.2. The RFC 2460 IPv6 Specification is the base specification of the IPv6 protocol. It specifies a number of parameters that enable successful completion of IPv6 traffic addressing and control. The Cisco 3845/7609 System met the test requirements.

Test Case C.1.14. The RFC 4443 identifies Internet Control Message Protocol messages for the IPv6 protocol. It includes message format and identifies two types of messages: error and informational. The Cisco 3845/7609 System met the test requirements.

Test Case C.1.3. The RFC 2461 Neighbor Discovery for IPv6 specifies the neighbor discovery function that is similar to address resolution protocol in IP Version 4 (IPv4). It is necessary for implementing neighbor solicitations and neighbor advertisements within IPv6. The Cisco 3845/7609 System met the test requirements.

Test Case C.1.1. The RFC 1981 Path Maximum Transmission Unit Discovery for IPv6 is necessary for proper IPv6 implementations. It acts as a mechanism to determine the maximum size of packets to traverse the network without fragmentation. The Cisco 3845/7609 System met the test requirements.

Test Case C.1.4. The RFC 2462 IPv6 Stateless Address Auto-configuration specifies how a host auto-configures its interfaces in IPv6. These steps include determining whether the source addressing should be stateless or stateful, whether the information obtained should be solely the address or include other information, and Duplicate Address Detection. The Cisco 3845/7609 System met the test requirements.

Test Case C.3.8. The RFC 3315 DHCP for IPv6 (DHCPv6) specifies the use of an enabled DHCP server passing configuration parameters such as IPv6 network addresses to IPv6 nodes. The Cisco 3845/7609 System met the test requirements.

Test Case C.1.13. The RFC 4291 IPv6 Addressing Architecture defines the specifications for the addressing architecture of the IPv6 protocol. The definitions cover unicast addresses, anycast addresses, and multicast addresses. The Cisco 3845/7609 System met the test requirements.

Test Case C.1.11. The RFC 4007 IPv6 Scoped Address Architecture defines the nature and characteristics for the usage of IPv6 addresses of different scopes. The Cisco 3845/7609 System met the test requirements.

Test Case C.1.12. The RFC 4193 Unique Local IPv6 Unicast Addresses defines the address format and how it is globally unique. Local IPv6 unicast addressing is intended to be used for local communications and is not expected to be routed to the Internet. The Cisco 3845/7609 System met the test requirements.

Test Case C.1.8. The RFC 2710 Multicast Listener Discovery (MLD) for IPv6 specifies the protocol used by an IPv6 router to discover the presence of multicast listeners (i.e., nodes wishing to receive multicast packets) on its directly attached links, and to discover specifically which multicast addresses are of interest to those neighboring nodes. The Cisco 3845/7609 System met the test requirements.

Test Case C.1.10. The RFC 3810 MLD Version 2 is used by IPv6 routers to discover the presence of multicast listeners on their directly attached links, and to discover specifically which multicast addresses are interests to those neighboring node. The Cisco 3845/7609 System met the test requirements.

Test Case C.1.5. The RFC 2464 Transmission of IPv6 Packets over Ethernet Networks specifies the frame format for transmission of IPv6 link-local addresses and statelessly auto-configured addresses on Ethernet networks. The Cisco 3845/7609 System met the test requirements.

b. IPsec.

Test Case C.2.1. The RFC 2401 Security Architecture for the IP specifies the base architecture for IPsec compliant systems. The Cisco 3845/7609 System met the test requirements.

Test Case C.2.2. The RFC 2402 IP Authentication Header (AH) is used to provide connectionless integrity and data origin authentication for IP datagrams to provide protection against replays. The Cisco 3845/7609 System met the test requirements.

Test Case C.2.3. The RFC 2406 IP Encapsulating Security Payload (ESP) headers are designed to provide a mix of security services in IPv4 and IPv6. The ESP may be applied alone, in combination with the IP AH, or in a nested fashion (e.g., through the use of tunnel mode). The Cisco 3845/7609 System met the test requirements.

Test Case C.2.4. The RFC 2407 Internet Security Association and Key Management Protocol (ISAKMP) defines a framework for security association management and cryptographic key establishment for the Internet. This framework consists of defined exchanges, payloads, and processing guidelines that occur within a given Domain of Interpretation. The Cisco 3845/7609 System met the test requirements.

Test Case C.2.4. The RFC 2408 ISAKMP describes a protocol utilizing security concepts necessary for establishing Security Associations (SA) and cryptographic keys in an Internet environment. The Cisco 3845/7609 System met the test requirements.

Test Case C.2.4. The RFC 2409 Internet Key Exchange (IKE) describes a protocol using part of Oakley and part of Secure Key Exchange Mechanism in conjunction with ISAKMP to obtain authenticated keying material for use with ISAKMP, and for other SAs such as AH and ESP for Internet Engineering Task Force IPsec Domain of Interpretation. The Cisco 3845/7609 System met the test requirements.

Test Case C.2.2. The RFC 4302 IP AH is used to provide connectionless integrity and data origin authentication for IP datagrams and to provide protection against replays. The Cisco 3845/7609 System met the test requirements.

Test Case C.2.8. The RFC 4109 Algorithms for IKE Version 1 updates the original IKEv1 definition (RFC 2409) and requires SHA-1 for hashing and HMAC functions, Pre-shared secrets for authentication, and Diffie-Hellman Modern Programming Practice MODP group 2 as Musts. The Cisco 3845/7609 System met the test requirements.

Test Case C.2.4. The RFC 4305 Cryptographic Algorithm Implementation Requirements for ESP and AH defines the ability to successfully establish IPsec utilizing all of the required encryption and authentication algorithms. The DUT was able to communicate over the established IPsec links using IPv6. The Cisco 3845/7609 System met the test requirements.

Test Case C.2.7. The RFC 4308 Cryptographic Suites for IPsec suites should not be considered extensions to IPsec, IKE, and IKEv2, but instead administrative methods for describing sets of configurations. The IPsec, IKE, and IKEv2 protocols rely on security algorithms to provide privacy and authentication between the initiator and responder. The Cisco 3845/7609 System met the test requirements.

c. Transition Mechanisms.

Test Case C.3.19. The RFC 4213 Transition Mechanisms for IPv6 Host and Routers specifies IPv4 co-existence mechanisms that can be implemented by IPv6 devices. The Cisco 3845/7609 System met the test requirements.

d. Quality of Service.

Test Case C.3.3. The RFC 2474 Definition of the Differentiated Services (DiffServ) Field in the IPv4 and IPv6 Headers defines the DiffServ field. In IPv4, it defines the layout of the Type-of-Service octet and in IPv6, the Traffic Class octet. In addition, a base set of packet forwarding treatments, or per-hop behaviors, is defined. The Cisco 3845/7609 System met the test requirements.

e. Network Management.

Test Case C.3.10. The RFC 3411 An Architecture for Describing SNMP Management Frameworks is designed to be modular to allow the evolution of the SNMP protocol standards over time. The major portions of the architecture are an SNMP engine containing a Message Processing Subsystem, a Security Subsystem, and an Access Control Subsystem, and possibly multiple SNMP applications, which provide specific functional processing of management data. The Cisco 3845/7609 System met the test requirements.

Test Case C.3.11. The RFC 3412 Message Processing and Dispatching for the SNMP describes the Message Processing and Dispatching for SNMP messages within the SNMP architecture. It defines the procedures for dispatching potentially multiple versions of SNMP messages to the proper SNMP Message Processing Models, and for dispatching Protocol Data Units to SNMP applications. The Cisco 3845/7609 System met the test requirements.

Test Case C.3.12. The RFC 3413 SNMP Applications describes five types of SNMP applications which make use of an SNMP engine as described in Standard 62, RFC 3411. The types of application described are Command Generators, Command Responders, Notification Originators, Notification Receivers, and Proxy Forwarders. The Cisco 3845/7609 System met the test requirements.

Testing the Management Information Base (MIB) requirements was preformed by using an automated tool suite called SimpleTesterPro. The test suite includes Syntax, MIB-II Semantic, RMON Semantic, SNMPv3 Semantic, Diffie-Hellman Semantic, and performance tests.

f. Router.

Test Case C.3.6. The RFC 2784 Generic Routing Encapsulation is a protocol for encapsulation of an arbitrary Network Layer Protocol (NLP) over another arbitrary NLP when a system has a payload packet that needs to be encapsulated and delivered to some destination. The Cisco 3845/7609 System met the test requirements.

Test Case C.3.2. The RFC 2473 Generic Packet Tunneling in IPv6 Specification defines the model and generic mechanisms for IPv6 encapsulation of IPv6 and IPv4 packets. The model and mechanisms can be applied to other protocol packets such as AppleTalk, Internetwork Packet Exchange (IPX), Connectionless Network Protocol, and/or others. The Cisco 3845/7609 System met the test requirements.

Test Case C.3.5. The RFC 2740 Open Shortest Path First (OSPF) for IPv6 handles the increased address size of IPv6. The fundamental mechanisms of OSPF (flooding, Designated Router election, OSPF area support, Shortest Path First algorithms) remain unchanged. However, addressing semantics have been removed from OSPF packets and the basic Link State Advertisements (LSA). New LSAs were created to carry IPv6 addresses and prefixes. The OSPF now runs on a per-link basis, instead of on a per-IP-subnet basis. The Cisco 3845/7609 System met the test requirements.

Test Case C.3.20. The RFC 4271 Border Gateway Protocol (BGP) Version 4 (BGP-4) is capable of carrying routing information only for IPv4. This RFC defines extensions to BGP-4 to enable it to carry routing information for multiple NLPs (e.g., IPv6 or IPX). The extensions are backward compatible - a router that supports the extensions can interoperate with a router that does not support the extensions. The Cisco 3845/7609 System met the test requirements.

Test Case C.3.1. The RFC 1772 Application of the BGP in the Internet is an inter-Autonomous System routing protocol. Based on performance, preference, and policy constraints, the network reachability information exchanged via BGP provides sufficient information to detect routing loops and enforce routing decisions. The Cisco 3845/7609 System met the test requirements.

Test Case C.3.4. The RFC 2545 BGP Extensions for IPv6 Interdomain Routing describes two BGP attributes (MP_REACH_NLRI and MP_UNREACH_NLRI) that can be used to announce and withdraw the announcement of reachability information. The RFC defines how systems should make use of these attributes for conveying IPv6 routing information. The Cisco 3845/7609 System met the test requirements.

Test Case C.3.20. The RFC 2858 Multiprotocol Extensions for BGP-4 allows the use of extensions to enable BGP-4 to carry routing information for multiple NLP (e.g., IPv6 or IPX). A router that supports the extensions can interoperate with a router that does not support the extensions thus making the extensions backward compatible. The Cisco 3845/7609 System met the test requirements.

g. Conclusion. Cisco 3845/7609 System met all the required RFCs and routed traffic properly within the IPv6 MO2 enclave architecture.

12 TEST AND ANALYSIS REPORT. No detailed test report was written in accordance with the DITO. All test data is maintained in the Advanced IP Technology Capability and is available upon request. This certification is available on the Joint Interoperability Tool (JIT). The JIT homepage is <http://jit.fhu.disa.mil> (NIPRNet), or <http://199.208.204.125/> (SIPRNet). The JIT has links to JITC interoperability documents to provide the DoD community, including the warfighter in the field, easy access to the latest interoperability information. System 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/>.