



DEFENSE INFORMATION SYSTEMS AGENCY

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

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

3 Dec 08

MEMORANDUM FOR DISTRIBUTION

SUBJECT: Special Interoperability Test Certification of the IBM z/OS Version 1.10 Operating System for IBM Mainframe Computer Systems for Internet Protocol Version 6 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 IBM z/OS Version 1.10 operating system for IBM mainframe computer systems has met the Internet Protocol (IP) Version 6 (IPv6) Capable interoperability requirements of an Advanced Server 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 IBM z/OS Version 1.10 operating system for IBM mainframe computer systems 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 IPv6 Capable. This certification expires upon changes that could affect interoperability, but no later than 3 years from the date of this memorandum.
3. This special certification is based on IPv6 Capable Interoperability testing conducted by JITC at Fort Huachuca, Arizona, and the vendor's Letter of Conformance (LoC) dated 8 February 2008. Interoperability testing was conducted from 6 through 24 October 2008 at JITC's Advanced IP Technology Capability. Conformance testing was confirmed by IBM and was verified in the LoC provided. Enclosure 2 documents the summary test results and describes the devices. Users should verify interoperability before deploying the devices in an environment that varies significantly from that described.
4. The device's interoperability status summary is in Table 1, and Table 2 contains the equipment listing.

JITC Memo, JTE, Special Interoperability Test Certification of the IBM z/OS Version 1.10 Operating System for IBM Mainframe Computer Systems for Internet Protocol Version 6 Capability

Table 1. Interoperability Status Summary

IBM z/OS		
Functional Category	Requirement	Verified
Base IPv6	M	Yes
IPSec	M	Yes
Transition Mechanisms	S	Yes
Quality of Service	O	No
Mobility	CM	No
Bandwidth Limited Networks	O	No
Server	O	Yes
Host	M	Yes
LEGEND:		
CM	Conditional Must	M Must
IPSec	Internet Protocol Security	O Optional
IPv6	Internet Protocol Version 6	S Should
NOTE: The terms Conditional Must, Must, Should, Should+, and Optional are used to reference specifically 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. Equipment Listing

IBM z/OS		
Component	Firmware/Software	Interface
IBM z/OS	Version 1.10	RJ45 100 Mbps Ethernet
LEGEND:		
Mbps	Megabits Per Second	RJ Registered Jack

5. No detailed test report was written in accordance with the Assistant Secretary of Defense-Networks Information and Integration. 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 testing is on the UC APL at http://jitc.fhu.disa.mil/adv_ip/register/register.html.

JITC Memo, JTE, Special Interoperability Test Certification of the IBM z/OS Version 1.10
Operating System for IBM Mainframe Computer Systems for Internet Protocol Version 6
Capability

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

FOR THE COMMANDER:



for RICHARD A. MEADOR
Chief
Battlespace Communications Portfolio

2 Enclosures a/s

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

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

IBM, Attn: Marianne Mostachetti, 2455 South Road, M/S P328, Poughkeepsie, New York 12601

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) Defense Information Systems Agency, Joint Interoperability Test Command, "DoD IPv6 Generic Test Plan Version 3," August 2007
- (e) DoD Chief Information Officer (CIO) Memorandum, "IPv6," 9 June 2003
- (f) DoD CIO Memorandum, "IPv6 Interim Transition Guidance," 29 September 2003
- (g) DoD IPv6 Transition Office, "DoD IPv6 Master Test Plan, Version 2," September 2006
- (h) DoD, "DISR Global Information Grid (GIG) Convergence Master Plan (GCMP), Version 5.25," 29 March 2006

INTERNET PROTOCOL VERSION 6 CAPABLE TESTING SUMMARY

1. **SYSTEM TITLE.** The IBM z/OS Version 1.10, hereafter referred to as the device under test (DUT).
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 Sam Assi, P.O. Box 4502, Arlington, VA 22204-4502, (703) 882-0241, e-mail: sam.assi@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. **DEVICE UNDER TEST DESCRIPTION.** The DUT is the premier operating system for IBM mainframe computer systems.
6. **OPERATIONAL ARCHITECTURE.** The operational architecture was the JITC simulated Defense Information Systems Network (DISN) IP Core Network as depicted in Figure 2-1.
7. **REQUIRED DEVICE INTERFACES.** All IPv6-capable products to be included on the Unified Capabilities Approved Product 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 Advanced Server profile requirements for conformance and interoperability are in Table 2-1.

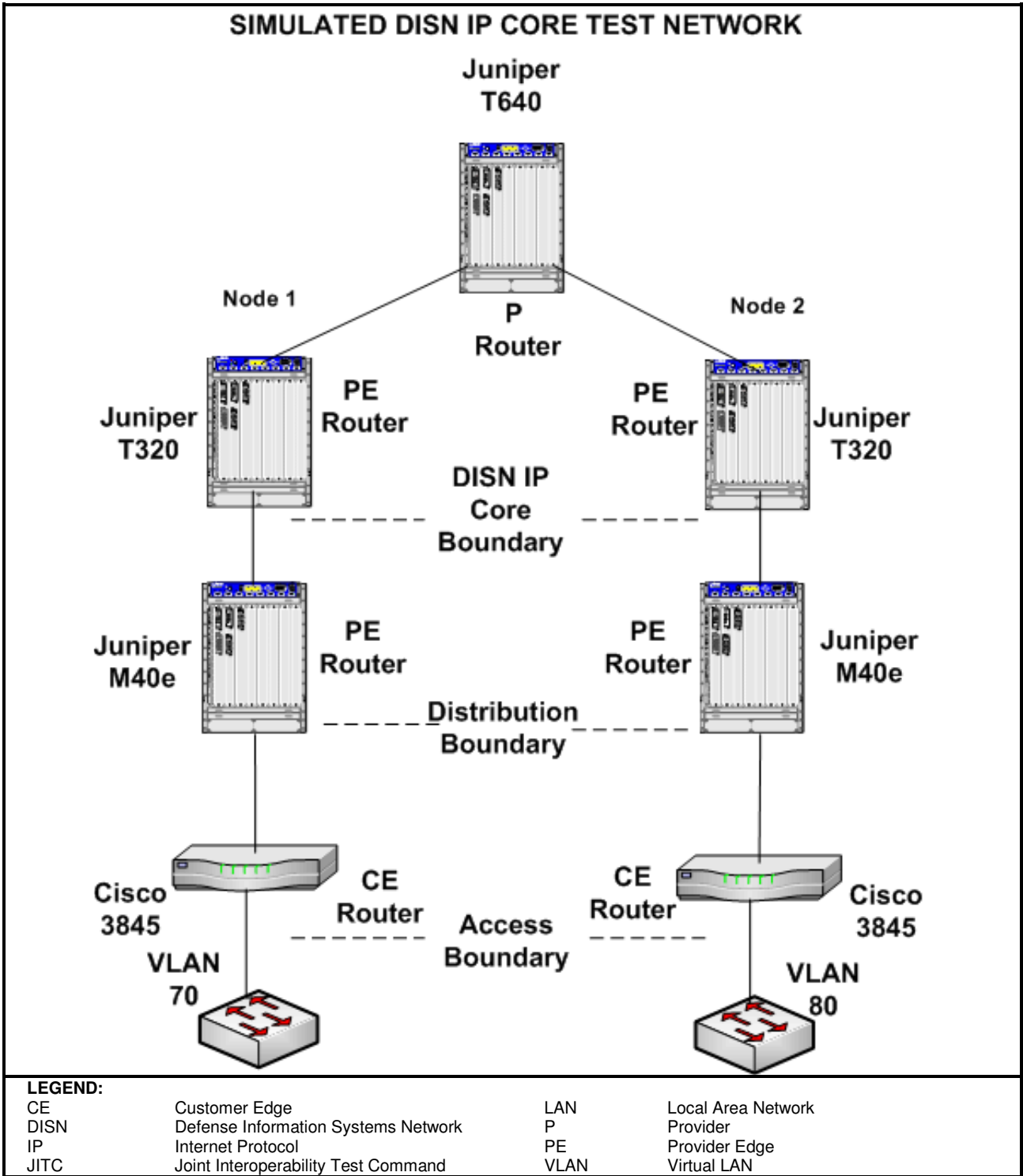


Figure 2-1. JITC Simulated DISN IP Core Network

Table 2-1. IPv6 Capability Requirements and Status

IBM z/OS							
RFC	RFC Title	Testing Completed		Advanced Server		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)	Not Stated	Not Tested	M	Not Tested	No	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							
4301	Security Architecture for the Internet Protocol	Stated in LoC	Yes	M	Met	Yes	
4302	IP Authentication Header	Stated in LoC	Yes	S	Met	Yes	
4303	IP Encapsulating Security Payload (ESP)	Stated in LoC	Yes	M	Met	Yes	
4304	Extended Sequence Number (ESN) Addendum to IPsec Domain of Interpretation (DOI) for Internet Security Association and Key Management Protocol (ISAKMP)	Stated in LoC	Yes	S	Met	Yes	
4305	Cryptographic Algorithm Implementation Requirements for Encapsulating Security Payload (ESP) and Authentication Header (AH)	Stated in LoC	Yes	M	Met	Yes	
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	Not Stated	Not Tested	S+ CM	Not Tested	No	
2407	The Internet IP Security Domain of Interpretation for ISAKMP	Stated in LoC	Yes	O	Met	Yes	
2408	Internet Security Association and Key Management Protocol	Stated in LoC	Yes	O	Met	Yes	

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

IBM z/OS							
RFC	RFC Title	Testing Completed		Advanced Server		Implemented	Comments
		Conformance	Interoperability	Requirement	Met/Not Met		
2409	The Internet Key Exchange (IKE)	Stated in LoC	Yes	O	Met	Yes	
4109	Internet Key Exchange (IKEv1) Protocol	Stated in LoC	Yes	O	Met	Yes	
4308	Cryptographic Suites for IPsec	Stated in LoC	Yes	O	Met	Yes	
Transition Mechanisms							
4213	Transition Mechanisms for IPv6 Host and Routers	Stated in LoC	Yes	CM	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	CM	Not Tested	No	
QoS							
2474	Definition of the Differentiated Services Field (DS Field) in the IPv4 and IPv6 Headers	Not Stated	Not Tested	O	Not Tested	No	
2205	Resource ReSerVation Protocol (RSVP) – Version 1 Functional Specification	Not Stated	Not Tested	O	Not Tested	No	
2207	RSVP Extensions for IPSEC Data Flows	Not Stated	Not Tested	O	Not Tested	No	
2210	The Use of RSVP with IETF Integrated Services	Not Stated	Not Tested	O	Not Tested	No	
2750	RSVP Extensions for Policy Control	Not Stated	Not Tested	O	Not Tested	No	
3175	Aggregation of RSVP for IPv4 and IPv6 Reservations	Not Stated	Not Tested	O	Not Tested	No	
Mobility							
3775	Mobility Support in IPv6	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	
Server							
959	File Transfer Protocol	Stated in LoC	Yes	O	Met	Yes	
2428	FTP Extensions for IPv6 and NAT	Not Stated	Not Tested	O	Not Tested	No	
2821	Simple Mail Transfer Protocol (SMTP)	Not Stated	Not Tested	O	Not Tested	No	
2911	Internet Printing Protocol	Not Stated	Not Tested	O	Not Tested	No	
3162	RADIUS (Remote Authentication dial-In User Service) and IPv6	Not Stated	Not Tested	O	Not Tested	No	

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

IBM z/OS																																																																											
RFC	RFC Title	Testing Completed		Advanced Server		Implemented	Comments																																																																				
		Conformance	Interoperability	Requirement	Met/Not Met																																																																						
2355	TN3270 Enhancements (TN3270e)	Stated in LoC	Yes	O	Met	Yes																																																																					
4330	Simple Network Time Protocol (SNTP)	Not Stated	Not Tested	O	Not Tested	No																																																																					
3226	DNS Security and IPv6 A6 Aware Server/Resolver Message Size Requirements	Stated in LoC	Yes	O	Met	Yes																																																																					
3261	Session Initiation Protocol (SIP)	Not Stated	Not Tested	O	Not Tested	No																																																																					
3596	DNS Extensions to Support IPv6	Not Stated	Not Tested	O	Not Tested	No																																																																					
Host																																																																											
3484	Default Address Selection for IPv6	Stated in LoC	Yes	M	Met	Yes																																																																					
3596	DNS Extensions to Support IPv6	Stated in LoC	Yes	M	Met	Yes																																																																					
3986	Uniform Resource Identifier (URI): Generic Syntax	Stated in LoC	Yes	M	Met	Yes																																																																					
<p>LEGEND:</p> <table> <tr> <td>CBC</td> <td>Cipher Block Chaining</td> <td>MAC</td> <td>Message Authentication Code</td> </tr> <tr> <td>CCM</td> <td>CBC MAC Mode</td> <td>MIB</td> <td>Management Information Base</td> </tr> <tr> <td>CM</td> <td>Conditional Must</td> <td>NAT</td> <td>Network Address Translation</td> </tr> <tr> <td>CS</td> <td>Conditional Should</td> <td>O</td> <td>Optional (May)</td> </tr> <tr> <td>CS+</td> <td>Conditional Should+</td> <td>OSPF</td> <td>Open Shortest Path First</td> </tr> <tr> <td>DHCPv6</td> <td>Dynamic Host Configuration Protocol Version 6</td> <td>PPP</td> <td>Point-to-Point Protocol</td> </tr> <tr> <td>DNS</td> <td>Domain Name Service</td> <td>QoS</td> <td>Quality of Service</td> </tr> <tr> <td>DoD</td> <td>Department of Defense</td> <td>RFC</td> <td>Request for Comment</td> </tr> <tr> <td>FTP</td> <td>File Transfer Protocol</td> <td>RoHC</td> <td>Robust Header Compression</td> </tr> <tr> <td>IETF</td> <td>Internet Engineering Task Force</td> <td>RSVP</td> <td>Resource ReSerVation Protocol</td> </tr> <tr> <td>IKEv2</td> <td>Internet Key Exchange Version 2</td> <td>RTP</td> <td>Real-Time Transport Protocol</td> </tr> <tr> <td>IP</td> <td>Internet Protocol</td> <td>S</td> <td>Should</td> </tr> <tr> <td>IPSec</td> <td>Internet Protocol Security</td> <td>SLAAC</td> <td>Stateless Address Auto-configuration</td> </tr> <tr> <td>IPv4</td> <td>Internet Protocol Version 4</td> <td>SN</td> <td>Should Not</td> </tr> <tr> <td>IPv6</td> <td>Internet Protocol Version 6</td> <td>S+</td> <td>Should+</td> </tr> <tr> <td>LoC</td> <td>Letter of Conformance</td> <td>UDP</td> <td>User Datagram Protocol</td> </tr> <tr> <td>M</td> <td>Must</td> <td></td> <td></td> </tr> </table> <p>NOTES:</p> <ol style="list-style-type: none"> 1. All Product Classes MUST support a method of autonomous configuration, either SLAAC or DHCPv6 client. 2. 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. 								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		
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																																																																										

8. TEST NETWORK DESCRIPTION. The DUT was tested as part of the JITC simulated DISN IP Core Network managed by the Advanced IP Technology Capability, and configured as shown in Figure 2-2.

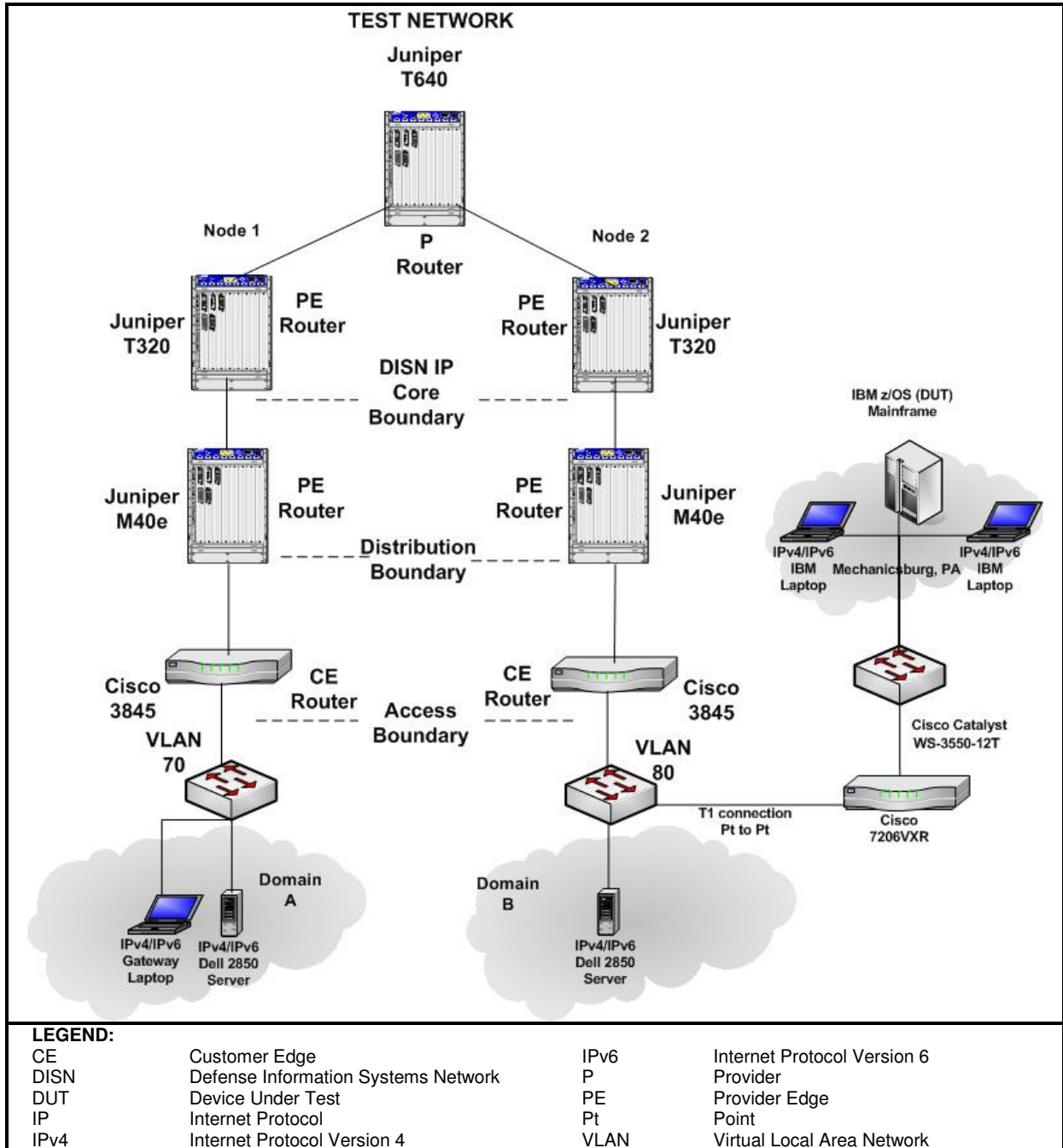


Figure 2-2. Test Network

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			
IBM Mainframe - DUT	z/OS	V 1.10	
Cisco Router	Cisco 7206VXR	12.4(20)T	
2 Cisco Routers	Cisco 3845	12.4(11)T	
Cisco Switch	Catalyst WS-3550-12T	12.1(22)EA10b	
2 Juniper Routers	Juniper M40e	V 7.6R3.6	
2 Juniper Routers	Juniper T320	V 7.5R4.4	
Juniper Router	Juniper T640	V 7.5R4.4	
2 Dell Power Edge Servers	2850	MS 2003 Server	
Gateway Notebook	450ROG	Windows XP Professional	
2 IBM Lenovo ThinkPad Notebooks	T61t	Windows XP Professional/Ubuntu Linux	
Software			
Windows XP Professional	N/A	Build 5.1.2600 SP2	
Windows Server 2003	N/A	Build 5.2.3790 SP1	
Ubuntu Linux	N/A	2.6.24-21	
Openswan	N/A	2.4.9	
Hummingbird	N/A	11.0.0.0	
TightVNC Viewer	N/A	1.3.9	
VLC media player	N/A	0.8.6i	
Xlight FTP Server	N/A	2.86	
Wireshark	N/A	V 0.99.2 (SVN Rev 18752)	
LEGEND:			
DUT	Device Under Test	Rev	Revision
IOS	Internetworking Operating System	SP	Service Pack
LAN	Local Area Network	SVN	Software Version Number
MS	Microsoft	T	New Technology
N/A	Not Applicable	V	Version
OS	Operating System	VLC	Video LAN Client
R	Release		

10. TEST LIMITATIONS. None.

11. TEST RESULTS.

a. IPv6 Base.

Test Case C.1.1. The Request for Comments (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 IBM z/OS mainframe operating system met the test requirement.

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 IBM z/OS mainframe operating system met the test requirement.

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 IBM z/OS mainframe operating system met the test requirement.

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 IBM z/OS mainframe operating system met the test requirement.

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 IBM z/OS mainframe operating system met the test requirement.

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 IBM z/OS mainframe operating system met the test requirement.

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 IBM z/OS mainframe operating system met the test requirement.

Test Case C.1.12. The RFC 4193 Unique Local IPv6 Unicast Addresses defines globally unique local addresses. Local IPv6 unicast addressing is intended to be used for local communications and is not expected to be routed to the Internet. The IBM z/OS mainframe operating system met the test requirement.

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 IBM z/OS mainframe operating system met the test requirement.

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 IBM z/OS mainframe operating system met the test requirement.

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 nodes. The IBM z/OS mainframe operating system met the test requirement.

b. IP Security (IPSec)

Test Case C.2.1. The RFC 4301 defines the security architecture for IP. The document defines what IPSec is and how it works. The IBM z/OS mainframe operating system met the test requirement.

Test Case C.2.2. The RFC 4302 IP Authentication Header (AH) is used to provide connectionless integrity and data origin authentication for IP datagrams, and provides protection against replays. The IBM z/OS mainframe operating system met the test requirement.

Test Cases C.2.3. In the RFC 4303 IP Encapsulating Security Payload (ESP), the ESP header is designed to provide a mix of security services in IPv4 and IPv6. The IBM z/OS mainframe operating system met the test requirement.

Test Cases C.2.8. The RFC 4304 Extended Sequence Number Addendum to IPSec Domain of Interpretation (DOI) for Internet Security Association and Key Management Protocol (ISAKMP) defines how sequence numbers can be used to detect replay. The IBM z/OS mainframe operating system met the test requirement.

Test Cases C.2.4. The RFC 4305 Cryptographic Algorithm Implementation defines the requirements for ESP and AH. The IBM z/OS mainframe operating system met the test requirement.

Test Cases C.2.8. The RFC 2408 ISAKMP describes a protocol utilizing security concepts necessary for establishing Security Associations (SAs) and cryptographic keys in an Internet environment. The IBM z/OS mainframe operating system met the test requirement.

Test Cases C.2.8. 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 DOI. The IBM z/OS mainframe operating system met the test requirement.

Test Cases C.2.8. The RFC 4109 Algorithms for IKE Version 1 (IKEv1) updates the original IKEv1 definition (RFC 2409) and requires Secure Hashing Algorithm 1 for hashing and Hashed Message Authentication Code functions; Pre-shared secrets for authentication; and Diffie-Hellman Modern Programming Practice group 2 as Musts. The IBM z/OS mainframe operating system met the test requirement.

Test Cases C.2.7. The RFC 4308 Cryptographic Suites for IPsec suites should not be considered extensions to IPsec, IKE, and IKE Version 2 (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 IBM z/OS mainframe operating system met the test requirement.

Test Cases C.2.8. The RFC 2407 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 DOI. The IBM z/OS mainframe operating system met the test requirement.

c. Transition Mechanisms.

Test Case C.3.18. The RFC 4213 Transition Mechanisms for IPv6 Host and Routers specifies IPv4 co-existence mechanisms that can be implemented by IPv6 devices. The IBM z/OS mainframe operating system met the test requirement.

d. Server.

Test Case Not Applicable (N/A). The RFC 959 File Transfer Protocol defines how computers can transfer files between devices. The IBM z/OS mainframe operating system met the test requirement.

Test Case N/A. The RFC 2355 TN3270 Enhancements defines a method of emulating terminal members of the 3270 family of devices via Telnet. The IBM z/OS mainframe operating system met the test requirement.

Test Case N/A. The RFC 3226 Domain Name Service (DNS) Security and IPv6 A6 aware server/resolver message size requirements define support for Extension Mechanisms for DNS in DNS entities claiming to support either DNS Security Extensions or A6 records. The IBM z/OS mainframe operating system met the test requirement.

Test Case C.3.13. The RFC 3596 DNS Extensions to Support IPv6 defines the changes that need to be made to the DNS to support hosts running IPv6. The IBM z/OS mainframe operating system met the test requirement.

e. Host.

Test Case C. 3.12. The RFC 3484 Default Address Selection IPv6 defines two algorithms, one for source address selection, and the other for destination address selection. Each algorithm specifies what the default behavior is for IPv6 implementation. The IBM z/OS mainframe operating system met the test requirement.

Test Case C.3.17. The RFC 3986 Uniform Resource Identifier Generic Syntax provides a simple and extensible means for identifying a resource. The IBM z/OS met the test requirement.

f. Conclusion. The IBM z/OS mainframe operating system met all the required RFCs.

12. TEST AND ANALYSIS REPORT. No detailed test report was written in accordance with the Assistant Secretary of Defense-Networks Information and Integration. 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/>.