



DEFENSE INFORMATION SYSTEMS AGENCY

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

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

29 Oct 08

MEMORANDUM FOR DISTRIBUTION

SUBJECT: Special Interoperability Test Certification of the Brocade SilkWorm 200E Fiber Channel Switch Running Fabric Operating System Version 6.2 Software 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 Brocade SilkWorm 200E Fiber Channel (FC) switch running Fabric Operating System (OS) Version (V) 6.2 software has met the Internet Protocol (IP) Version 6 (IPv6) Capable interoperability requirements of a Network Appliance 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 Brocade SilkWorm 200E FC switch running Fabric OS V 6.2 software 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 10 April 2008. Interoperability testing was conducted from 22 through 26 September 2008 at JITC's Advanced IP Technology Capability. Conformance testing was confirmed by Brocade 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 Brocade SilkWorm 200E Fiber Channel Switch Running Fabric Operating System Version 6.2 Software for Internet Protocol Version 6 Capability

Table 1. Interoperability Status Summary

Brocade SilkWorm 200E FC Switch		
Functional Category	Requirement	Verified
Base IPv6	M	Yes
IPSec	S+	No
Transition Mechanisms	S	Yes
Quality of Service	O	No
Mobility	CS	No
Bandwidth Limited Networks	O	No
Host	S	No
LEGEND:		
CS	Conditional Should	M Must
FC	Fiber Channel	O Optional
IPSec	Internet Protocol Security	S Should
IPv6	Internet Protocol Version 6	S+ Should Plus
NOTE: The terms Conditional Should, Must, Should, Should Plus, 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 IPv6 Generic Test Plan.		

Table 2. Equipment Listing

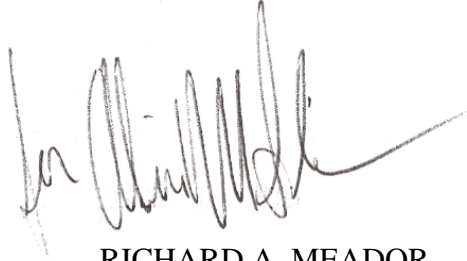
Brocade SilkWorm 200E FC Switch		
Component	Firmware/Software	Interface
SilkWorm 200E	Kernel 2.6.14.2/Fabric OS V6.2.0jharan_V6.2.0_pit_01_2008_09_02	RJ45 Gigabit Ethernet
LEGEND:		
FC	Fiber Channel	RJ Registered Jack
OS	Operating System	V Version

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 testing is on the UC APL at http://jitic.fhu.disa.mil/adv_ip/register/register.html.

JITC Memo, JTE, Special Interoperability Test Certification of the Brocade SilkWorm 200E Fiber Channel Switch Running Fabric Operating System Version 6.2 Software 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:



RICHARD A. MEADOR
Chief
Battlespace Communications Portfolio

2 Enclosures a/s

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

Brocade, Attn: Ian Whiting, 1745 Technology Dr., San Jose, CA 95110

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.** Brocade SilkWorm 200E Fiber Channel (FC) switch running Fabric Operating System (OS) Version (V) 6.2, 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 a fiber channel switch used to support storage area network technology.
- 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 Network Appliance profile requirements for conformance and interoperability are in Table 2-1.

Table 2-1. IPv6 Capability Requirements and Status

Brocade SilkWorm 200E FC Switch							
RFC	RFC Title	Testing Completed		Network Appliance		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	S	Met	No	
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	Not Stated	Not Tested	S	Not Tested	No	
2464	Transmission of IPv6 Packets over Ethernet Networks	Stated in LoC	Yes	CM	Not Tested	Yes	
IPSec							
4301	Security Architecture for the Internet Protocol	Not Stated	Not Tested	S+	Not Tested	No	
4302	IP Authentication Header	Not Stated	Not Tested	S	Not Tested	No	
4303	IP Encapsulating Security Payload (ESP)	Not Stated	Not Tested	S+	Not Tested	No	
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)	Not Stated	Not Tested	S+	Not Tested	No	
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	

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

Brocade SilkWorm 200E FC Switch							
RFC	RFC Title	Testing Completed		Network Appliance		Implemented	Comments
		Conformance	Interoperability	Requirement	Met/Not Met		
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	Not Tested	No	
4306	Internet Key Exchange (IKEv2) Protocol	Not Stated	Not Tested	S+	Not Tested	No	
4307	Cryptographic Algorithms for Internet Key Exchange Version 2 (IKEv2)	Not Stated	Not Tested	S+	Not Tested	No	
Transition Mechanisms							
4213	Transition Mechanisms for IPv6 Host and Routers	Stated in LoC	Yes	S	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	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	CS	Not Tested	No	
4282	The Network Address Identifier	Not Stated	Not Tested	CS	Not Tested	No	
4283	Mobile Node Identifier for Option for IPv6	Not Stated	Not Tested	CS	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	

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

Brocade SilkWorm 200E FC Switch							
RFC	RFC Title	Testing Completed		Network Appliance		Implemented	Comments
		Conformance	Interoperability	Requirement	Met/Not Met		
Host							
3484	Default Address Selection for IPv6	Not Stated	Not Tested	S	Not Tested	No	
3596	DNS Extensions to Support IPv6	Not Stated	Not Tested	S	Not Tested	No	
3986	Uniform Resource Identifier (URI): Generic Syntax	Not Stated	Not Tested	S	Not Tested	No	
LEGEND:							
CBC	Cipher Block Chaining		M		Must		
CCM	CBC MAC Mode		MAC		Message Authentication Code		
CM	Conditional Must		O		Optional (May)		
CS	Conditional Should		PPP		Point-to-Point Protocol		
DHCPv6	Dynamic Host Configuration Protocol Version 6		QoS		Quality of Service		
DNS	Domain Name Service		RFC		Request for Comment		
DoD	Department of Defense		RoHC		Robust Header Compression		
FC	Fiber Channel		RSVP		Resource ReSerVation Protocol		
HTTP	Hypertext Transfer Protocol		RTP		Real-Time Transport Protocol		
IETF	Internet Engineering Task Force		S		Should		
IP	Internet Protocol		S+		Should+		
IPSec	Internet Protocol Security		SN		Should Not		
IPv4	Internet Protocol Version 4		SLAAC		Stateless Address Auto-configuration		
IPv6	Internet Protocol Version 6		UDP		User Datagram Protocol		
LoC	Letter of Conformance						
NOTES:							
1. The device must implement one of the automatic configuration mechanisms SLAAC or DHCPv6.							
2. The terms Must, Conditional Must, Should, Should Plus, 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 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.

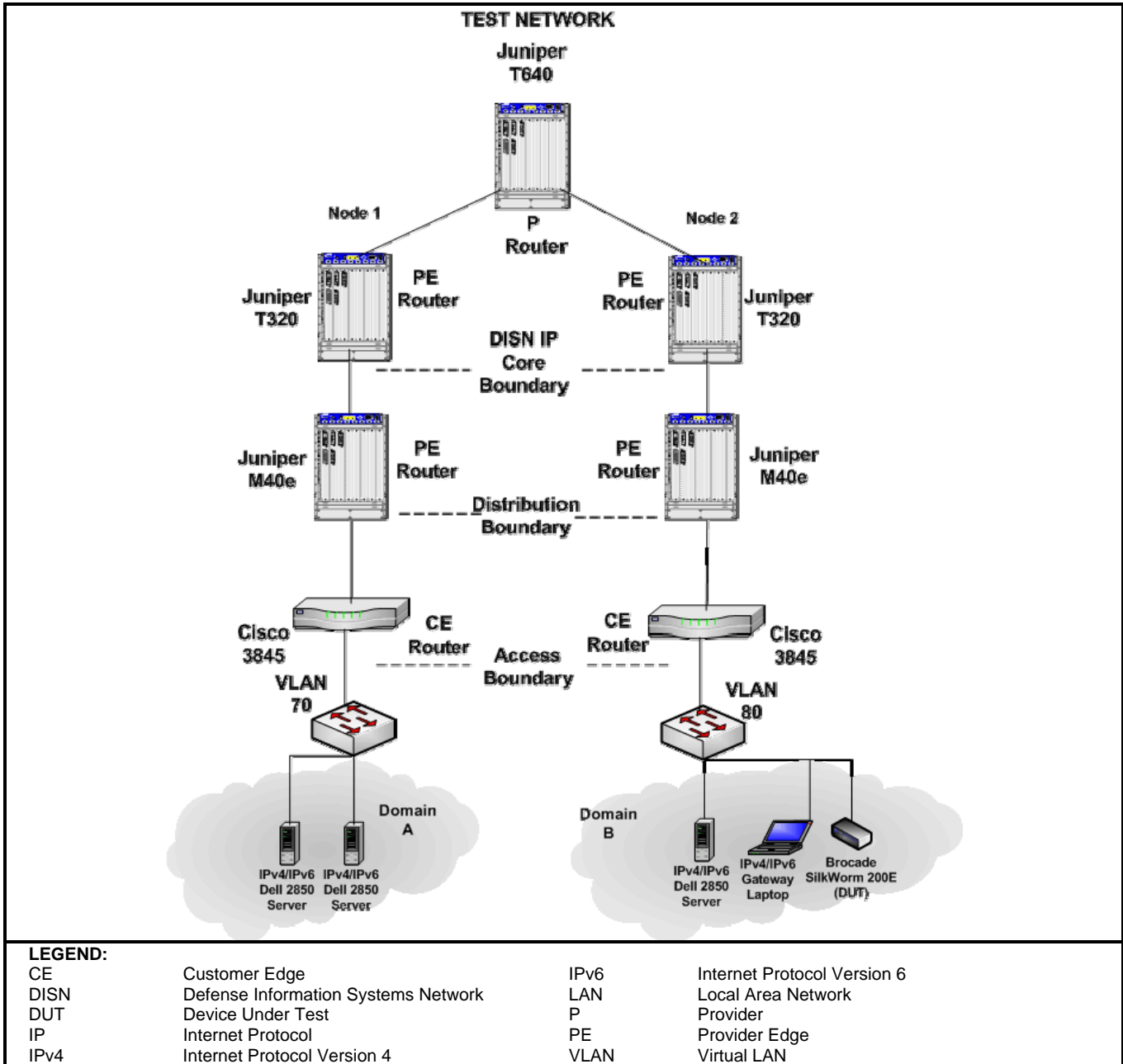


Figure 2-2. Test Network

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			
Brocade FC Switch	SilkWorm 200E	Fabric OS Version 6.2	
2 Cisco Router	Cisco 3845	12.4(11)T	
2 Juniper Router	Juniper M40e	V 7.6R3.6	
2 Juniper Router	Juniper T320	V 7.5R4.4	
Juniper Router	Juniper T640	V 7.5R4.4	
3 Dell Power Edge Servers	2850	MS 2003 Server	
1 Gateway Notebook	450ROG	Windows XP Professional	
Software			
Fabric OS Version 6.2	N/A	V6.2.0jharN_V6.2.0_PIT_01_2008_09_02	
Windows XP Professional	N/A	Build 5.1.2600 SP3	
Windows Server 2003	N/A	Build 5.2.3790 SP2	
Wireshark	N/A	V 1.0.3 (SVN Rev 26134)	
LEGEND:			
DUT	Device Under Test	R	Release
FC	Fiber Channel	Rev	Revision
IOS	Internetworking Operating System	SP	Service Pack
MS	Microsoft	SVN	Software Version Number
N/A	Not Applicable	T	New Technology
OS	Operating System	V	Version

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 Brocade SilkWorm 200E FC Switch has 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 Brocade SilkWorm 200E FC Switch has 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 Brocade SilkWorm 200E FC Switch has 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 Brocade SilkWorm 200E FC Switch has 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 Brocade SilkWorm 200E FC Switch has 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 Brocade SilkWorm 200E FC Switch has 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 Brocade SilkWorm 200E FC Switch has 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 Brocade SilkWorm 200E FC Switch has 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 Brocade SilkWorm 200E FC Switch has 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 Brocade SilkWorm 200E FC Switch has met the test requirement.

b. 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 Brocade SilkWorm 200E FC Switch has met the test requirement.

c. Conclusion. The Brocade SilkWorm 200E FC Switch running Fabric OS 6.2 software has met all the required RFCs.

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/>.