



## DEFENSE INFORMATION SYSTEMS AGENCY

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

IN REPLY  
REFER TO: Battlespace Communications Portfolio (JTE)

**10 Jul 08**

### MEMORANDUM FOR DISTRIBUTION

**SUBJECT:** Special Interoperability Test Certification of the Novell SuSE Linux Enterprise Server 10, Service Pack 2 Running on an IBM P-Series High Volume Open Power Personal Computer Server, IBM X-Series 226 x86 Server, Dell Precision M6300 32 and 64-bit x86 Laptop, and Dell Precision T5400 32 and 64-bit x86 Desktop for 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 Novell SuSE Linux Enterprise Server 10, Service Pack 2 running on an IBM P-Series High Volume Open Power Personal Computer Server, IBM X-Series 226 x86 Server, Dell Precision M6300 32-bit and 64-bit x86 Laptop, and Dell Precision T5400 32-bit and 64-bit x86 Desktop has met the IPv6 Capable interoperability requirements of a Host and 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 Novell SuSE Linux Enterprise Server 10, Service Pack 2 has successfully completed the related IPv6 Interoperability portions of the "DoD IPv6 Generic Test Plan 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). Interoperability testing was conducted from 15 to 20 May 2008 at JITC's Advanced IP Technology Capability. Conformance was confirmed by Novell 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 devices' interoperability status summary is in table 1 and table 2 contains the equipment list.

JITC Memo, JTE, Special Interoperability Test Certification of the Novell SuSE Linux Enterprise Server 10, Service Pack 2 Running on an IBM P-Series High Volume Open Power Personal Computer Server, IBM X-Series 226 x86 Server, Dell Precision M6300 32 and 64-bit x86 Laptop, and Dell Precision T5400 32 and 64-bit x86 Desktop for IPv6 Capability

**Table 1. Interoperability Status Summary**

| Novell SuSE Linux Enterprise Server10, Service Pack 2  |                             |                    |
|--|-----------------------------|--------------------|
| Functional Category  | Requirement                 | Verified           |
| Base IPv6  | M                           | Yes                |
| IPSec  | M                           | Yes                |
| Transition Mechanisms  | M                           | Yes                |
| Quality of Service   | O                           | No                 |
| Mobility   | CM                          | No                 |
| Bandwidth Limited Networks   | O                           | No                 |
| Server   | M                           | Yes                |
| Host   | M                           | Yes                |
| <b>LEGEND:</b>   |                             |                    |
| CM   | Conditional Must            | M Must             |
| IPSec  | Internet Protocol Security  | N/A Not Applicable |
| IPv6   | Internet Protocol Version 6 | O Optional         |
| <b>NOTE:</b> The terms Must, Conditional Must, 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. Equipment Listing**

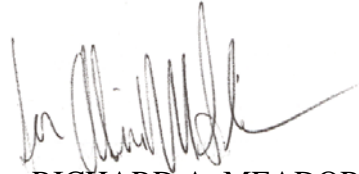
| Novell SuSE Linux Enterprise Server10, Service Pack 2 |  |                      |
|---|--|----------------------|
| Component   | Firmware/Software  | Interface            |
| IBM P-Series High Volume Open Power PC Server         | SuSE Linux Enterprise Server10, Service Pack 2/<br>GNU/Linux Kernel 2.6.16.60-0.21 | Ethernet 10/100Mbps  |
| IBM X-Series 226 x86 Server                           | SuSE Linux Enterprise Server10, Service Pack 2/<br>GNU/Linux Kernel 2.6.16.60      | Ethernet 10/100Mbps  |
| Dell Precision M6300 32-bit x86 Laptop                | SuSE Linux Enterprise Server10, Service Pack 2/<br>GNU/Linux Kernel 2.6.16.60      | Ethernet 10/100Mbps  |
| Dell Precision M6300 64-bit x86 Laptop                | SuSE Linux Enterprise Server10, Service Pack 2/<br>GNU/Linux Kernel 2.6.16.60      | Ethernet 10/100Mbps  |
| Dell Precision T5400 32-bit x86 Desktop               | SuSE Linux Enterprise Server10, Service Pack 2/<br>GNU/Linux Kernel 2.6.16.60      | Ethernet 10/100Mbps  |
| Dell Precision T5400 64-bit x86 Desktop               | SuSE Linux Enterprise Server10, Service Pack 2/<br>GNU/Linux Kernel 2.6.16.60      | Ethernet 10/100Mbps  |
| <b>LEGEND:</b>  |  |                      |
| GNU   | GNUs Not Unix  | PC Personal Computer |
| Mbps  | Megabits per second  | OS Operating System  |

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://jitc.fhu.disa.mil/adv\\_ip/register/register.html](http://jitc.fhu.disa.mil/adv_ip/register/register.html).

JITC Memo, JTE, Special Interoperability Test Certification of the Novell SuSE Linux Enterprise Server 10, Service Pack 2 Running on an IBM P-Series High Volume Open Power Personal Computer Server, IBM X-Series 226 x86 Server, Dell Precision M6300 32 and 64-bit x86 Laptop, and Dell Precision T5400 32 and 64-bit x86 Desktop for IPv6 Capability

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

Distribution:

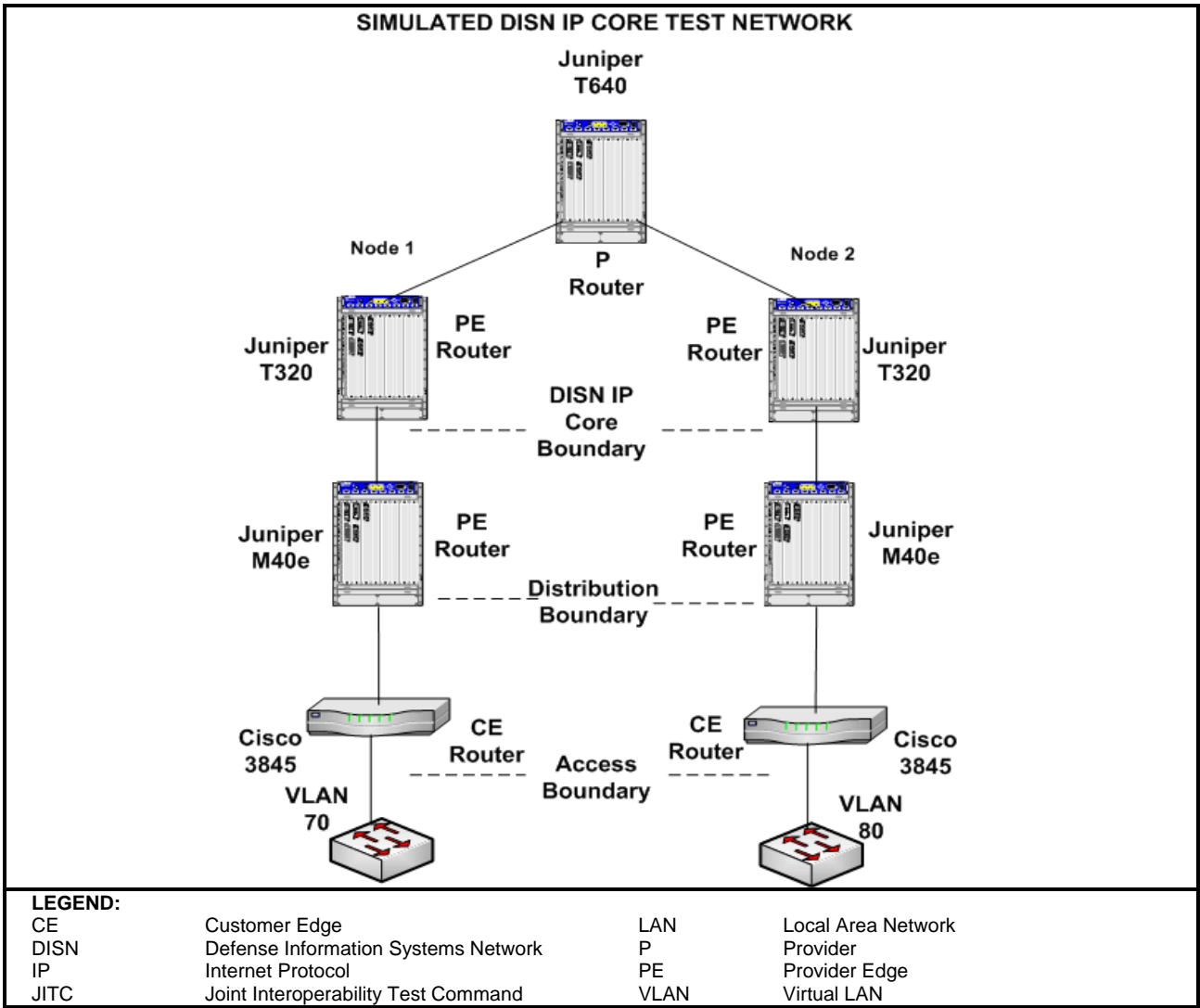
Joint Staff J6I, Room 1E596, Pentagon, Washington, DC 20318-6000  
Joint Interoperability Test Command, Liaison, ATTN: TED/JT1, 2W24-8C, P.O. Box 4502, Falls Church, VA 22204-4502  
Defense Information Systems Agency, Net-Centricity Requirements and Assessment Branch, ATTN: GE333, Room 244, P.O. Box 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  
Novell Inc., Attn: Jason Ganovsky, 7900 404 Wyman Street, Suite 500, Waltham, MA 02451  
Novell Inc., Attn: Roger Levy, 7900 404 Wyman Street, Suite 500, Waltham, MA 02451

## **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) 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 Novell SuSE Linux Enterprise Server (SLES) 10, Service Pack (SP) 2 Running on an IBM P-Series High Volume Open (HVO) Power Personal Computer (PC) Server, IBM X-Series 226 x86 Server, Dell Precision M6300 32-bit and 64-bit x86 Laptop, and Dell Precision T5400 32-bit and 64-bit x86 Desktop, hereafter referred to as the devices under test (DUTs).
- 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, 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 DUTs were divided into two categories all running Novell SLES 10, SP 2. The host category DUTs were the Dell Precision M6300 32-bit and 64-bit x86 laptops and the Dell T5400 32-bit and 64-bit x86 desktops. The advanced server DUTs were the IBM P-Series HVO Power PC Server and IBM X-Series 226 Server. Each device can act as a host (workstation running client-side applications) and advanced server (server running server-side applications).
- 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 products to be included on the Unified Capabilities Approved Products List must meet the requirements of the DoD Information Technology Standards Registry, "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 Version 3," August 2007. The IPv6 Host/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**

| Novell SuSE Linux Enterprise Server 10, Service Pack 2 |  |                   |                  |                      |               |             |                  |
|--|--|-------------------|------------------|----------------------|---------------|-------------|------------------|
| RFC  | RFC Title  | Testing Completed |                  | Host/Advanced Server |               | Implemented | Comments         |
|  |  | Conformance       | Interoperability | Requirement          | Met/Not Met   |             |                  |
| <b>IPv6 Base</b>                                       |  |                   |                  |                      |               |             |                  |
| 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         |                  |
| 3315   | DHCPv6 (Client)  | Stated in LoC     | Yes              | M                    | Met           | Yes         | Note 1<br>Note 4 |
| 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         |                  |
| <b>IPSec</b>   |  |                   |                  |                      |               |             |                  |
| 4301   | Security Architecture for the Internet Protocol  | Stated in LoC     | Yes              | M                    | Met           | Yes         | Note 2           |
| 4302   | IP Authentication Header   | Not Tested        | Not Tested       | S                    | Not Tested    | No          |                  |
| 4303   | IP Encapsulating Security Payload (ESP)  | Stated in LoC     | Yes              | M                    | Met           | Yes         | Note 2           |
| 4304   | Extended Sequence Number (ESN) Addendum to IPsec Domain of Interpretation (DOI) for Internet Security Association and Key Management Protocol (ISAKMP) | Not Tested        | 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         |                  |
| 4869   | Suite B Cryptographic Suites for IPsec   | Not Tested        | Partial Test     | S+                   | Partially Met | Partial     | Note 5           |

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

| Novell SuSE Linux Enterprise Server 10, Service Pack 2 |   |                   |                  |                      |             |             |          |
|--|---|-------------------|------------------|----------------------|-------------|-------------|----------|
| RFC  | RFC Title   | Testing Completed |                  | Host/Advanced Server |             | Implemented | Comments |
|  |   | Conformance       | Interoperability | Requirement          | Met/Not Met |             |          |
| 4309   | Using Advanced Encryption Standard (AES) CCM Mode with IPsec Encapsulating Security Payload (ESP) | Not Tested        | Not Tested       | S+                   | Not Tested  | No          |          |
| 3971   | Secure Neighbor Discovery   | Not Tested        | Not Tested       | S                    | Not Tested  | No          |          |
| 3972   | Cryptographically Generated Addresses   | Not Tested        | Not Tested       | S                    | Not Tested  | No          |          |
| 3041   | Privacy Extensions for Stateless Address Auto configuration in IPv6                               | Stated in LoC     | Yes              | S                    | Met         | Yes         |          |
| 4306   | Internet Key Exchange (IKEv2) Protocol  | Stated in LoC     | Yes              | M                    | Met         | Yes         |          |
| 4307   | Cryptographic Algorithms for Internet Key Exchange Version 2 (IKEv2)                              | Stated in LoC     | Yes              | M                    | Met         | Yes         |          |
| 4308   | Cryptographic Suites for IPsec  | Stated in LoC     | Yes              | S                    | 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 Tested        | Not Tested       | SN                   | Not Tested  | No          |          |
| 3053   | IPv6 Tunnel Broker  | Not Tested        | Not Tested       | CS                   | Not Tested  | No          |          |
| QoS  |   |                   |                  |                      |             |             |          |
| 2474   | Definition of the Differentiated Services Field (DS Field) in the IPv4 and IPv6 Headers           | Not Tested        | Not Tested       | O                    | Not Tested  | No          |          |
| 2205   | Resource ReSerVation Protocol (RSVP) – Version 1 Functional Specification                         | Not Tested        | Not Tested       | O                    | Not Tested  | No          |          |
| 2207   | RSVP Extensions for IPSEC Data Flows  | Not Tested        | Not Tested       | O                    | Not Tested  | No          |          |
| 2210   | The Use of RSVP with IETF Integrated Services   | Not Tested        | Not Tested       | O                    | Not Tested  | No          |          |
| 2750   | RSVP Extensions for Policy Control  | Not Tested        | Not Tested       | O                    | Not Tested  | No          |          |
| 3175   | Aggregation of RSVP for IPv4 and IPv6 Reservations  | Not Tested        | Not Tested       | O                    | Not Tested  | No          |          |
| Mobility   |   |                   |                  |                      |             |             |          |
| 3775   | Mobility Support in IPv6  | Not Tested        | Not Tested       | CM                   | Not Tested  | No          |          |
| 3776   | Using IPsec to Protect Mobile IPv6 Signaling Between Mobile Nodes and Home Agents                 | Not Tested        | Not Tested       | CM                   | Not Tested  | No          |          |
| 4282   | The Network Access Identifier   | Not Tested        | Not Tested       | CS+                  | Not Tested  | No          |          |
| 4283   | Mobile Node Identifier Option for Mobile IPv6 (MIPv6)   | Not Tested        | Not Tested       | CS+                  | Not Tested  | No          |          |

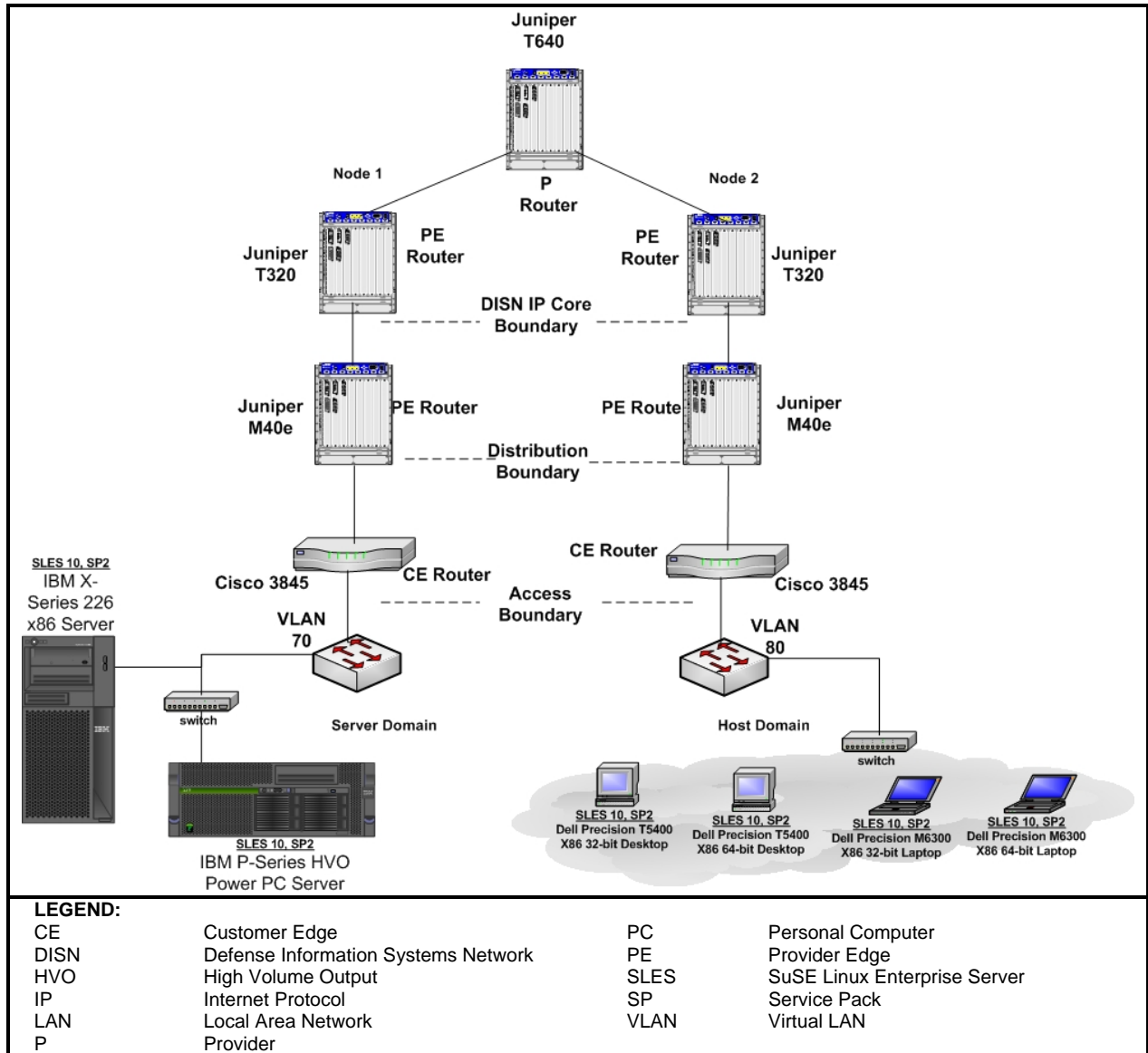
**Table 2-1. IPv6 Capability Requirements and Status (continued)**

| Novell SuSE Linux Enterprise Server 10, Service Pack 2 |  |                   |                  |                      |             |             |          |
|--|--|-------------------|------------------|----------------------|-------------|-------------|----------|
| RFC  | RFC Title  | Testing Completed |                  | Host/Advanced Server |             | Implemented | Comments |
|  |  | Conformance       | Interoperability | Requirement          | Met/Not Met |             |          |
| <b>Bandwidth Limited Networks</b>                      |  |                   |                  |                      |             |             |          |
| 3095   | Robust Header Compression (RoHC)   | Not Tested        | Not Tested       | O                    | Not Tested  | No          |          |
| 3241   | RoHC over PPP  | Not Tested        | Not Tested       | O                    | Not Tested  | No          |          |
| 3843   | RoHC: A Compression Profile for IP                                       | Not Tested        | Not Tested       | O                    | Not Tested  | No          |          |
| 4362   | RoHC: A Link-Layer Assisted Profile for IP/UDP/RTP                       | Not Tested        | Not Tested       | O                    | Not Tested  | No          |          |
| 2507   | IP Header Compression  | Not Tested        | Not Tested       | O                    | Not Tested  | No          |          |
| 2508   | Compressing IP/UDP/RTP Headers for Low-Speed Serial Links                | Not Tested        | Not Tested       | O                    | Not Tested  | No          |          |
| <b>Server</b>  |  |                   |                  |                      |             |             |          |
| 959  | File Transfer Protocol   | Stated in LoC     | Yes              | O                    | Met         | Yes         |          |
| 2428   | FTP Extensions for IPv6 and NAT  | Stated in LoC     | Yes              | O                    | Met         | Yes         |          |
| 2821   | Simple Mail Transfer Protocol (SMTP)                                     | Stated in LoC     | Yes              | O                    | Met         | Yes         |          |
| 2911   | Internet Printing Protocol   | Not Tested        | Not Tested       | O                    | Not Tested  | No          |          |
| 3162   | RADIUS (Remote Authentication Dial-In User Service) and IPv6             | Not Tested        | Not Tested       | O                    | Not Tested  | No          |          |
| 4330   | Simple Network Time Protocol (SNTP)                                      | Stated in LoC     | Yes              | O                    | Met         | Yes         |          |
| 3226   | DNS Security and IPv6 A6 Aware Server/Resolver Message Size Requirements | Not Tested        | Not Tested       | O                    | Not Tested  | No          |          |
| 2616   | Hypertext Transfer Protocol  | Stated in LoC     | Yes              | O                    | Met         | Yes         |          |
| 3261   | Session Initiation Protocol (SIP)  | Not Tested        | Not Tested       | O                    | Not Tested  | No          |          |
| 3315   | DHCPv6 (Server)  | Stated in LoC     | Yes              | M                    | Met         | Yes         | Note 4   |
| 3596   | DNS Extensions to Support IPv6   | Stated in LoC     | Yes              | M                    | Met         | Yes         |          |
| <b>Host</b>  |  |                   |                  |                      |             |             |          |
| 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         |          |

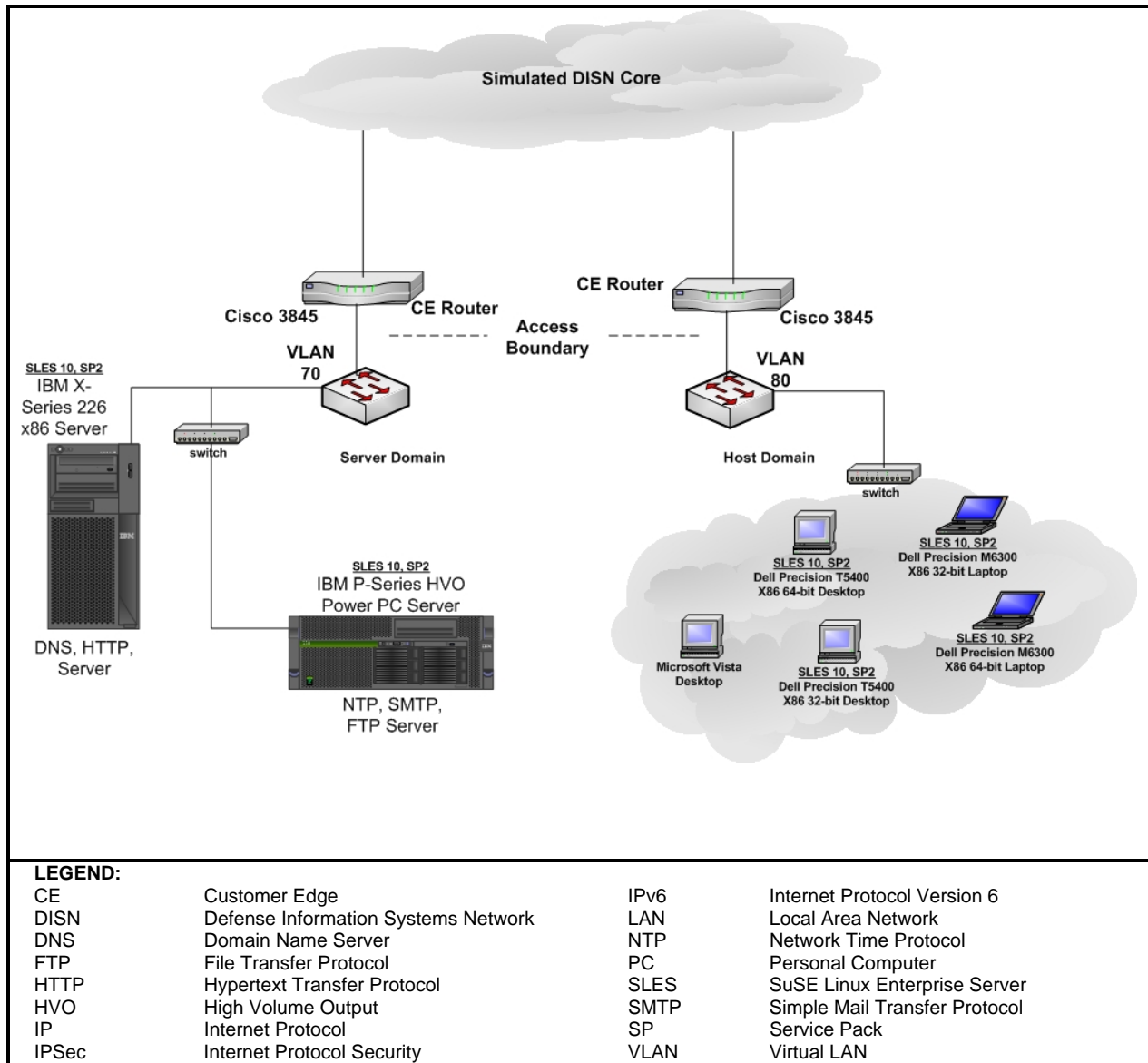
**Table 2-1. IPv6 Capability Requirements and Status (continued)**

| Novell SuSE Linux Enterprise Server 10, Service Pack 2  |   |                   |                  |                      |                                      |             |          |
|---|---|-------------------|------------------|----------------------|--------------------------------------|-------------|----------|
| RFC   | RFC Title   | Testing Completed |                  | Host/Advanced Server |                                      | Implemented | Comments |
|   |   | Conformance       | Interoperability | Requirement          | Met/Not Met                          |             |          |
| 3986  | Uniform Resource Identifier (URI): Generic Syntax | Stated in LoC     | Yes              | M                    | Met                                  | Yes         |          |
| <b>LEGEND:</b>  |   |                   |                  |                      |                                      |             |          |
| AES   | Advanced Encryption Standard                      |                   | LoC              |                      | Letter of Conformance                |             |          |
| CBC   | Cipher Block Chaining                             |                   | M                |                      | Must                                 |             |          |
| CCM   | CBC MAC Mode                                      |                   | MAC              |                      | Message Authentication Code          |             |          |
| CM  | Conditional Must                                  |                   | NAT              |                      | Network Address Translation          |             |          |
| CS  | Conditional Should                                |                   | O                |                      | Optional (May)                       |             |          |
| DHCPv6  | Dynamic Host Configuration Protocol Version 6     |                   | PPP              |                      | Point-to-Point Protocol              |             |          |
| DNS   | Domain Name Service                               |                   | QoS              |                      | Quality of Service                   |             |          |
| DoD   | Department of Defense                             |                   | RoHC             |                      | Robust Header Compression            |             |          |
| FTP   | File Transfer Protocol                            |                   | RSVP             |                      | Resource ReSerVation Protocol        |             |          |
| GCM   | Galois/Counter Mode                               |                   | RTP              |                      | Real-Time Transport Protocol         |             |          |
| GMAC  | Galois Message Authentication Code                |                   | S                |                      | Should                               |             |          |
| IETF  | Internet Engineering Task Force                   |                   | SHA              |                      | Secure Hash Algorithm                |             |          |
| IP  | Internet Protocol                                 |                   | SLAAC            |                      | Stateless Address Auto-configuration |             |          |
| IPSec   | Internet Protocol Security                        |                   | SLES             |                      | SuSE Linux Enterprise Server         |             |          |
| IPv4  | Internet Protocol Version 4                       |                   | SN               |                      | Should Not                           |             |          |
| IPv6  | Internet Protocol Version 6                       |                   | S+               |                      | Should+                              |             |          |
| JITC  | Joint Interoperability Test Command               |                   | UDP              |                      | User Datagram Protocol               |             |          |
| <b>NOTES:</b>   |   |                   |                  |                      |                                      |             |          |
| 1. All Products must support a method of autonomous configuration, either SLAAC or DHCPv6.  |   |                   |                  |                      |                                      |             |          |
| 2. Novell SuSE Linux Enterprise Server demonstrated capability with IKEv2 and IKEv1 for backwards compatibility and interoperability with nodes that do not support IKEv1.  |   |                   |                  |                      |                                      |             |          |
| 3. The terms Must, Conditional Must, Should, Should+, Conditional Should, Should Not, and Optional are used to reference specific required Request for Comments from the Internet Engineering Task Force, the DoD Information Technology Standards Registry, and the DoD Internet Protocol Version 6 Generic Test Plan. |   |                   |                  |                      |                                      |             |          |
| 4. The DHCPv6 client and server implementation on the Novell SuSE clients was recoded, fixed, and retested during the JITC IPv6 test window. Any SuSE servers and clients must use package "dhcp6-1.0.11-0.7" or greater to be a complete and certified system.   |   |                   |                  |                      |                                      |             |          |
| 5. SLES 10 was able to only perform successful demonstrations of Suite B, GCM 128 and 256 using AES and SHA algorithms. SLES 10 was not able to complete a successful test using any of the GMAC algorithms.  |   |                   |                  |                      |                                      |             |          |

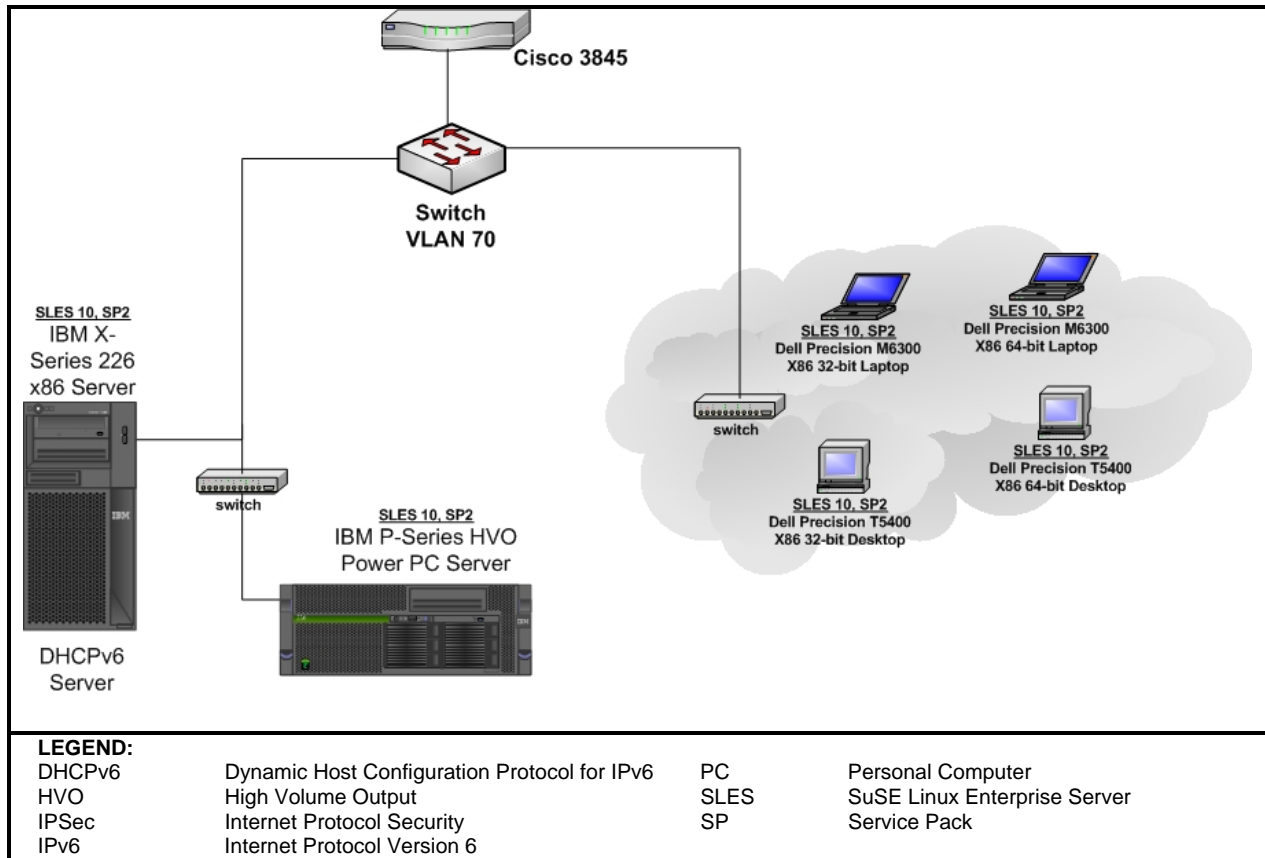
**8. TEST NETWORK DESCRIPTION.** The DUTs were tested as part of the JITC simulated DISN IP Core Network managed by the Advanced IP Technology Capability, and configured as shown in figures 2-2, 2-3, and 2-4.



**Figure 2-2. Test Network**



**Figure 2-3. IPSec and IPv6 Services Test Network**



**Figure 2-4. Multicast Listener Discovery and IPv6 Network Services 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)                    |                         |
|------------------------------------|---|--------------------------------------|-------------------------|
| <b>Hardware</b>                    |   |                                      |                         |
| IBM P-Series Server - DUT          | IBM P-Series High Volume Open Power PC Server | SuSE Linux Enterprise Server10, SP 2 |                         |
| IBM X-Series Server - DUT          | IBM X-Series 226 Server                       | SuSE Linux Enterprise Server10, SP 2 |                         |
| Dell 32-bit x86 Laptop - DUT       | Dell Precision M6300 32-bit x86 Laptop        | SuSE Linux Enterprise Server10, SP 2 |                         |
| Dell 64-bit x86 Laptop - DUT       | Dell Precision M6300 64-bit x86 Laptop        | SuSE Linux Enterprise Server10, SP 2 |                         |
| Dell 32-bit x86 Desktop - DUT      | Dell Precision T5400 32-bit x86 Desktop       | SuSE Linux Enterprise Server10, SP 2 |                         |
| Dell 64-bit x86 Desktop - DUT      | Dell Precision T5400 32-bit x86 Desktop       | SuSE Linux Enterprise Server10, SP 2 |                         |
| Cisco Router                       | Cisco 3845                                    | 12.4(11)T                            |                         |
| Cisco Router                       | Cisco 3845                                    | 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                            |                         |
| Dell Optiplex Desktop              | 745   | Microsoft Vista Enterprise           |                         |
| 1 Gateway Notebook                 | 450ROG  | MS Windows XP Professional           |                         |
| <b>Software</b>                    |   |                                      |                         |
| SuSE Linux Enterprise Server - DUT | N/A   | V 10 SP 2                            |                         |
| MS Windows XP Professional         | N/A   | Build 5.1.2600 SP 2                  |                         |
| Wireshark                          | N/A   | V 0.99.2 (SVN Rev 18752)             |                         |
| <b>LEGEND:</b>                     |   |                                      |                         |
| DUT                                | Device Under Test                             | R                                    | Release                 |
| IOS                                | Internetworking Operating System              | Rev                                  | Revision                |
| MS                                 | Microsoft                                     | SP                                   | Service Pack            |
| N/A                                | Not Applicable                                | SVN                                  | Software Version Number |
| OS                                 | Operating System                              | T                                    | New Technology          |
| PC                                 | Personal Computer                             | 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. TracePath6 was the Linux used to verify the packet exchange between host and router. The SLES 10, SP 2 met the test requirement running on all Dell workstations and IBM servers.

**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 SLES 10, SP 2 met the test requirement running on all Dell workstations and IBM servers.

**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 SLES 10, SP 2 met the test requirement running on all Dell workstations and IBM servers.

**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 SLES 10, SP 2 met the test requirement running on all Dell workstations and IBM servers.

**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 SLES 10, SP 2 met the test requirement running on all Dell workstations and IBM servers.

**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 SLES 10, SP 2 met the test requirement running on all Dell workstations and IBM servers.

**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 SLES 10, SP 2 met the test requirement running on all Dell workstations and IBM servers.

**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 SLES 10, SP 2 met the test requirement running on all Dell workstations and IBM servers.

**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 SLES 10, SP 2 met the test requirement running on all Dell workstations and IBM servers.

**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 SLES 10, SP 2 met the test requirement running on all Dell workstations and IBM servers.

**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 SLES 10, SP 2 met the test requirement running on all Dell workstations and IBM servers.

**Test Case C.3.8.** The RFC 3315 Dynamic Host Configuration Protocol (DHCP) for IPv6 (DHCPv6) specifies the use of an enabled DHCP server passing configuration parameters such as IPv6 network addresses and name server options to IPv6 nodes. During the course of testing, a bug was found in the operation of the DHCPv6 client on SLES 10, SP 2. Further actions from the SuSE engineers produced an updated DHCPv6 client and server application. The tested application version is “dhcp6-1.0.11-0.7.”

It was also discovered that SLES implements DHCPv6 differently than Microsoft Windows Server 2008 and Microsoft Vista. The SLES implementation is identical to the functions in DHCP for IPv6 as outlined in RFC 3315. However, Microsoft implements DHCPv6 differently in that the Vista client receives a DHCPv6 “relay” from the router on the network. A message from the router to the client indicates where the DHCPv6 server is. The Vista client will then receive the configuration options and address from the Server 2008 DHCPv6 server.

This is a significant difference in the implementation of DHCPv6, but does not create an interoperability issue. The SLES 10, SP 2 met the test requirement running on all Dell workstations and IBM servers.

#### **b. IP Security (IPSec).**

**Test Case C.2.1.** The RFC 2401 and 4301 Security Architecture for the IP specifies the base architecture for IPSec compliant systems. The SLES 10, SP 2 met the test requirement running on all Dell workstations and IBM servers.

**Test Case C.2.3.** The RFC 2406 and 4303 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 Authentication Header, or in a nested fashion (e.g., through the use of tunnel mode). All ESP sessions were done in both tunnel and transport modes. The SLES 10, SP 2 met the test requirement running on all Dell workstations and IBM servers.

**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 SLES 10, SP 2 met the test requirement running on all Dell workstations and IBM servers.

**Test Case C.2.5.** The RFC 4306 Internet Key Exchange (IKE) Version 2 (IKEv2) is the update to IKE Version 1 (IKEv1). Both IKEs operate in similar styles yet are not interoperable with each other. The original IKEv1 was overhauled to bring together the several RFCs that compromised the protocol and to make it generally easier to use and more secure. The SLES 10, SP 2 met the test requirement running on all Dell workstations and IBM servers.

**Test Case C.2.6.** The RFC 4307 Cryptographic Algorithms for Use in the IKEv2 provides a mechanism to negotiate which algorithms should be used in any given association. However, to ensure interoperability between disparate implementations, it is necessary to specify a set of mandatory to implement algorithms to ensure that there is at least one algorithm that all implementations will have available. This RFC defines the current set of algorithms that are mandatory to implement as part of IKEv2, as well as algorithms that should be implemented because they may be promoted to mandatory at some future time. The SLES 10, SP 2 met the test requirement running on all Dell workstations and IBM servers.

**Test Case C.2.8.** 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 SLES 10, SP 2 met the test requirement running on all Dell workstations and IBM servers.

**Test Case C.2.8.** The RFC 2408 ISAKMP describes a protocol utilizing security concepts necessary for establishing Security Associations (SA) and cryptographic keys in an Internet environment. The SLES 10, SP 2 met the test requirement running on all Dell workstations and IBM servers.

**Test Case C.2.8.** The RFC 2409 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 ESP and AH for Internet Engineering Task Force IPsec Domain of Interpretation. The SLES 10, SP 2 met the test requirement running on all Dell workstations and IBM servers.

**Test Case C.3.7.** The RFC 3041 Privacy Extensions for Stateless Address Auto-configuration in IPv6 specifies nodes using IPv6 stateless address auto-configuration to generate addresses without the necessity of a DHCP server. The SLES 10, SP 2 met the test requirement running on all Dell workstations and IBM servers.

**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 SLES 10, SP 2 met the test requirement running on all Dell workstations and IBM servers.

**d. Server.**

**Test Case Deviation - 4.** The RFC 4330 Simple Network Time Protocol (SNTP) Version 4 for IPv4, IPv6 and Open Systems Interconnect – Network Time Protocol (NTP) Server and Client Role specifies the basic protocol for the Internet NTP. The NTP server gives the client the requested time including offset and stratum. The functionality of the SNTP was tested by setting up an SNTP server and requesting SNTP traffic from a client. The SLES 10, SP 2 met the test requirement running on all Dell workstations and IBM servers.

**Test Case Deviation - 5.** The RFC 2616 Hypertext Transfer Protocol (HTTP) specifies the functions of web servers and clients in performing basic Uniform Resource Identifier (URI) lookups and transfers using both IPv4 and IPv6. The HTTP server application used to test was Apache Hypertext Transfer Protocol Daemon (HTTPD), and the client application used to test was Mozilla Firefox 2. The SLES 10, SP 2 met the test requirement running on all Dell workstations and IBM servers.

**Test Case Deviation - 6.** The RFC 2428 File Transfer Protocol (FTP) Extensions for IPv6 and Network Address Translations specify that a Server must be capable of transferring files with IPv6 and support Extended Data Port (EPRT) and Extended Passive (EPSV) commands. The functionality of the FTP was tested by setting up an FTP server with EPRT, then EPSV enabled and sent FTP traffic to and from a client. The SLES 10, SP 2 met the test requirement running on all Dell workstations and IBM servers.

**Test Case Deviation - 6.** The RFC 959 FTP specifies the use of the FTP server to share and store files. The functionality of the FTP was tested by setting up an FTP server and sending FTP traffic to and from a client. The SLES 10, SP 2 met the test requirement running on all Dell workstations and IBM servers.

**Test Case Deviation - 7.** The RFC 2821 Simple Mail Transfer Protocol (SMTP) specifies the basic protocol for the Internet electronic mail transport. The functionality of the SMTP was tested by setting up an SMTP server and sending SMTP traffic to and from an SMTP client. Applications like Postfix and Novell Evolution were used to verify

interoperability with SMTP and Internet Message Access Protocol. The SLES 10, SP 2 met the test requirement running on all Dell workstations and IBM servers.

**Test Case C.3.13.** The RFC 3596 Domain Name Service (DNS) Extensions to Support IPv6 specifies that DNS servers must properly assign IPv4 addresses “A” records and IPv6 addresses “AAAA” records. The network servers must always respond to queries by clients in the protocol requests. The network clients must always be able to query “A” and “AAAA” records in both IPv4 and IPv6. Bind was the server application used in the testing. All SLES and Microsoft Vista clients correctly resolved multiple hostnames using AAAA records over IPv6. The SLES 10, SP 2 met the test requirement running on all Dell workstations and IBM servers.

**e. Host.**

**Test Case C.3.12.** The RFC 3484 Default Address Selection for IPv6 specifies the use of two algorithms, one for source address selection and the other for destination address selection. The algorithms specify default behavior for all IPv6 implementations. The SLES 10, SP 2 met the test requirement running on all Dell workstations and IBM servers.

**Test Case C.3.13.** The RFC 3596 DNS Extensions to Support IPv6 specifies the changes that need to be made to the DNS to support hosts running IPv6. The extensions are designed to be compatible with existing applications and DNS implementations. The SLES 10, SP 2 met the test requirement running on all Dell workstations and IBM servers.

**Test Case C.3.17.** The RFC 3986 URI Generic Syntax specifies the use of URIs to provide a simple and extensible means for identifying a resource. A URI is a compact sequence of characters that identifies an abstract or physical resource. The SLES 10, SP 2 met the test requirement running on all Dell workstations and IBM servers.

**f. Conclusion.** The SLES 10, SP 2 running on the Dell workstations and IBM servers 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/>.