



## DEFENSE INFORMATION SYSTEMS AGENCY

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

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

**4 Mar 09**

### MEMORANDUM FOR DISTRIBUTION

**SUBJECT:** Special Interoperability Test Certification of the InfoWeapons SolidDNS 3.0 Domain Name System (DNS) Server Running the InfoWeapons SolidOS Operating System and the InfoWeapons SolidDNS 3.0 DNS Application Using Bind 9.5.0p2 Hosted on the Dell PowerEdge SC 1435 Server Hardware 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 6212.01E, "Interoperability and Supportability of Information Technology and National Security Systems," 15 December 2008  
(c) through (j), 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 InfoWeapons SolidDNS 3.0 domain name system (DNS) server running the InfoWeapons SolidOS operating system and the InfoWeapons SolidDNS 3.0 DNS application using Bind 9.5.0p2 hosted on the Dell PowerEdge SC 1435 server hardware met the Internet Protocol Version 6 (IPv6) Capable interoperability requirements for a Simple Server as described in the Department of Defense (DoD) Information Technology Standards Registry, "DoD IPv6 Standard Profiles for IPv6 Capable Products Version 3.0," July 2008, reference (c). This device 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 4 years from the date of this memorandum.

The InfoWeapons SolidDNS 3.0 DNS server also met the requirement of Office of Management and Budget Memorandum for Chief Information Officers M-08-23, "Securing the Federal Government's Domain Name System Infrastructure," 22 August 2008, reference (e), by following secure DNS configuration guidelines as described in the United States Department of Commerce, National Institute of Standards and Technology Special Publication 800-81, "Secure DNS Deployment Guide," May 2006, reference (f).

JITC Memo, JTE, Special Interoperability Test Certification of the InfoWeapons SolidDNS 3.0 Domain Name System (DNS) Server Running the InfoWeapons SolidOS Operating System and the InfoWeapons SolidDNS 3.0 DNS Application Using Bind 9.5.0p2 Hosted on the Dell PowerEdge SC 1435 Server Hardware for Internet Protocol Version 6 Capability

3. This special certification is based on IPv6 Capable Interoperability testing conducted by JITC at Fort Huachuca, Arizona, and the vendor's Letters of Conformance (LoCs) dated 18 December 2008, and 6 January 2009. Interoperability testing was conducted from 17 through 24 November 2008, and 5 through 9 January 2009, at JITC's Advanced IP Technology Capability. Conformance testing was confirmed by InfoWeapons and was verified in the LoCs 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.

**Table 1. Interoperability Status Summary**

InfoWeapons SolidDNS v3.0		
Functional Category	Requirement	Verified
Base IPv6	M	Yes
IPSec	S+	No
Transition Mechanisms	S	Yes
Quality of Service	O	No
Mobility	CS	No
RoHC	O	No
Automatic Configuration	CM	No
Server	O	No
Host	S	No
<b>LEGEND:</b> CM      Conditional Must      O      Optional IPSec    Internet Protocol Security    RoHC    Robust Header Compression IPv6     Internet Protocol Version 6    S      Should M        Must                                S+     Should Plus <b>NOTE:</b> The terms Conditional Must, Must, Should, Should+, and Optional are used to reference specific required Request for Comments from the Internet Engineering Task Force, the Department of Defense Information Technology Standards Registry, and the Department of Defense Internet Protocol Version 6 Generic Test Plan.		

**Table 2. Equipment Listing**

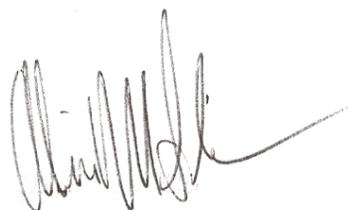
InfoWeapons SolidDNS v3.0		
Component	Firmware/Software	Interface
InfoWeapons SolidDNS v3.0	SolidOS	Gigabit Ethernet (1Gbs)
<b>LEGEND:</b> DNS    Domain Name Server                                v      version Gbs    Gigabits per second		

JITC Memo, JTE, Special Interoperability Test Certification of the InfoWeapons SolidDNS 3.0 Domain Name System (DNS) Server Running the InfoWeapons SolidOS Operating System and the InfoWeapons SolidDNS 3.0 DNS Application Using Bind 9.5.0p2 Hosted on the Dell PowerEdge SC 1435 Server Hardware for Internet Protocol Version 6 Capability

5. 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).

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

InfoWeapons Inc., Attn: Erroll D. Woods, 11465 Johns Creek Parkway, Suite 320, Duluth, GA 30097

## ADDITIONAL REFERENCES

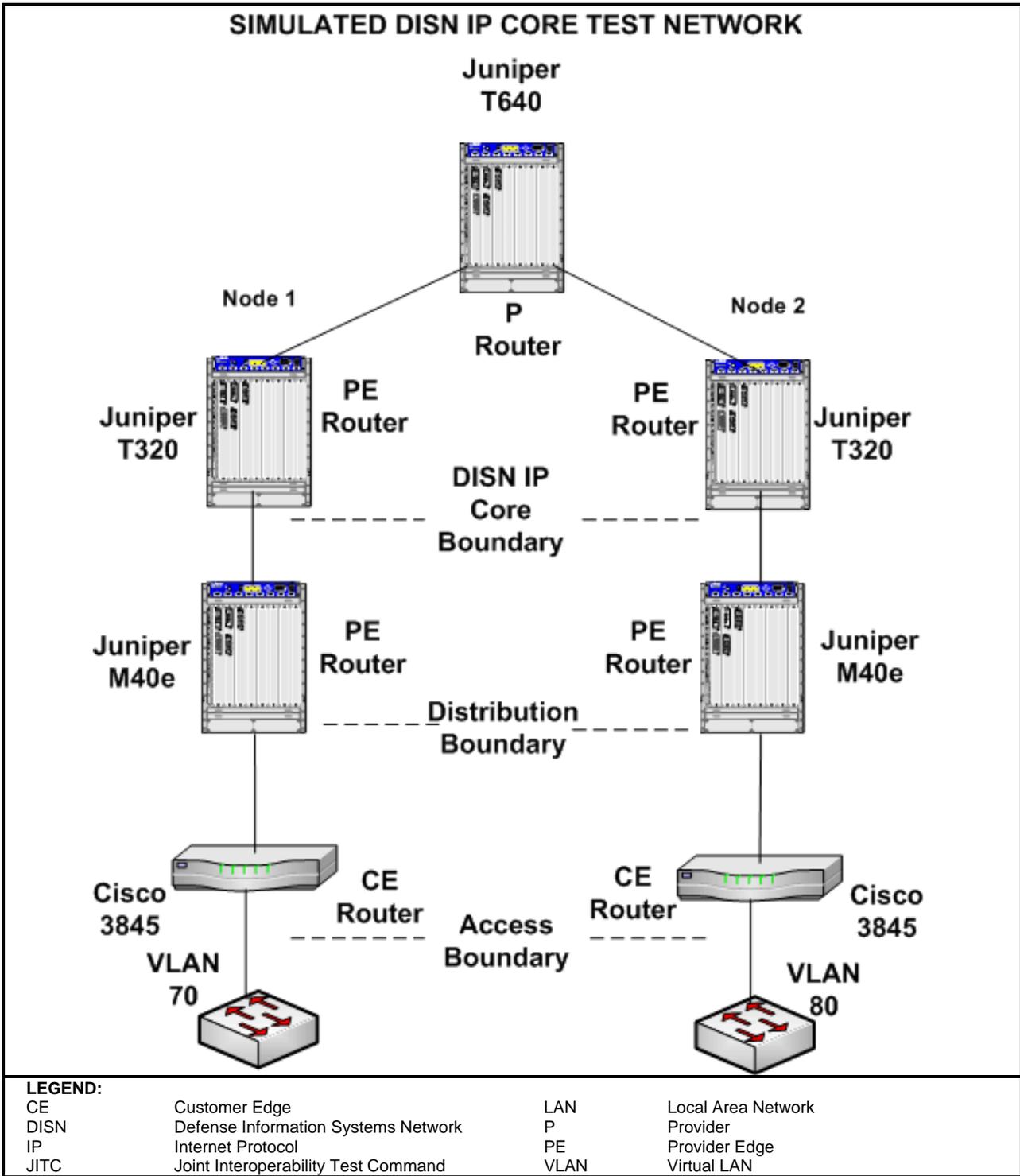
- (c) Department of Defense (DoD) Information Technology Standards Registry (DISR), "DoD Internet Protocol Version 6 (IPv6) Standard Profiles for IPv6 Capable Products Version 3.0," July 2008
- (d) Defense Information Systems Agency, Joint Interoperability Test Command, "DoD IPv6 Generic Test Plan Version 3," August 2007
- (e) Office of Management and Budget, Memorandum for Chief Information Officers (CIOs) M-08-23, "Securing the Federal Government's Domain Name System (DNS) Infrastructure," 22 August 2008
- (f) United States Department of Commerce, National Institute of Standards and Technology Special Publication 800-81 "Secure DNS Deployment Guide," May 2006
- (g) DoD CIO Memorandum, "IPv6," 9 June 2003
- (h) DoD CIO Memorandum, "IPv6 Interim Transition Guidance," 29 September 2003
- (i) DoD IPv6 Transition Office, "DoD IPv6 Master Test Plan, Version 2," September 2006
- (j) 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 InfoWeapons SolidDNS 3.0 domain name system (DNS) server running the InfoWeapons SolidOS operating system and the InfoWeapons SolidDNS 3.0 DNS application using Bind 9.5.0p2 hosted on the Dell PowerEdge SC 1435 server hardware, 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 server appliance platform designed by InfoWeapons to provide DNS with DNS Security (DNSSEC) and Dynamic Host Configuration Protocol service to networks of any size in a highly secure manner.
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 3.0," July 2008. Product testing conducted against these requirements is in accordance with the "DoD IPv6 Generic Test Plan (GTP) Version 3," August 2007. The IPv6 simple server profile requirements for conformance and interoperability are in Table 2-1.

In accordance with the Office of Management and Budget Memorandum for Chief Information Officers M-08-23, "Securing the Federal Government's DNS Infrastructure," 22 August 2008, DNS Servers must follow recommendations as described in the United States Department of Commerce, National Institute of Standards and Technology Special Publication 800-81, "Secure DNS Deployment Guide," May 2006. Table 2-2 includes selected Requests for Comments (RFCs) that the DUT has been tested against to represent compliance with these recommendations.



**Figure 2-1. JITC Simulated DISN IP Core Network**

**Table 2-1. IPv6 Capability Requirements and Status**

InfoWeapons SolidDNS v3.0							
RFC	RFC Title	Testing Completed		Simple 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	
2462	IPv6 Stateless Address Auto configuration	Stated in LoC	Yes	M	Met	Yes	
1981	Path Maximum Transmission Unit Discovery for IPv6	Not Stated	Not Tested	S	Not Tested	No	
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	O	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	Met	Yes	Note 1
<b>IPSec</b>							
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	
4308	Cryptographic Suites for IPSec	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	
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	

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

InfoWeapons SolidDNS v3.0							
RFC	RFC Title	Testing Completed		Simple Server		Implemented	Comments
		Conformance	Interoperability	Requirement	Met/Not Met		
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	
3168	The Addition of Explicit Congestion Notification (ECN) to IP	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	
3181	Signaled Preemption Priority Policy Object	Not Stated	Not Tested	O	Not Tested	No	
2961	RSVP Refresh Overhead Reduction Extension	Not Stated	Not Tested	O	Not Tested	No	
4495	A Resource Reservation Protocol (RSVP) Extension for the Reduction of Bandwidth of a Reservation Flow	Not Stated	Not Tested	O	Not Tested	No	
2998	A Framework for Integrated Services Operation over DiffServ Networks	Not Stated	Not Tested	O	Not Tested	No	
2996	Format of the RSVP DCLASS Object	Not Stated	Not Tested	O	Not Tested	No	
2746	RSVP Operation Over IP Tunnels	Not Stated	Not Tested	O	Not Tested	No	
3182	Identity Representation for RSVP	Not Stated	Not Tested	O	Not Tested	No	
2872	Application and Sub Application Identity Policy Element for Use with RSVP	Not Stated	Not Tested	O	Not Tested	No	
2747	RSVP Cryptographic Authentication	Not Stated	Not Tested	O	Not Tested	No	

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

InfoWeapons SolidDNS v3.0							
RFC	RFC Title	Testing Completed		Simple Server		Implemented	Comments
		Conformance	Interoperability	Requirement	Met/Not Met		
<b>Mobility</b>							
3775	Mobility Support in IPv6	Not Stated	Not Tested	CS	Not Tested	No	
3776	Using IPsec to Protect Mobile IPv6 Signaling Between Mobile Nodes and Home Agents	Not Stated	Not Tested	CS	Not Tested	No	
4877	Mobile IPv6 Operation with IKEv2 and the Revised IPsec Architecture	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	
<b>RoHC</b>							
3095	Robust Header Compression (RoHC)	Not Stated	Not Tested	O	Not Tested	No	
4815	Corrections and Clarification to RFC 3095	Not Stated	Not Tested	O	Not Tested	No	
4995	RoHC Framework	Not Stated	Not Tested	O	Not Tested	No	
4996	RoHC: A profile for TCP/IP	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	
3173	IP Payload Compression	Not Stated	Not Tested	O	Not Tested	No	
<b>Server</b>							
959	File Transfer Protocol	Not Stated	Not Tested	O	Not Tested	No	
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	
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	Not Stated	Not Tested	O	Not Tested	No	
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	
3053	IPv6 Tunnel Broker	Not Stated	Not Tested	O	Not Tested	No	

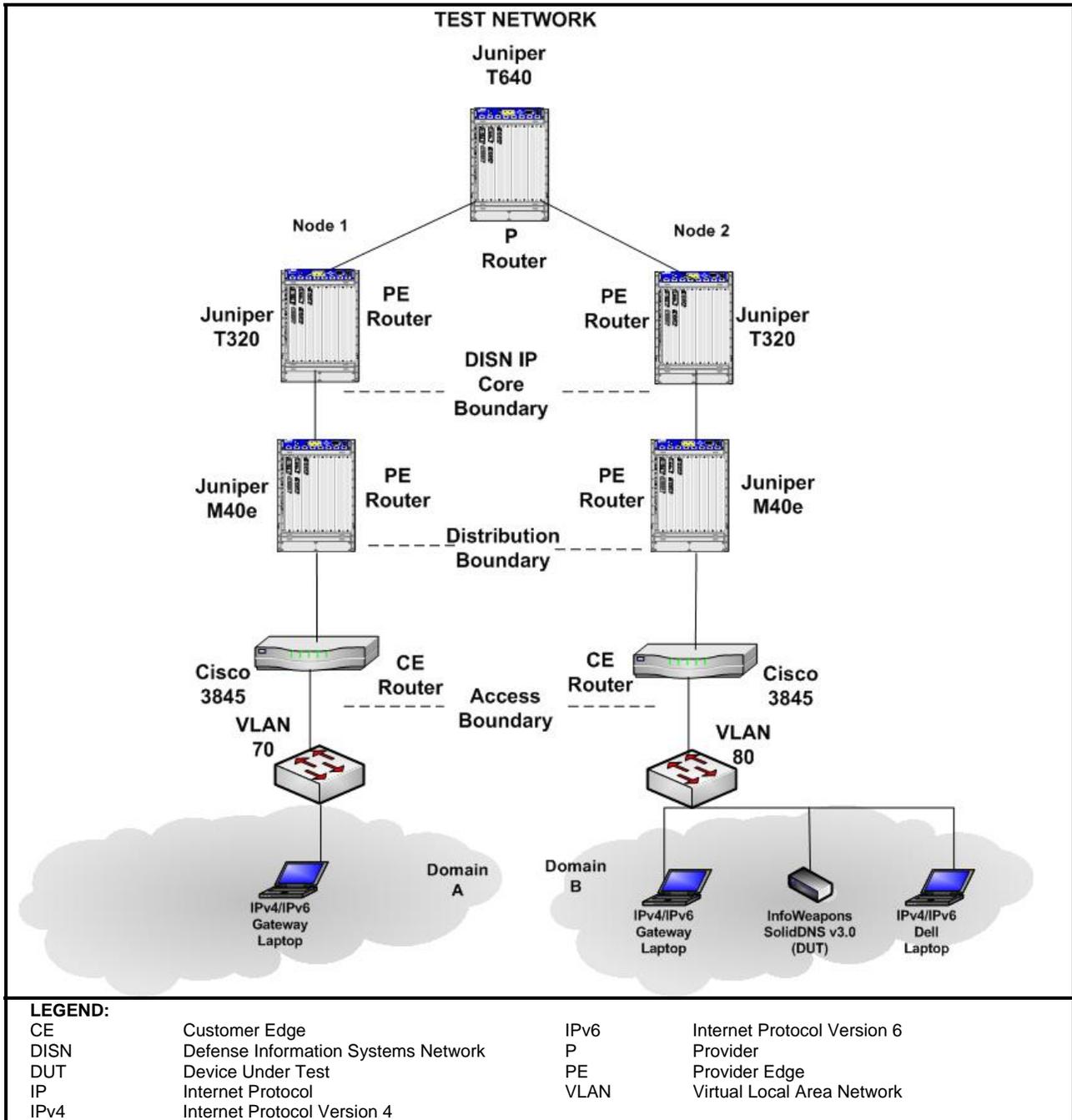
**Table 2-1. IPv6 Capability Requirements and Status (continued)**

InfoWeapons SolidDNS v3.0							
RFC	RFC Title	Testing Completed		Simple Server		Implemented	Comments
		Conformance	Interoperability	Requirement	Met/Not Met		
<b>Host</b>							
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	
<b>LEGEND:</b>							
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						
<b>NOTES:</b>							
1. The device must be conformant to at least one of the Connection Technologies protocols.							
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.							

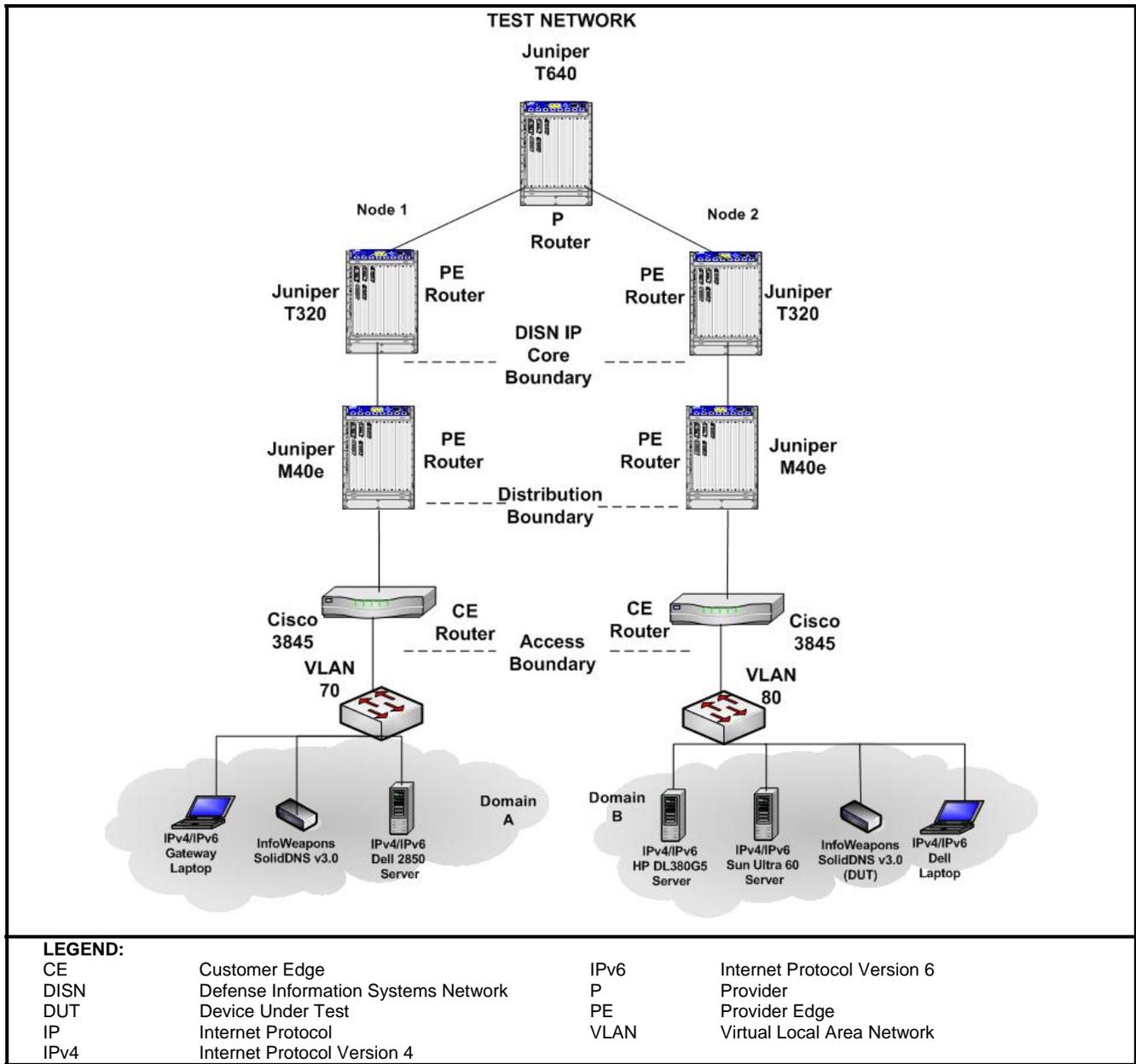
**Table 2-2. DNSSEC Capability Recommendations and Status**

<b>InfoWeapons SolidDNS v3.0</b>					
<b>RFC</b>	<b>RFC Title</b>	<b>Testing Completed</b>	<b>DNS Server</b>	<b>Implemented</b>	<b>Comments</b>
		<b>Conformance</b>	<b>Met/Not Met</b>		
4033	DNS Security Introduction and Requirements	Stated in LoC	Met	Yes	
4034	Resource Records for the DNS Security Extensions	Stated in LoC	Met	Yes	
4035	Protocol Modifications for the DNS Security Extensions	Stated in LoC	Met	Yes	
4431	The DNSSEC Lookaside Validation (DLV) DNS Resource Record	Stated in LoC	Met	Yes	
5074	DNSSEC Lookaside Validation (DLV)	Stated in LoC	Met	Yes	Note 1
<b>LEGEND:</b>					
DNS	Domain Name System	LoC	Letter of Conformance		
DNSSEC	DNS Security	RFC	Request for Comments		
<b>NOTE:</b> SolidDNS 3.0 supports section 3 and section 7 of RFC 5074					

**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 2-3 shows the DNSSEC test network configuration.



**Figure 2-2. InfoWeapons Test Network**



**Figure 2-3. DNSSEC Test Network**

**9. DEVICE CONFIGURATIONS.** Table 2-3 provides hardware and software components used in the InfoWeapons test network. Table 2-4 provides the hardware and software components used in the DNSSEC test network.

**Table 2-3. InfoWeapons Test Configuration Hardware and Software**

Equipment Name	Model Number	IOS/OS/Version(s)
<b>Hardware</b>		
InfoWeapons SolidDNS v3.0 Server - DUT	Dell PowerEdge SC 1435	SolidOS
2 Cisco Routers	Cisco 3845	12.4(11)T
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
1 Dell Notebook	Precision M6400	MS Windows Vista
2 Gateway Notebooks	450ROG	Windows XP Professional
<b>Software</b>		
MS Windows XP Professional	N/A	Version 5.1.2600, SP3 Build 2600
MS Windows Vista	N/A	Version 6.0.6001 SP1 Build 6001
SolidOS	N/A	Based on hardened FreeBSD 7.0
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	T New Technology
OS	Operating System	V Version

**Table 2-4. DNSSEC Test Configuration Hardware and Software**

Equipment Name	Model Number	IOS/OS/Version(s)
<b>Hardware</b>		
InfoWeapons SolidDNS v3.0 Server - DUT	Dell PowerEdge SC 1435	SolidOS
InfoWeapons SolidDNS v3.0 Server	Dell PowerEdge SC 1435	SolidOS
2 Cisco Routers	Cisco 3845	12.4(11)T
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
Dell Notebook	Inspiron 8100	MS Windows XP Professional
Gateway Notebook	450ROG	MS Windows XP Professional
HP ProLiant Server	DL380	MS Windows Server 2008
Sun Microsystems Server	Ultra 60	Sun Microsystems Solaris 10
Dell Server	2850	MS Windows Server 2003
<b>Software</b>		
MS Windows XP Professional	N/A	Build Version 5.1.2600, SP3
MS Windows Server 2003	N/A	Build Version 5.2.3790, SP2
MS Windows Server 2008	N/A	Build Version 6.0.6001 SP1
SolidOS	N/A	Based on hardened FreeBSD 7.0
Sun Microsystems Solaris 10	N/A	Solaris 10 SPARC 6/06 s10s_42wos_09a
Wireshark	N/A	V 1.0.3 (SVN Rev 26134)
<b>LEGEND:</b>		
DUT	Device Under Test	R Release
IOS	Internetworking Operating System	Rev Revision
MS	Microsoft	SP Service Pack
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.1.2.** 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 InfoWeapons SolidDNS v3.0 DNS Server met the 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 InfoWeapons SolidDNS v3.0 DNS Server met the 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 InfoWeapons SolidDNS v3.0 DNS Server met the 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 InfoWeapons SolidDNS v3.0 DNS Server met the 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 InfoWeapons SolidDNS v3.0 DNS Server met the 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 InfoWeapons SolidDNS v3.0 DNS Server met the 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 InfoWeapons SolidDNS v3.0 DNS Server met the requirement.

**Test Case C.1.8.** The RFC 2710 Multicast Listener Discovery 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 InfoWeapons SolidDNS v3.0 DNS Server met the 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 InfoWeapons SolidDNS v3.0 DNS Server met the 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 InfoWeapons SolidDNS v3.0 DNS Server met the requirement.

### **c. DNSSEC Testing.**

The RFC 4033 DNSSEC Introduction and Requirements defines the DNSSEC Extensions add data origin authentication and data integrity to the DNS. The InfoWeapons SolidDNS v3.0 DNS Server met the RFC requirements.

The RFC 4034 Resource Records for the DNSSEC are a collection of resource records and protocol modifications that provide source authentication for the DNS. The RFC defines the public key, delegation signer (DS), resource record digital signature, and authenticated denial of existence resource records. The InfoWeapons SolidDNS v3.0 DNS Server met the RFC requirements.

The RFC 4035 Protocol Modifications for the DNS Extensions are a collection of new resource records and protocol modifications that add data origin authentication and data integrity to the DNS. This RFC describes the DNSSEC protocol modifications. The InfoWeapons SolidDNS v3.0 DNS Server met the RFC requirements.

The RFC 4431 DNSSEC Lookaside Validation (DLV) DNS Resource Record defines a new DNS resource record, called the DNSSEC DLV RR, for publishing DNSSEC trust anchors outside of the DNS delegation chain. The InfoWeapons SolidDNS v3.0 DNS Server met the RFC requirements.

The RFC 5074 DNSSEC DLV is a mechanism for publishing DNSSEC trust anchors outside of the DNS delegation chain. It allows validating resolvers to validate DNSSEC-signed data from zones whose ancestors either are not signed or do not publish DS records for their children. The InfoWeapons SolidDNS v3.0 DNS Server met the RFC requirements.

**d. Conclusion.** The The InfoWeapons SolidDNS v3.0 DNS Server met all the DISR required RFCs and DNSSEC RFC requirements.

**12. TEST AND ANALYSIS REPORT.** 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/>.